ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN GRUP SIMETRI UNTUK MENGAMANKAN INFORMASI

SKRIPSI

OLEH
WASIATUN RISKIYAH
NIM. 12610009

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2016

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN GRUP SIMETRI UNTUK MENGAMANKAN INFORMASI

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Sains (S.Si)

Oleh
Wasiatun Riskiyah
NIM. 12610009

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2016

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN GRUP SIMETRI UNTUK MENGAMANKAN INFORMASI

SKRIPSI

Oleh
Wasiatun Riskiyah
NIM. 12610009

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 26 Mei 2016

Pembimbing I,	Pembimbing II,
H. Wahyu H. Irawan, M.Pd	Mohammad Jamhuri, M.Si
NIP. 19710420 200003 1 003	NIP. 19810502 200501 1 004

Mengetahui,
Ketua Jurusan Matematika

Dr. Abdussakir, M.Pd
NIP. 19751006 200312 1 001

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN GRUP SIMETRI UNTUK MENGAMANKAN INFORMASI

SKRIPSI

Oleh
Wasiatun Riskiyah
NIM. 12610009

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Si)
Tanggal 08 Juni 2016

Penguji Utama : Dr. H. Turmudi, M.Si, Ph.D .....

Ketua Penguji : Hairur Rahman, M.Si .....

Sekretaris Penguji : H. Wahyu H. Irawan, M.Pd .....

Anggota Penguji : Mohammad Jamhuri, M.Si .....

Mengetahui,
Ketua Jurusan Matematika

Dr. Abdussakir, M.Pd
NIP. 19751006 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Wasiatun Riskiyah

NIM : 12610009

Jurusan : Matematika

Fakultas : Sains Dan Teknologi

Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri Untuk Mengamankan Informasi.

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 26 Mei 2016
Yang membuat pernyataan

Wasiatun Riskiyah
NIM. 12610009

MOTO

Lihatlah ke belakang dengan penuh kepuasan dan pandanglah ke depan dengan penuh keyakinan.

PERSEMBAHAN

Dengan rasa syukur penulis persembahkan karya ini kepada:

Ayahanda Marsuki, Ibunda Musliatin dan Nenek Karoso tercinta yang telah memberikan do'a, dukungan, dan semangat kepada penulis. Para guru yang telah memberikan bekal ilmu pengetahuan yang bermanfaat serta sahabat-sahabat yang selalu memberikan semangat yang berarti bagi penulis.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan ke hadirat Allah Swt. yang telah melimpahkan rahmat dan Hidayah-Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul "*Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi*" ini dengan baik. Shalawat serta salam senantiasa tercurahkan kepada Nabi Muhammad Saw. yang telah membimbing umatnya dari berbagai permasalahan menuju kehidupan yang bahagia di dunia dan akhirat.

Suatu kebanggaan tersendiri bagi penulis dapat menyelesaikan skripsi ini yang tentunya tidak terlepas dari bantuan, dukungan, dan sumbangsih dari berbagai pihak. Oleh karena itu patutlah penulis hanturkan ucapan terimakasih yang sebesar-besarnya kepada:

1. Prof Dr. H. Mudjia Rahardjo, M.Si, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. drh. Bayyinatul Muchtaromah, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Abdussakir, M.Pd, selaku ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Drs. H. Turmudi, M.Si, Ph.D selaku dosen wali.
5. H. Wahyu H. Irawan, M.Pd, selaku dosen pembimbing I yang telah memberikan ide mengenai permasalahan skripsi ini serta meluangkan waktunya untuk memberikan bimbingan dengan baik sehingga penulis dapat menyelesaikan skripsi ini.

6. Mohammad Jamhuri, M.Si, selaku pembimbing II yang telah memberikan arahan dan bimbingan selama penyusunan skripsi ini.
7. Seluruh dosen dan staf administrasi Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan ilmu pengetahuan pada penulis.
8. Ayah dan ibu tercinta yang telah memberikan do'a, dukungan, dan semangat kepada penulis.
9. Semua teman-teman matematika 2012, khususnya Irnawati, Fatmawati Hidayat, dan Hendrik Widya Permata, yang selalu memberikan dukungan serta selalu bersama penulis dalam suka dan duka selama mencari ilmu di kampus tercinta serta penghuni kost "Islamiyah", khususnya Ziana Okta Faridah Zaini, Putri Ayu Rahmatilah, Nila Saadah, Daris Madhuri, Diah Atika Pramono, dan Iva Maisaroh atas semangat dan dukungannya kepada penulis.
10. Semua pihak yang tidak mungkin penulis sebut satu persatu, penulis ucapkan terimakasih atas bantuannya.

Akhir kata, semoga skripsi ini dapat memberikan manfaat dan menambah wawasan keilmuan bagi para pembaca.

Wassalamu'alaikum Wr. Wb.

Malang, Mei 2016

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Riskiyah, Wasiatun. 2016. **Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi.** Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (1) H. Wahyu H. Irawan, M.Pd. (II) Mohammad Jamhuri, M.Si.

Kata Kunci: enkripsi, dekripsi, pesan, grup simetri

Enkripsi adalah suatu proses penyandian yang melakukan perubahan pesan dari yang dapat dimengerti disebut dengan *plaintext* menjadi suatu pesan yang sulit dimengerti disebut dengan *ciphertext*, sedangkan proses kebalikannya untuk mengubah *ciphertext* menjadi *plaintext* disebut dekripsi. Proses enkripsi dan dekripsi membutuhkan sebuah kunci rahasia yang harus disepakati oleh pengirim pesan dan penerima pesan. Pada penelitian ini dibahas mengenai enkripsi dan dekripsi pesan dimana dalam perhitungannya menggunakan grup simetri S_n untuk menentukan kunci rahasia. Simulasi pada penelitian ini menggunakan aplikasi App Inventor.

Penelitian ini bertujuan untuk mengetahui proses enkripsi dan dekripsi pesan menggunakan grup simetri S_n untuk mengamankan pesan dan membuat program enkripsi dan dekripsi dalam mengolah pesan. Adapun metode yang digunakan dalam penelitian ini adalah metode kepustakaan yaitu menggunakan literatur yang berkaitan dengan penelitian seperti buku, jurnal penelitian, tesis, skripsi dan laporan penelitian, dengan langkah-langkah: 1) menentukan unsur-unsur grup simetri S_n, 2) menentukan order dari masing-masing unsur, 3) membentuk kunci menggunakan grup simetri S_n, 4) melakukan proses enkripsi dan dekripsi pesan menggunakan kunci grup simteri S_n dengan teknik transposisi (permutasi), dan 5) melakukan proses pembentukan kunci, enkripsi dan dekripsi menggunakan *Android*.

Hasil penelitian menunjukkan bahwa grup simetri S_n dapat diterapkan untuk menentukan kunci rahasia pada proses enkripsi dan dekripsi. Diperoleh kunci yang sama antara pengirim pesan dan penerima pesan, yaitu $K = K_1 = K_2$. Proses enkripsi dilakukan dengan cara mengubah *plaintext* menjadi *ciphertext* dan perhitungannya dilakukan dengan menggunakan kunci yang sudah disepakati, sedangkan proses dekripsi dilakukan dengan cara mengubah *ciphertext* menjadi *plaintext* dan perhitungannya dilakukan dengan menggunakan invers kunci yang sudah disepakati.

ABSTRACT

Riskiyah, Wasiatun. 2016. **Encryption and Decryption of Message Using Symmetry Group to Secure Information**. Thesis. Department of Mathematics Faculty of Science and Technology, State Islamic University of Maulana Malik Ibrahim Malang. Promotor: (1) H. Wahyu H. Irawan, M.Pd. (II) Mohammad Jamhuri, M.Si.

Kata Kunci: encryption, decryption, message, symmetry group

Encryption is encoding message from that can be understood referred to plaintext into a message that is difficult to be understood referred to ciphertext, while the opposite process is transforming ciphertext into plaintext referred to decryption. Encryption and decryption process need a secret key that must be agreed by the sender of message and receiver of message. This research discussed about encryption and decryption of message where in its calculation it uses symmetry group for determining the secret key. The simulation for this research used App Inventor aplication.

The aim of this study is to determine the encryption and decryption process of message using symmetry group to secure message and build an encryption and decryption program in processing message. This research used literature method that is used literature which is relevant to the research such as book, journal, thesis, and research report, by the steps: 1) deciding elements of symmetry group, 2) deciding order of every element, 3) determining the key using symmetry group, 4) encrypting and decrypting using the key of symmetry group key by transposition technique (permutation), and 5) key formating, encrypting and decrypting using android.

The research result show that the symmetry group can be applied to determine the secret key to process of encryption and decryption. It is obtained the same key between the sender and the receiver that is $K = K_1 = K_2$. Encryption process is done by encoding plaintext tobe ciphertext and the calculate is done by using key that has been agreed, while decryption process is done by changing ciphertext tobe plaintext and the calculation is done by using key inverse that has been agreed.

ملخص

رزكية، واسية. 2016. **تشفير وفك الشفرة الرسالة باستخدام symmetry group لأ من المعلومات**. بحث جامعي. شعبة الرياضيات. كلية العلوم والتكنولوجيا الجامعة الإسلامية الحكومية مولانا مالك إبراهيم مالنج. المشرف (1) الحج وحي هنكي إراوان الماجيستير المشرف (2) محمد جمهوري الماجستير.

الكلمات الرئيسية: تشفير، فك الشفرة، الرسالة، symmetry group

التشفير هو عملية رمزية تحويل الرسالة المفهومة يسمى نص بحرد مبحرد إلى الرسالة المصعبة يسمى بنص مشفر، والعكس يطلق فك الشفرة. في عملية التشفير وفك الشفرة تحتاج المفتاح السري المتفق على المرسل والمرسل. في هذا البحث الجامعي بحثت الباحثة تشفير وفك الشفرة الرسالة باستخدام symmetry groupS_n لتعيين المفتاح السري، وهذه المحاكاة باستخدام برمجة App Inventor.

وهدف البحث هو لمعرفة عملية تشفير وفك الشفرة الرسالة باستخدام symmetry S_n group لأمن المعلومات وصناعة برمجة التشفير وفك الشفرة في تنظيم الرسالة وينتهج هذا البحث بدراسة مكتبية وهي الاداب المعلقة بهذا البحث على سبيل المثال الكتب، المجلة العلمية، رسالة الماجستير، البحث الجامعي، والبحوث العلمية. وهذه هي الخطوات: (1) تعيين عناصرS_n symmetry group، (2) تعيين ترتين هذه العناصر، (3) تشكيل المفتاح باستخد امS_n symmetry group، (4) عملية تشفير وفك الشفرة الرسالة باستخدام symmetry groupS_n بطريقة التحويل (permutation)، و (5) عملية تشكيل المفتاح، التشفير وفك الشفرة باستخدام Android.

والنتائج لهذا البحث يدل على أن symmetry groupS_n يستطيع بتطبيق على تعيين المفتاح السري في عملية التشفير وفك الشفرة. ينال المفتاح المتسوي بين المرسل والمرسل وهو $K_2 = K_1 = K$. عملية التشفير بتحويل الرسالة المفهومة يسمى نص بحرد إلى الرسالة المصعبة يسمي بنص مشفر، ويستخدم الحساب بالمفتاح المتفق، والعكس يطلق بفك الشفرة ويستخدم الحساب بالمفتاح المتفق.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini, teknologi informasi dan komunikasi sangat berpengaruh besar terhadap segala aspek kehidupan, mulai dari aspek sosial, politik, budaya, pendidikan dan lain sebagainya. Salah satu kegunaan dari teknologi informasi dan komunikasi yaitu dalam proses pengiriman pesan. Namun, proses pengiriman pesan tidak begitu aman karena merupakan jalur komunikasi umum yang dapat digunakan oleh siapapun. Sehingga sangat rawan terhadap penyadap yang ingin merubah pesan yang dikirim. Salah satu solusi untuk mengatasi masalah tersebut adalah menggunakan enkripsi dan dekripsi pesan.

Enkripsi adalah suatu proses penyandian yang melakukan perubahan pesan dari yang dapat dimengerti disebut dengan *plaintext* menjadi suatu pesan yang sulit dimengerti disebut dengan *ciphertext,* sedangkan proses kebalikannya untuk mengubah *ciphertext* menjadi *plaintext* disebut dekripsi (Munir dalam Wicaksono, 2014). Proses enkripsi dan dekripsi bertujuan agar pesan yang dikirim tidak dibaca oleh orang yang tidak berhak menerimanya. Dengan kata lain, pesan adalah sebuah amanat yang harus disampaikan kepada penerimanya, seperti penggalan firman Allah Swt. dalam al-Quran surat an-Nisa'/4:58, yaitu:

إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi

pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat"(QS. an-Nisaa'/4:58).

Berdasarkan firman Allah Swt. dalam surat an-Nisaa' ayat 58 menjelaskan bahwa Allah menyuruh manusia untuk menyampaikan amanat kepada orang yang berhak menerimanya. Selain orang yang berhak menerima amanat tersebut maka orang lain tidak boleh mengetahuinya.

Proses enkripsi dan dekripsi pesan membutuhkan sebuah kunci rahasia yang disepakati oleh kedua belah pihak yaitu pengirim pesan dan penerima pesan. Untuk mengatasi masalah tersebut maka digunakan suatu metode dalam kriptografi yang disebut dengan protokol perjanjian kunci. Protokol perjanjian kunci bertujuan agar pengirim pesan dan penerima pesan dapat menentukan kunci rahasia yang sama. Pada penelitian Stickel (2005) dalam Myasnikov dkk (2008) diperkenalkan metode mengenai protokol perjanjian kunci yang menggunakan grup tidak komutatif. Grup $(G,\circ)$ disebut grup tidak komutatif jika operasi komposisi "$\circ$" tidak bersifat komutatif yaitu $(\forall\, a,b \in G)\; a \circ b \neq b \circ a$. Untuk menggunakan grup tidak komutatif, maka protokol perjanjian kunci dikontruksi terlebih dahulu menggunakan suatu permasalahan matematis yang ada pada grup tidak komutatif. Salah satu grup yang dapat digunakan yaitu grup simetri-n. Misal S adalah sebarang himpunan tak kosong dan S_n adalah himpunan yang memuat semua fungsi-fungsi bijektif dari S ke S. Himpunan S_n apabila dikenai operasi komposisi "$\circ$" atau $(S_n,\circ)$ disebut grup simetri S_n. Grup simetri S_n memiliki unsur sebanyak $n!$.

Berdasarkan uraian tersebut, pada penelitian ini dibahas mengenai enkripsi dan dekripsi pesan dimana dalam perhitungannya menggunakan grup simetri S_n

untuk menentukan kunci rahasia. Kunci tersebut yang akan digunakan pada proses enkripsi dan dekripsi pesan. Dengan demikian penulis mengambil judul "Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi".

1.2 Rumusan Masalah

Berdasarkan pada latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana proses enkripsi pesan menggunakan grup simetri S_n untuk mengamankan pesan?
2. Bagaimana proses dekripsi pesan menggunakan grup simetri S_n untuk mengamankan pesan?
3. Bagaimana program enkripsi dan dekripsi dalam mengolah pesan?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah:

1. Untuk mengetahui proses enkripsi pesan menggunakan grup simetri S_n untuk mengamankan pesan.
2. Untuk mengetahui proses dekripsi pesan menggunakan grup simetri S_n untuk mengamankan pesan.
3. Untuk membuat program enkripsi dan dekripsi dalam mengolah pesan.

1.4 Manfaat Penelitian

Penelitian ini dilakukan dengan harapan dapat bermanfaat bagi berbagai pihak berikut:

1. Bagi penulis

   Dapat memperkaya sumber pengetahuan tentang kriptografi khususnya pada enkripsi dan dekripsi pesan menggunakan grup simetri untuk mengamankan informasi.

2. Bagi pembaca

   Dapat menambah wawasan dan pengetahuan tentang kriptografi dan solusi bagi pihak-pihak yang menggunakan sarana informasi dan komunikasi untuk dapat melakukan pengiriman informasi secara aman.

3. Bagi lembaga

   Dapat menambah bahan kepustakaan dan informasi pembelajaran mata kuliah yang berhubungan dengan kriptografi.

1.5 Batasan Masalah

Agar pembahasan pada penelitian ini tidak meluas, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Grup simetri S_n yang digunakan yaitu dari grup simetri S_4 sampai grup simetri S_7.
2. Algoritma yang digunakan pada proses pembentukan kunci menggunakan protokol perjanjian kunci Stickel yang perhitungannya berdasarkan grup simetri oleh dua pihak yang berbeda yaitu pengirim pesan dan penerima pesan.

3. Pada proses enkripsi dan dekripsi menggunakan kunci grup simetri dengan teknik transposisi (permutasi).
4. Untuk mempermudah proses enkripsi dan dekripsi pesan digunakan alat bantu pemograman *Android*.

1.6 Metode Penelitian

Dalam penelitian ini, metode yang digunakan adalah metode kepustakaan (*library research*) yaitu menggunakan literatur yang berkaitan dengan penelitian seperti buku, jurnal penelitian, tesis, skripsi dan laporan penelitian. Untuk mencapai tujuan yang diinginkan maka langkah-langkah yang digunakan dalam penelitian ini adalah:

1. Menentukan unsur-unsur grup simetri S_n.
2. Menentukan order dari unsur-unsur grup simetri S_n.
3. Membentuk kunci menggunakan grup simetri S_n oleh dua pihak yang berbeda yaitu pengirim pesan dan penerima pesan.
4. Menerapkan proses nomor 3 pada grup simetri S_4 sampai grup simetri S_7.
5. Pengirim pesan menulis *plaintext*.
6. Pengirim pesan membagi *plaintext* per blok.
7. Pengirim pesan mengenkripsikan *plaintext* per blok menggunakan kunci grup simetri dengan teknik transposisi (permutasi) menjadi *ciphertext*.
8. Pengirim pesan mengirim *ciphertext* kepada penerima pesan.
9. Penerima pesan menerima *ciphertext* dari Pengirim pesan.
10. Penerima pesan membagai *ciphertext* per blok.

11. Penerima pesan mendekripsikan *ciphertext* per blok menggunakan invers kunci grup simetri dengan teknik transposisi (permutasi) menjadi *ciphertext*.
12. Penerima pesan menterjemahkan *plaintext*.
13. Pengirim pesan dan penerima pesan melakukan proses pembentukan kunci, enkripsi dan dekripsi menggunakan *Android*.

1.7 Sistematika Penulisan

Sistematika penulisan digunakan untuk mempermudah dalam memahami penelitian ini. Dalam sistematika penulisan penelitian ini terbagi menjadi empat bab dan masing-masing bab dibagi dalam subbab sebagai berikut:

Bab I Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metode penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Bab ini menjelaskan tentang definisi grup, grup simetri, order dari unsur, kelipatan persekutuan terkecil, kriptografi, enkripsi dan dekripsi dalam keamanan informasi, macam-macam algoritma kriptografi, kriptografi klasik dan modern, teknik transposisi (permutasi), protokol perjanjian kunci, dan definisi App Inventor.

Bab III Pembahasan

Bab ini menguraikan secara keseluruhan langkah-langkah yang disebutkan dalam metode penelitian dan menjawab semua rumusan masalah.

Bab IV Penutup

Bab ini berisi tentang kesimpulan penelitian dan saran untuk penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1 Definisi Grup

Sistem aljabar $(G,*)$ yang berisikan himpunan tak kosong G dan operasi $*$ disebut grup jika memenuhi aksioma- aksioma berikut:

1. Operasi $*$ bersifat tertutup di G

   $\forall a,b \in G$ maka $a * b \in G$.

2. Operasi $*$ bersifat assosiatif di G

   $(a * b) * c = a * (b * c),\ \forall a,b,c \in G$.

3. G mempunyai unsur identitas terhadap operasi $*$ terdapat unsur identitas di G yang dinotasikan dengan e sedemikian sehingga, $e * a = a * e = a, \forall a \in G$.

4. Setiap unsur di G mempunyai invers terhadap operasi $*$ untuk setiap $a \in G$ terdapat $a^{-1} \in G$ sedemikian sehingga $a^{-1} * a = a * a^{-1} = e$ (Raisinghania dan Aggarwal, 1980:31).

Contoh 2.1:

Misalkan Z adalah himpunan bilangan bulat, maka $(Z,+)$ adalah grup karena berlaku:

1. $\forall\ p,q \in Z$, maka $p + q \in Z$.

   Jadi Z tertutup terhadap operasi penjumlahan.

2. $\forall p,q,r \in Z$, maka $(p + q) + r = p + (q + r)$.

   Jadi operasi penjumlahan bersifat assosiatif di Z.

3. Ambil $0 \in Z$, sehingga $p + 0 = 0 + p = p, \forall\ p \in Z$.

Jadi 0 adalah unsur identitas pada operasi penjumlahan.

4. $\forall\, p \in Z$. Terdapat $-p \in Z$. Sehingga $p + (-p) = (-p) + p = 0$.

   Jadi invers dari p adalah $-p$.

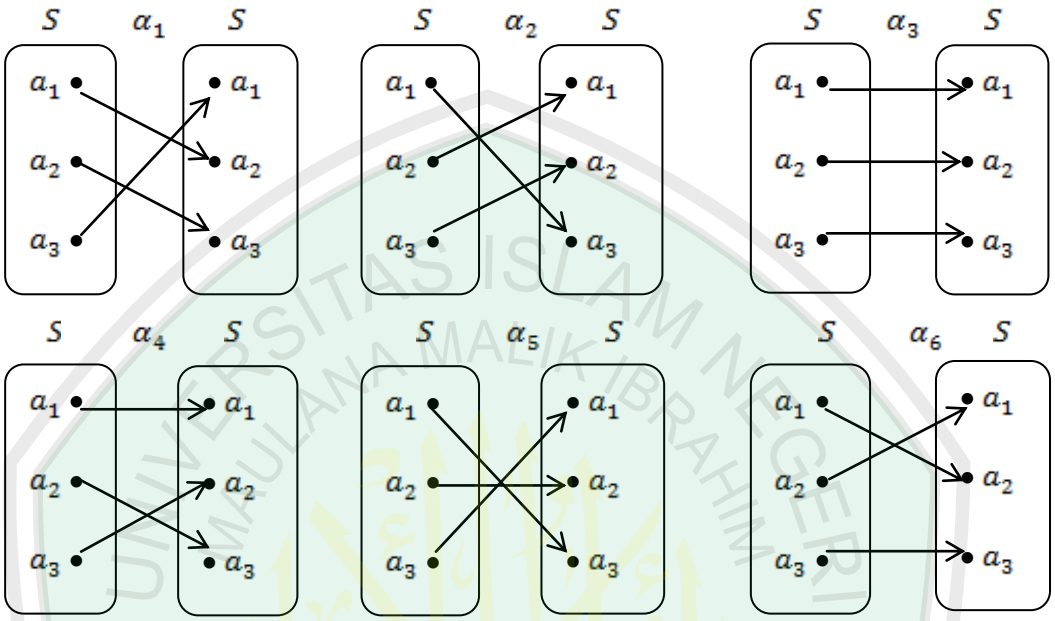
2.2 Grup Simetri

Misal Ω adalah sebarang himpunan tak kosong dan S_Ω adalah himpunan yang memuat semua fungsi-fungsi bijektif dari Ω ke Ω (atau himpunan yang memuat semua permutasi dari Ω). Himpunan S_Ω dengan operasi komposisi " $\circ$ " atau $(S_\Omega, \circ)$ adalah suatu grup. Operasi komposisi " $\circ$ " adalah suatu operasi biner pada S_Ω karena jika $\sigma: \Omega \to \Omega$ dan $\tau: \Omega \to \Omega$ adalah fungsi-fungsi bijektif maka $\sigma \circ \tau$ juga merupakan suatu fungsi bijektif dari Ω ke Ω. Selanjutnya operasi " $\circ$ " adalah komposisi fungsi yang bersifat assosiatif. Identitas dari S_Ω adalah permutasi 1 yang didefinisikan dengan $1(a) = a, \forall a \in \Omega$. Untuk setiap permutasi $\sigma: \Omega \to \Omega$ terdapat fungsi invers $\sigma^{-1}: \Omega \to \Omega$ yang memenuhi $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Dengan demikian semua aksioma grup telah dipenuhi oleh $(S_\Omega, \circ)$. Grup $(S_\Omega, \circ)$ disebut sebagai grup simetri pada himpunan Ω (Dummit dan Foote, 2004:29).

Karena fungsi-fungsi bijektifnya adalah dari Ω ke dirinya sendiri maka fungsi-fungsi bijektif tersebut dapat dinyatakan dalam bentuk permutasi. Sehingga himpunan S_Ω dapat dikatakan sebagai himpunan semua permutasi dari Ω ke Ω. Oleh karena itu, grup simetri $(S_\Omega, \circ)$ dapat pula dikatakan sebagai grup permutasi.

Contoh 2.2:

Misal diberikan himpunan tak kosong S, dengan $S = \{a_1, a_2, a_3\}$. Apabila S dikenai fungsi bijektif dari S ke S, maka dapat didaftar semua fungsi-fungsi bijektifnya sebagai berikut:



Gambar 2.1 Fungsi-Fungsi Bijektif dari Himpunan S ke S

Setelah mengetahui fungsi-fungsi bijektif dari himpunan S ke S, maka dapat dituliskan fungsi-fungsi bijektif tersebut ke dalam bentuk sikel berikut:

$$\alpha_1 = (a_1 \quad a_2 \quad a_3) \qquad \alpha_4 = (a_1)(a_2 \quad a_3)$$

$$\alpha_2 = (a_1 \quad a_3 \quad a_2) \qquad \alpha_5 = (a_2)(a_1 \quad a_3)$$

$$\alpha_3 = (a_1)(a_2)(a_3) \qquad \alpha_6 = (a_3)(a_1 \quad a_2)$$

Misal S_3 merupakan himpunan semua fungsi bijektif dari S ke S, dengan $S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$. Himpunan S_3 apabila dikenal operasi komposisi "$\circ$" pada S_3, maka struktur $(S_3, \circ)$ membentuk grup simetri-3. Hal tersebut dapat dilihat pada tabel Cayley seperti berikut:

Tabel 2.1 Tabel Cayley Hasil Operasi Komposisi dari S_3

$\circ$	α_1	α_2	α_3	α_4	α_5	α_6
α_1	α_2	α_3	α_1	α_6	α_4	α_5
α_2	α_3	α_1	α_2	α_5	α_6	α_4
α_3	α_1	α_2	α_3	α_4	α_5	α_6
α_4	α_5	α_6	α_4	α_3	α_4	α_2
α_5	α_6	α_4	α_5	α_2	α_3	α_4
α_6	α_4	α_5	α_6	α_4	α_2	α_3

Sehingga terbukti bahwa:

1. Operasi komposisi " $\circ$ " tertutup pada S_3.
2. Operasi komposisi " $\circ$ " assosiatif pada S_3.
3. S_3 mempunyai unsur identitas terhadap operasi komposisi yaitu α_3.
4. Setiap unsur S_3 mempunyai invers pada operasi komposisi " $\circ$ ".

Dengan demikian $(S_3,\circ)$ adalah grup.

2.3 Order dari Unsur

Misal $(G, *)$ adalah sebarang grup. Misal a adalah sebarang unsur dari G. Untuk suatu bilangan positif terkecil m yang memenuhi $a^m = e$ (e adalah unsur identitas di G) maka m dikatakan sebagai order dari unsur a dan dituliskan sebagai $|a| = m$ (Raisinghania dan Aggarwal, 1980:91).

Contoh 2.3:

Diberikan grup simetri S_3 dengan operasi komposisi " $\circ$ " atau $(S_3,\circ)$

Unsur-unsur dari grup simetri S_3 adalah sebagai berikut:

$$\alpha_1 = (a_1 \quad a_2 \quad a_3) \qquad \alpha_4 = (a_1)(a_2 \quad a_3)$$

$$\alpha_2 = (a_1 \quad a_3 \quad a_2) \qquad \alpha_5 = (a_2)(a_1 \quad a_3)$$

$$\alpha_3 = (a_1)(a_2)(a_3) \qquad \alpha_6 = (a_3)(a_1 \quad a_2)$$

Unsur identitas adalah α_3, maka

$\alpha_1 \circ \alpha_1 \circ \alpha_1 = \alpha_2 \circ \alpha_1 = \alpha_3$ maka $|\alpha_1| = 3$

$\alpha_2 \circ \alpha_2 \circ \alpha_2 = \alpha_1 \circ \alpha_2 = \alpha_3$ maka $|\alpha_2| = 3$

$|\alpha_3| = 1$

$\alpha_4 \circ \alpha_4 = \alpha_3$ maka $|\alpha_4| = 2$

$\alpha_5 \circ \alpha_5 = \alpha_3$ maka $|\alpha_5| = 2$

$\alpha_6 \circ \alpha_6 = \alpha_3$ maka $|\alpha_6| = 2$

Dengan demikian diperoleh

$|\alpha_1| = |\alpha_2| = 3$ dan $|\alpha_3| = 1$ $|\alpha_4| = |\alpha_5| = |\alpha_6| = 2$

2.4 Kelipatan Persekutuan Terkecil

Jika $x, y \in Z$, $x \neq 0$, dan $y \neq 0$, maka:

a. m disebut kelipatan persekutuan (*common multiple*) dari x dan y jika $x|m$ dan $y|m$

b. m disebut kelipatan persekutuan terkecil (*least common multiple*) dari x dan y jika m adalah bilangan bulat positif terkecil sehingga $x|m$ dan $y|m$

Notasi:

$m = [x, y]$ dibaca m adalah kelipatan persekutuan terkecil dari x dan y.

Dengan jalan yang sama dapat didefinisikan kelipatan persekutuan terkecil dari 3 bilangan, 4 bilangan, ..., n bilangan, misalnya:

$p = [x, y, z]$ dibaca p adalah kelipatan persekutuan terkecil dari $x, y,$ dan z.

$q = [a, b, c, d]$ dibaca q adalah kelipatan persekutuan terkecil dari $a, b, c,$ dan d. (Muhsetyo, 1997:77).

Contoh 2.4:

Diberikan grup simetri S_3 dengan operasi komposisi " $\circ$ " atau $(S_3, \circ)$

Unsur-unsur dari grup simetri S_3 adalah sebagai berikut:

$$\alpha_1 = (a_1 \quad a_2 \quad a_3) \qquad \alpha_4 = (a_1)(a_2 \quad a_3)$$

$$\alpha_2 = (a_1 \quad a_3 \quad a_2) \qquad \alpha_5 = (a_2)(a_1 \quad a_3)$$

$$\alpha_3 = (a_1)(a_2)(a_3) \qquad \alpha_6 = (a_3)(a_1 \quad a_2)$$

Unsur identitas adalah α_3, maka

Order dari unsur $\alpha_1 = (a_1 \quad a_2 \quad a_3)$ adalah $|\alpha_1| = 3$

Order dari unsur $\alpha_2 = (a_1 \quad a_3 \quad a_2)$ adalah $|\alpha_2| = 3$

Order dari unsur $\alpha_3 = (a_1)(a_2)(a_3)$ adalah $|\alpha_3| = 1$

Order dari unsur $\alpha_4 = (a_1)(a_2 \quad a_3)$ adalah $|\alpha_4| = [1,2] = 2$

Order dari unsur $\alpha_5 = (a_2)(a_1 \quad a_3)$ adalah $|\alpha_5| = [1,2] = 2$

Order dari unsur $\alpha_6 = (a_2)(a_1 \quad a_3)$ adalah $|\alpha_6| = [1,2] = 2$

2.5 Kriptografi

2.5.1 Pengertian dan Sejarah Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua yaitu *crypto* dan *graphia*, *crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain (Ariyus, 2008:13).

Kriptografi mempunyai sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang Mesir lewat *hieroglyph*. Jenis tulisan ini bukanlah bentuk standar untuk menulis pesan. Dikisahkan, pada Zaman Romawi Kuno, pada suatu saat julius Caesar ingin mengirim pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir. Karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka dijalan. Julius Caesar kemudian memikirkan bagaimana mengatasinya. Ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun terkecuali oleh jenderalnya saja. Tentu sang jenderal telah diberi tahu sebelumnya bagaimana cara membaca pesan teracak tersebut. Yang dilakukan Jelius Caesar adalah mengganti semua susunan alfabet dari a, b, c, yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya (Ariyus, 2008:13-14).

Selama bertahun-tahun kriptografi menjadi bidang khusus yang hanya dipelajari oleh pihak militer, seperti agen keamanan Nasioanal Amerika (*National Security Agency*), Uni Soviet, Inggris, Perancis, Israel, dan Negara-negara lainnya yang telah membelanjakan miliaran dolar untuk mengamankan komunikasi mereka dari pihak luar, tapi mereka selalu mempelajari kode-kode rahasia negara lain, dengan adanya persaingan ini maka kriptografi terus berkembang sesuai dengan perkembangan zaman (Ariyus, 2006:11).

2.5.2 Enkripsi dan Dekripsi dalam Keamanan Informasi

Pada dasarnya untuk menjaga keamanan informasi terdiri dari beberapa komponen, antara lain:

1. Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli disebut *plaintext* (teks biasa), yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode. Sama halnya dengan tidak mengerti sebuah kata maka dapat dilihat di dalam kamus atau daftar istilah. Untuk mengubah teks biasa ke bentuk teks kode dapat kita gunakan algoritma yang mengkodekan data yang kita inginkan.
2. Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli). Algoritma yang digunakan untuk dekripsi tertu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).
4. *Ciphertext* merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karekter yang tidak mempunyai makna (arti).
5. *Plaintext* sering disebut dengan *cleartext*. Teks asli atau teks biasa ini merupakan pesan yang ditulis atau diketik yang memiliki makna. Teks asli inilah yang diproses menggunakan algoritma kriptografi untuk menjadi *ciphertext* (teks kode).
6. Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dan lain sebagainya) atau yang disimpan di dalam media perekaman (kertas, *storage*, dan lain sebagainya).
7. *Cryptanalysis* bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks asli tanpa mengetahui kunci yang sah secara wajar. Jika

suatu teks kode berhasil diubah menjadi teks asli tanpa menggunakan kunci yang sah, proses tersebut dinamakan *breaking code*. Hal ini dilakukan oleh para kriptanalis. Analisis kode juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci atau teks asli dari teks kode yang dienkripsi dengan algoritma tertentu (Ariyus, 2008:10-11).

2.5.3 Macam-Macam Algoritma Kriptografi

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan dari kunci yang dipakainya:

1. Algoritma simetri (menggunakan satu kunci untuk enkripsi dan dekripsi).
2. Algoritma asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi).
3. *Hash function.*

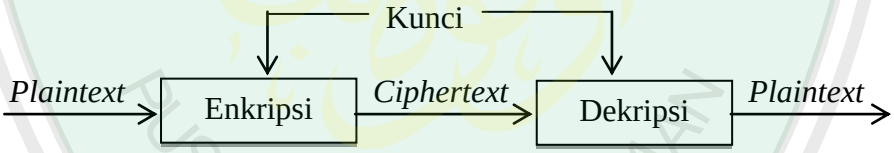
2.5.3.1 Algoritma Simetri

Algoritma ini juga sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Algoritma ini sudah ada lebih dari 4000 tahun yang lalu. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan tersebut (Ariyus, 2008:44). Masalah akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh sebanyak c pihak dan setiap dua

pihak yang melakukan pertukaran kunci, maka akan terdapat sebanyak $\frac{1}{2}c(c-1)$ kunci rahasia yang harus dipertukarkan secara aman (Riyanto, 2010:54). Algoritma yang memakai kunci simetri di antaranya adalah:

1. Substitusi,
2. Transposisi (permutasi),
3. *Data Encryption Standard* (DES),
4. RC2, RC4, RC5, RC6,
5. *International Data Encryption Algorithm* (IDEA),
6. *Advanced Encryption Standard* (AES),
7. *One Time Pad* (OTP),
8. A5, dan lain sebagainya.

Secara sederhana proses pengiriman pesan dengan algoritma simetri dapat digambarkan sebagai berikut:



Gambar 2.2 Skema Algoritma Simetri

2.5.3.2 Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1. Kunci umum (*public key*): Kunci yang boleh semua orang tahu (dipublikasikan).

2. Kunci rahasia (*private key*): Kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

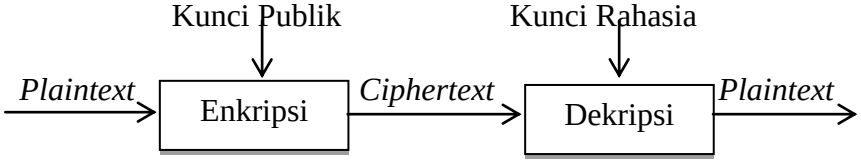
Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsinya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut. Algoritma asimetri bisa mengirimkan pesan dengan lebih aman daripada algoritma simetri. Contoh Bob mengirim pesan ke Alice menggunakan algoritma asimetri. Hal yang harus dilakukan adalah:

1. Bob memberitahukan kunci publiknya ke Alice.
2. Alice mengenkripsi pesan dengan menggunakan kunci publik Bob.
3. Bob mendekripsi pesan dari Alice dengan kunci rahasianya.
4. Begitu juga sebaliknya jika Bob ingin mengirim pesan ke Alice.

Algoritma yang memakai kunci publik di antaranya adalah:

1. *Digital Signature Algorithm (*DSA*),*
2. RSA,
3. *Diffie-Hellman* (DH),
4. *Elliptic Curve Cryptography* (ECC),
5. *Kriptografi Quantum*, dan lain sebagainya.

Secara sederhana proses pengiriman pesan dengan algoritma asimetri dapat digambarkan sebagai berikut:



Gambar 2.3 Skema Algoritma Asimetri

2.5.3.3 Fungsi Hash

Fungsi hash sering disebut dengan fungsi hash satu arah (*one-way function*), *meassage digest*, *fingerprint*, fungsi kompresi dan *message authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tepat. Fungsi hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda yang menandakan bahwa pesan tersebut benar-benar berasal dari orang yang diinginkan (Ariyus, 2008:44-46).

2.5.4 Kriptografi Klasik dan Modern

Kriptografi klasik merupakan suatu algoritma yang menggunakan suatu kunci untuk mengamankan data. Teknik ini sudah digunakan beberapa abad yang lalu. Dua teknik dasar yang biasa digunakan pada algoritma jenis ini adalah sebagai berikut:

1. Teknik substitusi: Penggantian setiap karakter teks-asli dengan karakter lain.
2. Teknik transposisi (permutasi): Dilakukan dengan menggunakan permutasi karakter.

Sedangkan kriptografi modern mempunyai kerumitan yang sangat kompleks karena dioperasikan menggunakan komputer (Ariyus, 2008:46).

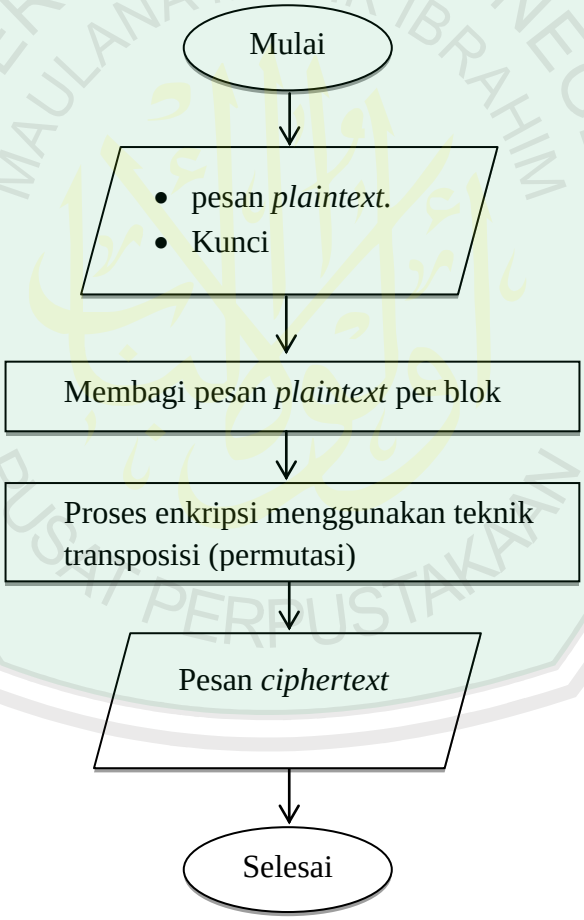
2.5.5 Teknik Transposisi (Permutasi)

Pada bagian ini akan dibahas teknik permutasi (transposisi kode). Teknik ini menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini

pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula (Ariyus, 2008:75). Algoritma enkripsi menggunakan teknik transposisi (permutasi) dengan melakukan permutasi π pada teks asli (*plaintext*), sedangkan algoritma dekripsi dengan melakukan invers permutasi π^{-1} pada teks kode (*ciphertext*) (Sadikin, 2012:61).

1. Proses Enkripsi Teknik Transposisi (Permutasi)

Proses enkripsi menggunakan teknik transposisi (permutasi) ini dapat dijelaskan dalam *flowchart* sebagai berikut:

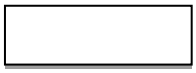


Gambar 2.4 Proses Enkripsi Teknik Transposisi (Permutasi)

Keterangan:

 : Permulaan atau akhir program.

: Poses input atau output data, parameter dan informasi.



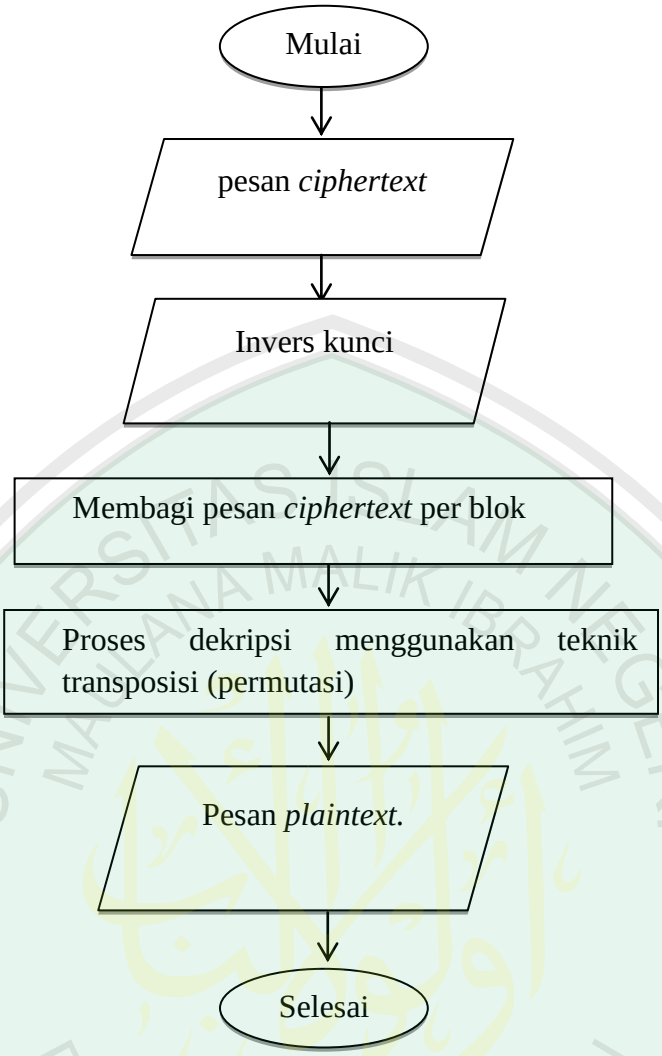
: Proses perhitungan atau proses pengolahan data.

: Arah aliran program

Langkah awal dari proses enkripsi dengan teknik transposisi (permutasi) adalah membagi pesan *plaintext* menjadi per blok yang terdiri dari beberapa huruf. Kunci pada teknik transposisi (permutasi) ini menggunakan bentuk permutasi-n, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula (Ariyus, 2008:75).

2. Proses Dekripsi Teknik Transposisi (Permutasi)

Proses dekripsi menggunakan teknik transposisi (permutasi) ini dapat dijelaskan dalam *flowchart* sebagai berikut:



Gambar 2.5 Proses Dekripsi Teknik Transposisi (Permutasi)

Pada dasarnya proses dekripsi sama saja dengan proses enkripsi, akan tetapi pada proses ini penerima pesan mendeskripsikan pesan *ciphertext* dengan menginverskan kunci yang telah disepakati.

Contoh 2.5:

Ada 6 kunci untuk melakukan permutasi kode:

x	a_1	a_2	a_3	a_4	a_5	a_6
$\pi(x)$	a_3	a_5	a_1	a_6	a_4	a_2

Dan 6 kunci untuk invers dari permutasi tersebut:

x	a_1	a_2	a_3	a_4	a_5	a_6
$\pi^{-1}(x)$	a_3	a_6	a_1	a_5	a_2	a_4

Seandainya kita akan melakukan permutasi terhadap kalimat dibawah ini:

SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

Terlebih dahulu kalimat tersebut dibagi menjadi 6 blok dan apabila terjadi kekurangan dari blok bisa ditambah dengan huruf yang disukai, misal $ dan spasi dilambangkan dengan #. Hal ini berguna untuk mempersulit analisis dari kode tersebut.

SAYA#S | EDANG# | BELAJA | R#KEAM

ANAN#K | OMPUTE | R$$$$$

Setelah dibagi menjadi 6 blok maka dengan menggunakan kunci nomor satu di atas setiap blok akan berubah menjadi seperti di bawah ini:

Blok I : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ S & A & Y & A & \# & S \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ Y & \# & S & S & A & A \end{pmatrix}$

$=$ Y#SSAA

Blok II : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ E & D & A & N & G & \# \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ A & G & E & \# & N & D \end{pmatrix}$

$=$ AGE#ND

Blok III : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ B & E & L & A & J & A \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ L & J & B & A & A & E \end{pmatrix}$

$=$ LJBAAE

Blok IV : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{R} & \# & \text{K} & \text{E} & \text{A} & \text{M} \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ \text{K} & \text{A} & \text{R} & \text{M} & \text{E} & \# \end{pmatrix}$

$=$ KARME#

Blok V : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{A} & \text{N} & \text{A} & \text{N} & \# & \text{K} \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ \text{A} & \# & \text{A} & \text{K} & \text{N} & \text{N} \end{pmatrix}$

$=$ A#AKNN

Blok VI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{O} & \text{M} & \text{P} & \text{U} & \text{T} & \text{E} \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ \text{P} & \text{T} & \text{O} & \text{E} & \text{U} & \text{M} \end{pmatrix}$

$=$ PTOEUM

Blok VII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{R} & \$ & \$ & \$ & \$ & \$ \\ a_3 & a_5 & a_1 & a_6 & a_4 & a_2 \\ \$ & \$ & \text{R} & \$ & \$ & \$ \end{pmatrix}$

$=$ $$R$$$

Jadi *ciphertext* yang dihasilkan

Y#SSAAAGE#NDLJBAAEKARME#A#AKNNPTOEUM$$R$$$

Untuk mengembalikan ke bentuk teks-asli maka dilakukan invers terhadap *ciphertext* dengan mengikuti kunci nomor dua di atas.

Ada banyak teknik untuk permutasi ini, seperti zig-zag, segitiga, spiral dan diagonal.

1. Zig-zag: memasukkan teks-asli dengan pola zig-zag seperti contoh di bawah ini:

			A						G						A						A						M					X
		Y		S				N		B				J		R				M		N				O		P				R	
	A				E		A				E		A				K		A				A		K				U		E		
S						D						L						E						N						T			

Teks kode dari teknik ini dengan membaca dari baris atas ke baris bawah

AGAAMXYSNBJRMNOPRAEAEAKAAKUESDLENTX

2. Segitiga: masukkan teks asli dengan pola segitiga dan dibaca dari atas ke bawah:

					S					
				A	Y	A				
			B	E	L	A	J			
		R	K	E	A	M	A	N		
	A	N	K	O	M	P	U	T	E	
R	X	X	X	X	X	X	X	X	X	X

Teks kodenya adalah:

RAXRNXBKKXAEEOXSYLAMXAAMPXJAUXNTXEXX

3. Spiral: teks asli dimasukkan secara spiral dan dapat dibaca dari atas ke bawah. Lihat contoh di bawah ini:

S	A	Y	A	S	E
A	M	A	N	A	D
E	E	R	X	N	A
K	T	X	X	K	N
R	U	P	M	O	G
A	J	A	L	E	B

Teks kodenya adalah:

SAEKRAAMETUJYARXPAANXXMLSANKOEEDANGB

4. Diagonal: Dengan menggunakan pola ini teks asli dimasukkan dengan cara diagonal. Coba perhatikan contoh di bawah ini:

S	D	L	E	N	T
A	A	A	A	K	E
Y	N	J	M	O	R
A	G	A	A	M	X
S	B	R	N	P	X
E	E	K	A	U	X

Teks kodenya adalah:

SDLENTAAAAKEYNJMORAGAAMXSBRNPXEEKAUX

Teknik transposisi (permutasi) memiliki bermacam-macam pola yang bisa digunakan untuk menyembunyikan pesan dari tangan orang-orang yang tidak berhak. Kombinasi tersebut merupakan dasar dari pembentukan algoritma kriptografi yang kita kenal sekarang ini (modern) (Ariyus, 2008:75-77).

2.5.6 Protokol Perjanjian Kunci

Protokol perjanjian kunci merupakan skema dalam kriptografi yang digunakan untuk mengatasi masalah perjanjian kunci rahasia. Kunci tersebut digunakan pada proses enkripsi dan dekripsi diantara dua pihak yang saling berkomunikasi. Tingkat keamanan dari protokol perjanjian kunci diletakkan pada tingkat kesulitan dari suatu permasalahan matematis dan bertujuan agar kedua belah pihak dapat menentukan kunci yang sama (Wicaksono, 2014).

Apabilah pengirim pesan dan penerima pesan menggunakan sistem kriptografi kunci rahasia, masalah utama yang muncul adalah keduanya harus menyepakati kunci yang sama, padahal keduanya tidak dapat bertemu secara langsung. Apabila pengirim pesan mengirim kunci kepada penerima pesan, maka penyadap dapat mengetahui kunci yang dikirimkan, hal ini dikarenakan proses pengiriman melalui jalur komunikasi yang tidak aman. Salah satu cara yang dapat digunakan untuk mengatasi masalah ini adalah menggunakan protokol perjanjian kunci (*key establishment protocol*). Protokol perjanjian kunci bertujuan agar kedua belah pihak dapat menentukan kunci yang sama walaupun dilakukan melalui jalur komunikasi yang tidak aman. Salah satu contoh protokol perjanjian

kunci yang paling sederhana adalah protol perjanjian kunci Diffie-Hillman yang dipublikasikan pada tahun 1976. Skema protokol perjanjian kunci Diffie-Hiellman disajikan pada tabel berikut:

Tabel 2.2 Protokol Perjanjian Kunci Diffie-Hellman (Myasnikov dkk, 2008:5)

Pengirim pesan atau penerima pesan mempublikasikan suatu grup siklik G dengan elemen pembangun $g \in G$.	
Pengirim pesan	Penerima pesan
1. Pengirim pesan memilih secara rahasia suatu bilangan bulat positif a 2. Pengirim pesan menghitung g^a 3. Pengirim pesan mengirim g^a kepada penerima pesan 4. Pengirim pesan menerima g^b dari penerima pesan 5. Pengirim pesan menghitung $K_1 = (g^b)^a = g^{ba}$	1. Penerima pesan memilih secara rahasia suatu bilangan bulat positif b 2. Penerima pesan menghitung g^b 3. Penerima pesan mengirim g^b kepada pengirim pesan 4. Penerima pesan menerima g^a dari pengirim pesan 5. Penerima pesan menghitung $K_2 = (g^a)^b = g^{ab}$
Pengirim pesan dan Penerima pesan telah menyepakati kunci rahasia $K = K_1 = K_2$	

Setiap grup siklik G merupakan grup komutatif, maka $ab = ba$, sehingga $K = K_1 = K_2$. Misalkan pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu K. Selanjutnya, kunci rahasia K yang telah disepakati digunakan untuk melakukan proses enkripsi-dekripsi. Di lain pihak, penyadap sebagai penyerang hanya dapat mengetahui nilai g, g^a dan g^b. Untuk mendapatkan kunci yang telah disepakati pengirim pesan dan peneima pesan, maka penyadap harus menentukan nilai a atau b. Dengan kata lain, penyadap harus menyelesaikan masalah logaritma diskrit pada G, yaitu menentukan nilai a apabila nilai g dan g^a diketahui. Tingkat keamanan dari protokol perjanjian kunci

Diffie-Hellman didasarkan pada masalah logaritma diskrit pada grup siklik (Myasnikov dkk, 2008:5-6).

Pada protokol perjanjian kunci Diffie-Hellman digunakan grup siklik yang merupakan grup komutatif. Akan tetapi, pada penelitian Stickel (2005) dalam Myasnikov dkk (2008) diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup tidak komutatif. Untuk dapat menggunakan grup tidak komutatif, protokol perjanjian kunci harus dapat dikonstruksi menggunakan suatu permasalahan matematis yang ada pada grup tidak komutatif. Skema protokol perjanjian kunci Stickel yang didasarkan atas grup tidak komutatif disajikan pada tabel berikut:

Tabel 2.3 Protokol Perjanjian Kunci Stickel

<table>
<tr><td colspan="2">Pengirim pesan atau penerima pesan mempublikasikan suatu grup tidak komutatif G dan $a, b \in G, ab \neq ba$, dengan R dan S berturut-turut adalah order dari a dan b.</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia bilangan asli $M < R$ dan $N < S$
2. Pengirim pesan menghitung $x = a^M b^N$
3. Pengirim pesan mengirim x kepada penerima pesan
4. Pengirim pesan menerima y dari penerima pesan
5. Pengirim pesan menghitung $K_1 = a^M y b^N$</td><td>1. Penerima pesan memilih secara rahasia bilangan asli $P < R$ dan $Q < S$
2. Penerima pesan menghitung $y = a^P b^Q$
3. Penerima pesan mengirim y kepada pengirim pesan
4. Penerima pesan menerima x dari pengirim pesan
5. Penerima pesan menghitung $K_2 = a^P x\, b^Q$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan telah menyepakati kunci rahasia yang sama yaitu
$K = K_1 = K_2$</td></tr>
</table>

M dan P merupakan sebarang bilangan asli kurang dari order a, N dan Q merupakan sebarang bilangan asli kurang dari order b. Sehingga dapat

ditunjukkan bahwa pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama, yaitu

$$K_1 = a^M y b^N = a^M a^P b^Q b^N = a^{M+P} b^{Q+N} = a^P a^M b^N b^Q = a^P x\, b^Q = K_2$$

Grup simetri S_n merupakan salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel. Penggunaan grup pada protokol Stickel ini dapat diperumum menjadi sebarang semigrup. Kunci tersebut yang digunakan pada proses enkripsi dan dekripsi. Proses enkripsi dan dekripsi bertujuan agar pesan yang dikirim tidak dibaca oleh orang yang tidak berhak menerimanya. Di dalam al-Quran juga menjelaskan tentang anjuran untuk menjaga pesan. Dengan kata lain, pesan adalah sebuah amanat yang harus disampaikan kepada penerimanya, seperti penggalan firman Allah Swt. dalam al-Quran surat an-Nisa'/4:58, yaitu:

إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat"(QS. an-Nisaa'/4:58).

Di dalam tafsir Ibnu Katsir disebutkan bahwa Allah Swt. memberitahukan bahwa Dia memerintahkan agar amanat-amanat itu disampaikan kepada yang berhak menerimanya. Di dalam hadits al-Hasan, dari samurah, disebutkan bahwa Rasulullah Saw. telah bersabda:

أَدِّ الأَ مَا نَةَ إِلَى مَنِ ائْتَمَنَكَ ،وَلاَ تَخُنْ مَنْ خَانَكَ

"Sampaikan amanat itu kepada orang yang mempercayaimu, dan janganlah kamu berkhianat terhadap orang yang berkhianat kepadamu."

Hadits riwayat Imam Ahmad dan semua pemilik kitab sunan. Makna hadits ini umum mencakup semua jenis amanat yang diharuskan bagi manusia untuk menyampaikannya.

Amanat tersebut antara lain yang menyangkut hak-hak Allah Swt. atas hamba-hamba-Nya, seperti salat, zakat, puasa, kifarat, semua jenis nazar dan lain sebagainya yang semisal yang dipercayakan kepada seseorang dan tiada seorang hamba pun yang dipercayakan kepada seseorang dan tidak seorang hamba pun yang memelihatnya. Juga termasuk pula hak-hak yang menyangkut hamba-hamba Allah sebagian dari mereka atas sebagian yang lain, seperti semua titipan dan lain-lainnya yang merupakan subjek titipan tanpa ada bukti yang menunjukkan ke arah itu. Maka Allah Swt. memerintahkan agar hal tersebut ditunaikan kepada yang berhak menerimanya. Barang siapa yang tidak melakukan hal tersebut di dunia, maka ia akan dituntut nanti di hari kiamat dan dihukum karenanya (ad-Dimasyqi, 2001:251-252).

Dan kadang amanah tersebut datang dari manusia itu sendiri. Sebagaimana yang tertera dalam al-Quran surat al-Baqarah/2:283, yaitu:

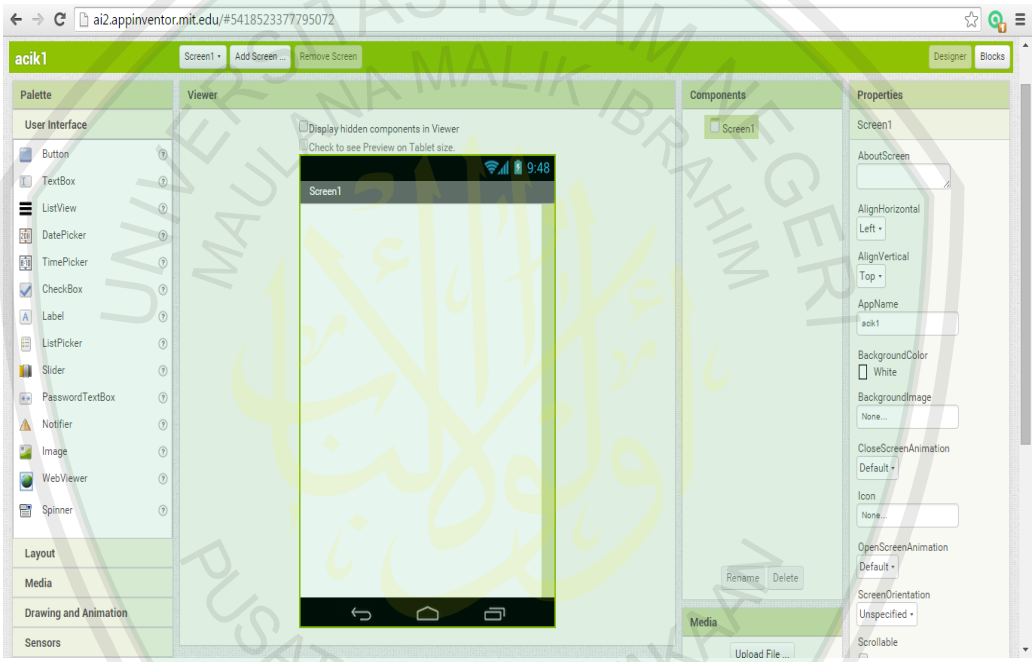
فَإِنۡ أَمِنَ بَعۡضُكُم بَعۡضٗا فَلۡيُؤَدِّ ٱلَّذِي ٱؤۡتُمِنَ أَمَٰنَتَهُۥ وَلۡيَتَّقِ ٱللَّهَ رَبَّهُۥ...

"... Jika sebagian kamu mempercayai sebagian yang lain, Maka hendaklah yang dipercayai itu menunaikan amanatnya (hutangnya) dan hendaklah ia bertakwa kepada Allah Tuhannya....." (QS. al-Baqarah/2:283)

2.6 Definisi App Inventor

App Inventor adalah suatu aplikasi berbasis *web* yang dibuat dan dikembangkan oleh *google*. Dirilis pada 15 Desember 2010, pada awalnya penelitian dilakukan oleh *google* dengan tujuan sebagai komputasi pendidikan

pada lingkungan pengembangan *online*. App Inventor berbentuk aplikasi *web* yang memungkinkan pengguna untuk membuat aplikasi yang hebat dan dapat digunakan di telepon selular berbasis *Android* dengan mengerti konsep programming tanpa harus menguasai bahasa pemprograman secara keseluruhan. *Android* adalah sistem operasi untuk telepon seluler yang berbasis *Linux* yang dikembangkan oleh *Android Inc* kemudian diakui oleh *Google Inc*. App Inventor dapat digambarkan sebagai berikut:



Gambar 2.6 Tampilan Aplikasi App Inventor

App Inventor merupakan aplikasi untuk membuat program yang terdiri dari dua bagian yaitu: *Design view* dan *Block Editor*. Membuat program dengan menggunakan App Inventor sangatlah seru karena kita mendesain sebuah program dengan cara menyusun *puzzle* atau *block-block* yang warna-warni. Untuk masuk ke dalam *Block Editor* tekan *blocks* yang berada pada sisi kanan atas. *Block* dalam App Inventor itu seperti sebuah *statement* atau instruksi yang berada dalam bahasa pemograman (Prasetiyo, 2014:1).

Design View terdiri dari lima komponen dasar:

1. *Palette*

Palette terdiri dari objek apa saja yang dapat digunakan ke dalam aplikasi. *Palette* terdiri dari beberapa grup semuanya dikembangkan ke dalam satu grup jika memiliki tema atau fungsi yang sama. Contohnya *User Interface* yang memiliki fungsi digunakan untuk mengatur interaksi aplikasi dengan si pengguna yang terdiri dari *button, check box, clock, image, label*, dan sebagainya.

2. *Viewer*

Terdiri dari tampilan *handphone* dan komponen-komponen yang dapat diklik. Di situ dapat dilihat komponen yang tidak dapat dilihat dengan *handphone*.

3. *Component*

Terdiri dari daftar komponen apa saja yang telah ditambahkan ke dalam projek baik secara terlihat maupun tidak terlihat dalam *handphone*. Tampilannya berupa susunan atau daftar untuk mengatur komponen atau melihat apa saja yang berbentuk seperti direktori.

4. Media

Kolom media terletak di bawah dari kolom *component*. Kolom ini digunakan untuk mengatur semua media komponen untuk mendukung aplikasi yang telah dibuat. Tipe media yang dapat ditambahkan ke dalam kolom media adalah gambar, *clip art*, musik, dan film. Pengguna juga dapat menambahkan media secara langsung ke dalam kolom *Propertiy*. Media yang ditambah ke dalam App Inventor diambil dari komputer dan di unggah ke dalam App Inventor. Semua media yang di tambahkan ke dalam aplikasi *Android* tidak boleh melebihi 5 MB.

5. *Properties*

Setiap komponen yang ditambah ke dalam projek, pengguna dapat mengatur komponen itu bagaimana dia berinteraksi dengan pengguna maupun dengan komponen lain, atau bagaimana tampilannya. Setiap komponen memiliki kolom *properties* yang berbeda-beda.

BAB III

PEMBAHASAN

Dalam bab pembahasan ini penulis akan menguraikan langkah-langkah tentang enkripsi dan dekripsi pesan menggunakan grup simetri-n untuk mengamankan informasi. Langkah awal yang dilakukan penulis yaitu menentukan unsur-unsur dari grup simetri S_n dan menentukan order dari masing-masing unsur tesebut, kemudian membentuk kunci menggunakan grup simetri S_n dan melakukan proses enkripsi dan dekripsi pesan. Untuk mempersempit masalah, pada pembahasan penulis hanya menggunakan grup simetri S_4 sampai dengan simetri S_7 dan simulasi proses pembentukan kunci, enkripsi dan dekripsi pesan menggunakan aplikasi App Inventor.

3.1 Grup Simetri S_n

Diberikan suatu himpunan tak kosong S, dengan $S = \{a_1, a_2, a_3, a_4, a_5, a_6, \dots, a_n\}$ dan misalkan S_n adalah himpunan yang memuat semua fungsi-fungsi bijektif dari S ke S. Himpunan S_n apabila dikenai operasi komposisi " $\circ$ " atau $(S_n, \circ)$ disebut grup simetri S_n. Grup simetri S_n memiliki unsur sebanyak $n!$, sehingga didapatkan unsur-unsur dari grup simetri S_n sebagai berikut:

$$\alpha_1 = (a_1)(a_2)(a_3)(a_4)(a_5)(a_6)(.)(.)(.)(a_n)$$

$$\alpha_2 = (a_1)(a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad \cdot \quad \cdot \quad \cdot \quad a_n)$$

$$\alpha_3 = (a_1)(a_2)(a_3 \quad a_4 \quad a_5 \quad a_6 \quad \cdot \quad \cdot \quad \cdot \quad a_n)$$

$$\alpha_4 = (a_1)(a_2)(a_3)(a_4 \quad a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_5 = (a_1)(a_2)(a_3)(a_4)(a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_6 = (a_1)(a_2)(a_3)(a_4)(a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_7 = (a_1)(a_2 \quad a_3)(a_4 \quad a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_8 = (a_1)(a_2)(a_3 \quad a_4)(a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_9 = (a_1)(a_2)(a_3)(a_4 \quad a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{10} = (a_1)(a_2 \quad a_3)(a_4 \quad a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{11} = (a_1)(a_2 \quad a_3 \quad a_4)(a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{12} = (a_1)(a_2)(a_3 \quad a_4 \quad a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{13} = (a_1)(a_2 \quad a_3 \quad a_4 \quad a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{14} = (a_1 \quad a_2)(a_3 \quad a_4 \quad a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{15} = (a_1 \quad a_2)(a_3 \quad a_4)(a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{16} = (a_1 \quad a_2)(a_3 \quad a_4 \quad a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{17} = (a_1 \quad a_2 \quad a_3)(a_4 \quad a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{18} = (a_1 \quad a_2 \quad a_3 \quad a_4)(a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{19} = (a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5)(a_6 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{20} = (a_1)(a_2 \quad a_3)(a_4 \quad a_5 \quad a_6)(a_7 \quad \cdot \cdot \cdot \quad a_n)$$

$$\alpha_{21} = (a_1 \quad a_2)(a_3 \quad a_4)(a_5 \quad a_6) \cdot \cdot \cdot (a_{n-1} \quad a_n)$$

$$\alpha_{22} = (a_1 \quad a_2 \quad a_3)(a_4 \quad a_5 \quad a_6) \cdot \cdot \cdot (a_{n-2} \quad a_{n-1} \quad a_n)$$

$$\vdots$$

$$\alpha_{n!} = (a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad \cdot \cdot \cdot \quad a_n)$$

3.1.1 Order dari Unsur-Unsur Grup Simetri S_n

Order dari unsur-unsur grup simetri S_n sebagai berikut:

$|\alpha_1| = 1$

$|\alpha_2| = [1, n-1]$

$|\alpha_3| = [1, 1, n-2]$

$|\alpha_4| = [1, 1, 1, n-3]$

$|\alpha_5| = [1, 1, 1, 1, n-4]$

$|\alpha_6| = [1, 1, 1, 1, 1, n-5]$

$|\alpha_7| = [1, 2, n-3]$

$|\alpha_8| = [1, 1, 2, n-4]$

$|\alpha_9| = [1, 1, 1, 2, n-5]$

$|\alpha_{10}| = [1, 2, 2, n-5]$

$|\alpha_{11}| = [1, 3, n-4]$

$|\alpha_{12}| = [1, 1, 3, n-5]$

$|\alpha_{13}| = [1, 4, n-5]$

$|\alpha_{14}| = [2, n-2]$

$|\alpha_{15}| = [2, 2, n-4]$

$|\alpha_{16}| = [2, 3, n-5]$

$|\alpha_{17}| = [3, n-3]$

$|\alpha_{18}| = [4, n-4]$

$|\alpha_{19}| = [5, n-5]$

$|\alpha_{20}| = [1, 2, 3, n-6]$

$|\alpha_{21}| = 2$

$|\alpha_{22}| = 3$

$\vdots$

$|\alpha_{n!}| = n$

3.1.2 Penerapan Grup Simetri S_n pada Proses Pembentukan Kunci

Misalkan pengirim pesan ingin mengirimkan pesan rahasia kepada penerima pesan menggunakan sistem kriptografi simetri dengan teknik transposisi (permutasi). Karena ada dua orang yang melakukan proses enkripsi dan dekripsi pesan menggunakan sistem kriptografi simetri maka akan terdapat sebanyak $\frac{1}{2}2(2-1) = 1$ kunci rahasia yang harus dipertukarkan secara aman.

Keamanan sistem kriptografi simetri terletak pada kerahasian kuncinya. Apabila pengirim pesan mengenkripsikan pesan menggunakan suatu kunci rahasia

sehingga menghasilkan *ciphertext*, maka pesan yang dikirim tidak bisa dibaca oleh penerima pesan, karena penerima pesan tidak mengetahui kunci yang digunakan. Penerima pesan tidak boleh mengirim kunci yang digunakan kepada penerima pesan karena ada menyadap yang ingin mengetahui pesan yang dikirim. Oleh karena itu pengirim pesan dan penerima pesan harus melakukan suatu perjanjian kunci rahasia. Pada penelitian Stickel (2005) dalam Myasnikov dkk (2008) diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup tidak komutatif. Grup simetri S_n merupakan salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel. Berdasarkan grup simetri S_n dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada tabel sebagai berikut:

Tabel 3.1 Protokol Perjanjian Kunci Stickel atas Grup Simetri S_n

<table>
<tr><td colspan="2">Pengirim pesan dan penerima pesan mempublikasikan suatu grup simetri S_n dan $\alpha_{n!}, \alpha_{22} \in S_n, \alpha_{n!} \circ \alpha_{22} \neq \alpha_{22} \circ \alpha_{n!}$
Pilih $\alpha_{n!} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{n-1} & a_n & a_1 \end{pmatrix}$ dan $\alpha_{22} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}$</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia bilangan asli M dan N
Pilih: $M = n-1$ dan $N = 2$
2. Pengirim pesan menghitung
$x = {\alpha_{n!}}^M \circ {\alpha_{22}}^N$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{n-1} & a_n & a_1 \end{pmatrix}^{n-1} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}^2$
$x = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_n & a_1 & a_2 & a_3 & a_4 & a_5 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \end{pmatrix} \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_1 & a_2 & a_6 & a_4 & a_5 & \cdots & a_n & a_{n-2} & a_{n-1} \end{pmatrix}$
$x = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_n & a_1 & a_5 & a_3 & a_4 & \cdots & a_{n-1} & a_{n-2} & a_{n-2} \end{pmatrix}$
3. Pengirim pesan mengirim x kepada penerima pesan
4. Pengirim pesan menerima y dari penerima pesan
5. Pengirim pesan menghitung
$K_1 = {\alpha_{n!}}^M \circ y \circ {\alpha_{22}}^N$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{n-1} & a_n & a_1 \end{pmatrix}^{n-1} \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_1 & a_2 & a_n & a_4 & a_5 & a_3 & \cdots & a_{n-2} & a_{n-1} & a_{n-2} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}^2$
$K_1 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_n & a_1 & a_2 & a_3 & a_4 & a_5 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_1 & a_2 & a_n & a_4 & a_5 & a_3 & \cdots & a_{n-2} & a_{n-1} & a_{n-2} \end{pmatrix} \right) \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_1 & a_2 & a_6 & a_4 & a_5 & \cdots & a_n & a_{n-2} & a_{n-1} \end{pmatrix}$
$K_1 = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_n & a_1 & a_{n-1} & a_2 & a_4 & a_3 & \cdots & a_{n-3} & a_{n-2} & a_{n-4} \end{pmatrix} \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_1 & a_2 & a_6 & a_4 & a_5 & \cdots & a_n & a_{n-2} & a_{n-1} \end{pmatrix}$
$K_1 = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_{n-1} & a_n & a_1 & a_2 & a_3 & a_4 & \cdots & a_{n-3} & a_{n-2} & a_{n-2} \end{pmatrix}$</td><td>1. Penerima pesan memilih secara rahasia bilangan asli P dan Q
Pilih: $P = n-1$ dan $Q = 1$
2. Penerima pesan menghitung
$y = {\alpha_{n!}}^P \circ {\alpha_{22}}^Q$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{n-1} & a_n & a_1 \end{pmatrix}^{n-1} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}^2$
$y = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_n & a_1 & a_2 & a_3 & a_4 & a_5 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \end{pmatrix} \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}$
$y = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_1 & a_2 & a_n & a_4 & a_5 & a_3 & \cdots & a_{n-2} & a_{n-1} & a_{n-2} \end{pmatrix}$
3. Penerima pesan mengirim y kepada pengirim pesan
4. Penerima pesan menerima x dari pengirim pesan
5. Penerima pesan menghitung
$K_2 = {\alpha_{n!}}^P \circ x \circ {\alpha_{22}}^Q$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{n-1} & a_n & a_1 \end{pmatrix}^{n-1} \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_n & a_1 & a_5 & a_3 & a_4 & \cdots & a_{n-1} & a_{n-2} & a_{n-2} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}^2$
$K_2 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_n & a_1 & a_2 & a_3 & a_4 & a_5 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_n & a_1 & a_5 & a_3 & a_4 & \cdots & a_{n-1} & a_{n-2} & a_{n-2} \end{pmatrix} \right) \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}$
$K_2 = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_1 & a_{n-1} & a_n & a_4 & a_2 & a_3 & \cdots & a_{n-2} & a_{n-4} & a_{n-2} \end{pmatrix} \circ \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}$
$K_2 = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & \cdots & u_{n-2} & u_{n-1} & u_n \\ a_{n-1} & a_n & a_1 & a_2 & a_3 & a_4 & \cdots & a_{n-4} & a_{n-3} & a_{n-2} \end{pmatrix}$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu
$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_{n-1} & a_n & a_1 & a_2 & a_3 & a_4 & \cdots & a_{n-4} & a_{n-3} & a_{n-2} \end{pmatrix}$</td></tr>
</table>

Berdasarkan grup simetri S_n diperoleh:

$$K_1 = {a_{n!}}^M \circ y \circ {a_{22}}^N$$

$$= {a_{n!}}^M \circ {a_{n!}}^P \circ {a_{22}}^Q \circ {a_{22}}^N$$

$$= {a_{n!}}^{M+P} \circ {a_{22}}^{Q+N}$$

$$= a_{n!}{}^{P} \circ a_{n!}{}^{M} \circ a_{22}{}^{N} \circ a_{22}{}^{Q}$$

$$= a_{n!}{}^{P} \circ x \circ a_{22}{}^{Q}$$

$$= K_2$$

Oleh karena itu pengirim pesan dan penerima pesan telah berhasil menyepakati kunci yang sama, yaitu $K = K_1 = K_2$.

3.2 Penerapan Grup Simetri S_4 pada Proses Pembentukan Kunci

Berdasarkan grup simetri S_4 dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada tabel sebagai berikut:

Tabel 3.2 Protokol Perjanjian Kunci Stickel atas Grup Simetri S_4

<table>
<tr><td colspan="2">Pengirim pesan dan penerima pesan mempublikasikan suatu grup simetri S_4 dan $\alpha_1, \alpha_2 \in S_4$
Pilih $\alpha_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}$ dan $\alpha_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}$</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia bilangan asli M dan N
Pilih: $M = 3$ dan $N = 2$
2. Pengirim pesan menghitung
$z = \alpha_1^M \cdot \alpha_2^N$
$z = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}^3 \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}^2$
$z = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_2 & a_3 \end{pmatrix}$
$z = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_1 & a_2 \end{pmatrix}$
3. Pengirim pesan mengirim x kepada penerima pesan
4. Pengirim pesan menerima y dari penerima pesan
5. Pengirim pesan menghitung
$K_1 = \alpha_1^M \cdot y \cdot \alpha_2^N$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}^3 \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_1 & a_2 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}^2$
$K_1 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_1 & a_2 \end{pmatrix} \right) \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_2 & a_3 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_1 & a_2 & a_4 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_2 & a_3 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$</td><td>1. Penerima pesan memilih secara rahasia bilangan asli P dan Q
Pilih: $P = 3$ dan $Q = 1$
2. Penerima pesan menghitung
$y = \alpha_1^P \cdot \alpha_2^Q$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}^3 \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}^1$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_3 & a_2 \end{pmatrix}$
3. Penerima pesan mengirim y kepada pengirim pesan
4. Penerima pesan menerima x dari pengirim pesan
5. Penerima pesan menghitung
$K_2 = \alpha_1^P \cdot x \cdot \alpha_2^Q$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}^3 \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_1 & a_2 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}^1$
$K_2 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_1 & a_2 \end{pmatrix} \right) \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_1 & a_4 & a_2 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_4 & a_2 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu
$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$</td></tr>
</table>

3.2.1 Implementasi Algoritma atas Grup Simetri S_4 untuk Pengamanan Pesan

a. Proses Enkripsi

Plaintext yang ditulis yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

Kemudian *plaintext* dienkripsikan terlebih dahulu oleh pengirim pesan dengan menggunakan kunci yang sudah disepakati yaitu:

$$K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$$

Karena kunci yang digunakan adalah bentuk permutasi P_4, maka *plaintext* dibagi menjadi blok-blok yang terdiri dari 4 huruf. Jika dalam blok ada huruf yang kurang maka dapat ditambah dengan huruf yang disukai, misal $ dan spasi dilambangkan dengan #, sehingga diperoleh blok-blok sebagai berikut:

KESA	BARA	N#AD	ALAH
#OBA	T#TE	RBAI	K#DA
RI#S	EGAL	A#KE	SULI
TAN$			

Proses enkripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \mathrm{K} & \mathrm{E} & \mathrm{S} & \mathrm{A} \\ a_3 & a_4 & a_1 & a_2 \\ \mathrm{S} & \mathrm{A} & \mathrm{K} & \mathrm{E} \end{pmatrix} =$ SAKE

Blok II : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{B} & \text{A} & \text{R} & \text{A} \\ a_3 & a_4 & a_1 & a_2 \\ \text{R} & \text{A} & \text{B} & \text{A} \end{pmatrix} =$ RABA

Blok III : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{N} & \# & \text{A} & \text{D} \\ a_3 & a_4 & a_1 & a_2 \\ \text{A} & \text{D} & \text{N} & \# \end{pmatrix} =$ ADN#

Blok IV : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{A} & \text{L} & \text{A} & \text{H} \\ a_3 & a_4 & a_1 & a_2 \\ \text{A} & \text{H} & \text{A} & \text{L} \end{pmatrix} =$ AHAL

Blok V : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \# & \text{O} & \text{B} & \text{A} \\ a_3 & a_4 & a_1 & a_2 \\ \text{B} & \text{A} & \# & \text{O} \end{pmatrix} =$ BA#O

Blok VI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{T} & \# & \text{T} & \text{E} \\ a_3 & a_4 & a_1 & a_2 \\ \text{T} & \text{E} & \text{T} & \# \end{pmatrix} =$ TET#

Blok VII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{R} & \text{B} & \text{A} & \text{I} \\ a_3 & a_4 & a_1 & a_2 \\ \text{A} & \text{I} & \text{R} & \text{B} \end{pmatrix} =$ AIRB

Blok VIII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{K} & \# & \text{D} & \text{A} \\ a_3 & a_4 & a_1 & a_2 \\ \text{D} & \text{A} & \text{K} & \# \end{pmatrix} =$ DAK#

Blok IX : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{R} & \text{I} & \# & \text{S} \\ a_3 & a_4 & a_1 & a_2 \\ \# & \text{S} & \text{R} & \text{I} \end{pmatrix} =$ #SRI

Blok X : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{E} & \text{G} & \text{A} & \text{L} \\ a_3 & a_4 & a_1 & a_2 \\ \text{A} & \text{L} & \text{E} & \text{G} \end{pmatrix} =$ ALEG

Blok XI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{A} & \# & \text{K} & \text{E} \\ a_3 & a_4 & a_1 & a_2 \\ \text{K} & \text{E} & \text{A} & \# \end{pmatrix} =$ KEA#

Blok XII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ S & U & L & I \\ a_3 & a_4 & a_1 & a_2 \\ L & I & S & U \end{pmatrix} =$ LISU

Blok XIII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ T & A & N & \$ \\ a_3 & a_4 & a_1 & a_2 \\ N & \$ & T & A \end{pmatrix} =$ N$TA

Dari proses enkripsi di atas diperoleh *ciphertext* yang akan dikirim kepada penerima pesan yaitu:

SAKERABAADN#AHALBA#OTET#AIRBDAK##S
RIALEGKEA#LISUN$TA

b. Proses Dekripsi

Proses selanjutnya adalah proses dekripsi. C*iphertext* yang diterima yaitu:

SAKERABAADN#AHALBA#OTET#AIRBDAK##S
RIALEGKEA#LISUN$TA

Pada proses ini penerima pesan mendeskripsikan *ciphertext* dengan menginverskan kunci yang telah disepakati yaitu:

$$K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$$

C*iphertext* terlebih dahulu diubah menjadi blok-blok yang terdiri dari 4 huruf sehingga diperoleh blok-blok sebagai berikut:

SAKE	RABA	ADN#	AHAL
BA#O	TET#	AIRB	DAK#
#SRI	ALEG	KEA#	LISU

N$TA

Proses dekripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ S & A & K & E \\ a_3 & a_4 & a_1 & a_2 \\ K & E & S & A \end{pmatrix} =$ KESA

Blok II : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ R & A & B & A \\ a_3 & a_4 & a_1 & a_2 \\ B & A & R & A \end{pmatrix} =$ BARA

Blok III : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ A & D & N & \# \\ a_3 & a_4 & a_1 & a_2 \\ N & \# & A & D \end{pmatrix} =$ N#AD

Blok IV : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ A & H & A & L \\ a_3 & a_4 & a_1 & a_2 \\ A & L & A & H \end{pmatrix} =$ ALAH

Blok V : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ B & A & \# & O \\ a_3 & a_4 & a_1 & a_2 \\ \# & O & B & A \end{pmatrix} =$ #OBA

Blok VI : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ T & E & T & \# \\ a_3 & a_4 & a_1 & a_2 \\ T & \# & T & E \end{pmatrix} =$ T#TE

Blok VII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ A & I & R & B \\ a_3 & a_4 & a_1 & a_2 \\ R & B & A & I \end{pmatrix} =$ RBAI

Blok VIII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ D & A & K & \# \\ a_3 & a_4 & a_1 & a_2 \\ K & \# & D & A \end{pmatrix} =$ K#DA

Blok IX : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \# & S & R & I \\ a_3 & a_4 & a_1 & a_2 \\ R & I & \# & S \end{pmatrix} =$ RI#S

LAJ

LAJ

LAJ

Blok X : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{A} & \text{L} & \text{E} & \text{G} \\ a_3 & a_4 & a_1 & a_2 \\ \text{E} & \text{G} & \text{A} & \text{L} \end{pmatrix} =$ EGAL

Blok XI : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{K} & \text{E} & \text{A} & \# \\ a_3 & a_4 & a_1 & a_2 \\ \text{A} & \# & \text{K} & \text{E} \end{pmatrix} =$ A#KE

Blok XII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{L} & \text{I} & \text{S} & \text{U} \\ a_3 & a_4 & a_1 & a_2 \\ \text{S} & \text{U} & \text{L} & \text{I} \end{pmatrix} =$ SULI

Blok XIII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \text{N} & \$ & \text{T} & \text{A} \\ a_3 & a_4 & a_1 & a_2 \\ \text{T} & \text{A} & \text{N} & \$ \end{pmatrix} =$ TAN$

Dari proses dekripsi di atas diperoleh pesan *plaintext* yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

3.3 Penerapan Grup Simetri S_5 pada Proses Pembentukan Kunci

Berdasarkan grup simetri S_5 dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada tabel sebagai berikut:

Tabel 3.3 Protokol Perjanjian Kunci Stickel atas Grup Simetri S_5

<table>
<tr><td colspan="2">Pengirim pesan dan penerima pesan mempublikasikan suatu grup simetri S_5
dan $\alpha_1, \alpha_2 \in S_5$
Pilih $\alpha_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix}$ dan $\alpha_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}$</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia bilangan asli M dan N. Pilih: $M = 4$ dan $N = 2$
2. Pengirim pesan menghitung
$x = {\alpha_1}^M \circ {\alpha_2}^N$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix}^4 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}^2$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_3 & a_5 & a_3 & a_4 \end{pmatrix}$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_4 & a_3 & a_3 \end{pmatrix}$
3. Pengirim pesan mengirim x kepada penerima pesan
4. Pengirim pesan menerima y dari penerima pesan
5. Pengirim pesan menghitung
$K_1 = {\alpha_1}^M \circ y \circ {\alpha_2}^N$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix}^4 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_4 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}^2$
$K_1 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_4 & a_3 \end{pmatrix} \right) \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_5 & a_3 & a_4 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_3 & a_3 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_5 & a_3 & a_4 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_3 & a_3 \end{pmatrix}$</td><td>1. Penerima pesan memilih secara rahasia bilangan asli P dan Q. Pilih: $P = 4$ dan $Q = 1$
2. Penerima pesan menghitung
$y = {\alpha_1}^P \circ {\alpha_2}^Q$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix}^4 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}^1$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_4 & a_3 \end{pmatrix}$
3. Penerima pesan mengirim y kepada pengirim pesan
4. Penerima pesan menerima x dari pengirim pesan
5. Penerima pesan menghitung
$K_2 = {\alpha_1}^P \circ y \circ {\alpha_2}^Q$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix}^4 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_4 & a_3 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}^1$
$K_2 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_3 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_4 & a_3 & a_3 \end{pmatrix} \right) \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_4 & a_5 & a_3 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_3 & a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_3 & a_4 & a_5 & a_3 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_3 & a_3 \end{pmatrix}$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu
$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_3 & a_3 \end{pmatrix}$</td></tr>
</table>

3.3.1 Implementasi Algoritma atas Grup Simetri S_5 untuk Pengamanan Pesan

a. Proses Enkripsi

Plaintext yang ditulis yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

Kunci yang digunakan yaitu:

$$K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix}$$

Kemudian *plaintext* dienkripsikan terlebih dahulu oleh pengirim pesan. Karena kunci yang digunakan adalah bentuk permutasi P_5, maka *plaintext* dibagi menjadi blok-blok yang terdiri dari 5 huruf. Jika dalam blok ada huruf yang kurang maka dapat ditambah dengan huruf yang disukai, misal $ dan spasi dilambangkan dengan #. Sehingga diperoleh blok-blok sebagai berikut:

KESAB	ARAN#	ADALA	H#OBA
T#TER	BAIK#	DARI#	SEGAL
A#KES	ULITA	N$$$$	

Proses enkripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{K} & \text{E} & \text{S} & \text{A} & \text{B} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{A} & \text{B} & \text{K} & \text{E} & \text{S} \end{pmatrix}$

$=$ ABKES

Blok II : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \text{R} & \text{A} & \text{N} & \# \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{N} & \# & \text{A} & \text{R} & \text{A} \end{pmatrix}$

$=$ N#ARA

Blok III : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \text{D} & \text{A} & \text{L} & \text{A} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{L} & \text{A} & \text{A} & \text{D} & \text{A} \end{pmatrix}$

$=$ LAADA

Blok IV : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{H} & \# & \text{O} & \text{B} & \text{A} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{B} & \text{A} & \text{H} & \# & \text{O} \end{pmatrix}$

$=$ BAH#O

Blok V : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{T} & \# & \text{T} & \text{E} & \text{R} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{E} & \text{R} & \text{T} & \# & \text{T} \end{pmatrix}$

$=$ ERT#T

Blok VI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{B} & \text{A} & \text{I} & \text{K} & \# \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{K} & \# & \text{B} & \text{A} & \text{I} \end{pmatrix}$

$=$ K#BAI

Blok VII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{D} & \text{A} & \text{R} & \text{I} & \# \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{I} & \# & \text{D} & \text{A} & \text{R} \end{pmatrix}$

$=$ I#DAR

Blok VIII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{S} & \text{E} & \text{G} & \text{A} & \text{L} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{A} & \text{L} & \text{S} & \text{E} & \text{G} \end{pmatrix}$

$=$ ALSEG

Blok IX : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \# & \text{K} & \text{E} & \text{S} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{E} & \text{S} & \text{A} & \# & \text{K} \end{pmatrix}$

$=$ ESA#K

Blok X : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{U} & \text{L} & \text{I} & \text{T} & \text{A} \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \text{T} & \text{A} & \text{U} & \text{L} & \text{I} \end{pmatrix}$

$=$ TAULI

Blok XI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{N} & \$ & \$ & \$ & \$ \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ \$ & \$ & \text{N} & \$ & \$ \end{pmatrix}$

$=$ $$N$$

Dari proses enkripsi di atas diperoleh *ciphertext* yang akan dikirim kepada penerima pesan yaitu:

ABKESN#ARALAADABAH#OERT#TK#BAII#DAR

ALSEGESA#KTAULI$$N$$

b. Proses Dekripsi

Proses selanjutnya adalah proses dekripsi. *Ciphertext* yang diterima yaitu:

ABKESN#ARALAADABAH#OERT#TK#BAII#DAR

ALSEGESA#KTAULI$$N$$

Pada proses ini penerima pesan mendeskripsikan *ciphertext* dengan menginverskan kunci yang telah disepakati yaitu:

$$K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix}$$

Ciphertext terlebih dahulu diubah menjadi blok-blok yang terdiri dari 5 huruf sehingga diperoleh sebagai berikut:

ABKES	N#ARA	LAADA	BAH#O
ERT#T	K#BAI	I#DAR	ALSEG
ESA#K	TAULI	$$N$$	

Proses dekripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \text{B} & \text{K} & \text{E} & \text{S} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{K} & \text{E} & \text{S} & \text{A} & \text{B} \end{pmatrix}$

$=$ KESAB

Blok II : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{N} & \# & \text{A} & \text{R} & \text{A} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{A} & \text{R} & \text{A} & \text{N} & \# \end{pmatrix}$

$=$ ARAN#

Blok III : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{L} & \text{A} & \text{A} & \text{D} & \text{A} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{A} & \text{D} & \text{A} & \text{L} & \text{A} \end{pmatrix}$

$=$ ADALA

Blok IV : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{B} & \text{A} & \text{H} & \# & \text{O} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{H} & \# & \text{O} & \text{B} & \text{A} \end{pmatrix}$

$=$ H#OBA

Blok V : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{E} & \text{R} & \text{T} & \# & \text{T} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{T} & \# & \text{T} & \text{E} & \text{R} \end{pmatrix}$

$$= \boxed{\text{T\#TER}}$$

Blok VI : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{K} & \# & \text{B} & \text{A} & \text{I} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{B} & \text{A} & \text{I} & \text{K} & \# \end{pmatrix}$

$$= \boxed{\text{BAIK\#}}$$

Blok VII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{I} & \# & \text{D} & \text{A} & \text{R} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{D} & \text{A} & \text{R} & \text{I} & \# \end{pmatrix}$

$$= \boxed{\text{DARI\#}}$$

Blok VIII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \text{L} & \text{S} & \text{E} & \text{G} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{S} & \text{E} & \text{G} & \text{A} & \text{L} \end{pmatrix}$

$$= \boxed{\text{SEGAL}}$$

Blok IX : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{E} & \text{S} & \text{A} & \# & \text{K} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{A} & \# & \text{K} & \text{E} & \text{S} \end{pmatrix}$

$$= \boxed{\text{A\#KES}}$$

Blok X : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{T} & \text{A} & \text{U} & \text{L} & \text{I} \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{U} & \text{L} & \text{I} & \text{T} & \text{A} \end{pmatrix}$

$$= \boxed{\text{ULITA}}$$

Blok XI : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \$ & \$ & \text{N} & \$ & \$ \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ \text{N} & \$ & \$ & \$ & \$ \end{pmatrix}$

$$= \boxed{\text{N\$\$\$\$}}$$

Dari proses dekripsi di atas diperoleh *plaintext* yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

3.4 Penerapan Grup Simetri S_6 pada Proses Pembentukan Kunci

Berdasarkan grup simetri S_6 dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada tabel sebagai berikut:

Tabel 3.4 Protokol Perjanjian Kunci Stickel atas Grup Simetri S_6

<table>
<tr><td colspan="2">Pengirim pesan dan penerima pesan mempublikasikan suatu grup simetri S_6 dan $\alpha_1, \alpha_2 \in S_6$
Pilih $\alpha_5 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}$ dan $\alpha_9 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}$</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia bilangan asli M dan N. Pilih: $M = 5$ dan $N = 2$
2. Pengirim pesan menghitung
$x = \alpha_1^M \circ \alpha_2^N$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_6 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^2$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_6 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_1 & a_2 & a_6 & a_4 & a_5 \end{pmatrix}$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_4 & a_1 & a_5 & a_3 & a_6 \end{pmatrix}$
3. Pengirim pesan mengirim x kepada penerima pesan
4. Pengirim pesan menerima y dari penerima pesan
5. Pengirim pesan menghitung
$K_1 = \alpha_1^M \circ y \circ \alpha_2^N$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_6 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_2 & a_6 & a_4 & a_5 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^2$
$K_1 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_6 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_2 & a_6 & a_4 & a_5 & a_3 \end{pmatrix} \right) \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_1 & a_2 & a_6 & a_4 & a_5 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_6 & a_1 & a_5 & a_3 & a_4 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_1 & a_2 & a_6 & a_4 & a_5 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$</td><td>1. Penerima pesan memilih secara rahasia bilangan asli P dan Q. Pilih: $P = 5$ dan $Q = 1$
2. Penerima pesan menghitung
$y = \alpha_1^P \circ \alpha_2^Q$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_6 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^1$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_6 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_2 & a_6 & a_4 & a_5 & a_3 \end{pmatrix}$
3. Penerima pesan mengirim y kepada pengirim pesan
4. Penerima pesan menerima x dari pengirim pesan
5. Penerima pesan menghitung
$K_2 = \alpha_1^P \circ y \circ \alpha_2^Q$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_6 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_6 & a_1 & a_5 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^1$
$K_2 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_6 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_6 & a_1 & a_5 & a_3 & a_4 \end{pmatrix} \right) \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_4 & a_5 & a_6 & a_4 & a_2 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu
$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$</td></tr>
</table>

3.4.1 Implementasi Algoritma atas Grup Simetri S_6 untuk Pengamanan Pesan

a. Proses Enkripsi

Plaintext yang ditulis yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

Kunci yang digunakan yaitu:

$$K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

Kemudian *plaintext* dienkripsikan terlebih dahulu oleh pengirim pesan. Karena kunci yang digunakan adalah bentuk permutasi P_6, maka *plaintext* dibagi menjadi blok-blok yang terdiri dari 6 huruf. Jika dalam blok ada huruf yang kurang maka dapat ditambah dengan huruf yang disukai, misal $ dan spasi dilambangkan dengan #. Sehingga diperoleh blok-blok sebagai berikut:

KESABA	RAN#AD	ALAH#O	BAT#TE
RBAIK#	DARI#S	EGALA#	KESULI
TAN$$$			

Proses enkripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{K} & \text{E} & \text{S} & \text{A} & \text{B} & \text{A} \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \text{B} & \text{A} & \text{K} & \text{E} & \text{S} & \text{A} \end{pmatrix}$

$=$ BAKESA

Blok II : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{R} & \text{A} & \text{N} & \# & \text{A} & \text{D} \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \text{A} & \text{D} & \text{R} & \text{A} & \text{N} & \# \end{pmatrix}$

$=$ ADRAN#

Blok III : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{A} & \text{L} & \text{A} & \text{H} & \# & \text{O} \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \# & \text{O} & \text{A} & \text{L} & \text{A} & \text{H} \end{pmatrix}$

$=$ #OALAH

Blok IV : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{B} & \text{A} & \text{T} & \# & \text{T} & \text{E} \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \text{T} & \text{E} & \text{B} & \text{A} & \text{T} & \# \end{pmatrix}$

$=$ TEBAT#

Blok V : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{R} & \text{B} & \text{A} & \text{I} & \text{K} & \# \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \text{K} & \# & \text{R} & \text{B} & \text{A} & \text{I} \end{pmatrix}$

$=$ K#RBAI

Blok VI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{D} & \text{A} & \text{R} & \text{I} & \# & \text{S} \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \# & \text{S} & \text{D} & \text{A} & \text{R} & \text{I} \end{pmatrix}$

$=$ #SDARI

Blok VII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{E} & \text{G} & \text{A} & \text{L} & \text{A} & \# \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \text{A} & \# & \text{E} & \text{G} & \text{A} & \text{L} \end{pmatrix}$

$=$ A#EGAL

Blok VIII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{K} & \text{E} & \text{S} & \text{U} & \text{L} & \text{I} \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \text{L} & \text{I} & \text{K} & \text{E} & \text{S} & \text{U} \end{pmatrix}$

$=$ LIKESU

Blok IX: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{T} & \text{A} & \text{N} & \$ & \$ & \$ \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ \$ & \$ & \text{T} & \text{A} & \text{N} & \$ \end{pmatrix}$

$= \boxed{\$\$\text{TAN}\$}$

Dari proses enkripsi di atas diperoleh *ciphertext* yang akan dikirim kepada penerima pesan yaitu:

BAKESAADRAN##OALAHTEBAT#K#RBAI#SDA
RIA#EGALLIKESU$$TAN$

b. Proses Dekripsi

Proses selanjutnya adalah proses dekripsi. *Ciphertext* yang diterima yaitu:

BAKESAADRAN##OALAHTEBAT#K#RBAI#SDA
RIA#EGALLIKESU$$TAN$

Pada proses ini penerima pesan mendeskripsikan *ciphertext* dengan menginverskan kunci yang telah disepakati yaitu:

$$K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix}$$

Ciphertext terlebih dahulu diubah menjadi blok-blok yang terdiri dari 6 huruf sehingga diperoleh blok-blok sebagai berikut:

BAKESA	ADRAN#	#OALAH	TEBAT#
K#RBAI	#SDARI	A#EGAL	LIKESU
$$TAN$			

Proses dekripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ B & A & K & E & S & A \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ K & E & S & A & B & A \end{pmatrix}$

$=$ KESABA

Blok II : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ A & D & R & A & N & \# \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ R & A & N & \# & A & D \end{pmatrix}$

$=$ RAN#AD

Blok III : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \# & O & A & L & A & H \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ A & L & A & H & \# & O \end{pmatrix}$

$=$ ALAH#O

Blok IV : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ T & E & B & A & T & \# \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ B & A & T & \# & T & E \end{pmatrix}$

$=$ BAT#TE

Blok V : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ K & \# & R & B & A & I \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ R & B & A & I & K & \# \end{pmatrix}$

$=$ RBAIK#

Blok VI : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \# & S & D & A & R & I \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ D & A & R & I & \# & S \end{pmatrix}$

$=$ DARI#S

Blok VII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ A & \# & E & G & A & L \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ E & G & A & L & A & \# \end{pmatrix}$

$=$ EGALA#

Blok VIII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{L} & \text{I} & \text{K} & \text{E} & \text{S} & \text{U} \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ \text{K} & \text{E} & \text{S} & \text{U} & \text{L} & \text{I} \end{pmatrix}$

$=$ KESULI

Blok VIII : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ \text{\$} & \text{\$} & \text{T} & \text{A} & \text{N} & \text{\$} \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ \text{T} & \text{A} & \text{N} & \text{\$} & \text{\$} & \text{\$} \end{pmatrix}$

$=$ TAN$$$

Dari proses dekripsi di atas diperoleh pesan *plaintext* yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

3.5 Penerapan Grup Simetri S_7 pada Proses Pembentukan Kunci

Berdasarkan grup simetri S_7 dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada tabel sebagai berikut:

Tabel 3.5 Protokol Perjanjian Kunci Stickel atas Grup Simetri S_7

<table>
<tr><td colspan="2">Pengirim pesan dan penerima pesan mempublikasikan suatu grup simetri S_7 dan $\alpha_1, \alpha_2 \in S_7$
Pilih $\alpha_5 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \end{pmatrix}$ dan $\alpha_9 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}$</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia bilangan asli M dan N. Pilih: $M = 6$ dan $N = 2$
2. Pengirim pesan menghitung
$x = {\alpha_1}^M \circ {\alpha_2}^N$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \end{pmatrix}^6 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}^2$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_4 & a_2 & a_3 & a_7 & a_5 & a_6 \end{pmatrix}$
$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_3 & a_1 & a_2 & a_6 & a_4 & a_5 \end{pmatrix}$
3. Pengirim pesan mengirim x kepada penerima pesan
4. Pengirim pesan menerima y dari penerima pesan
5. Pengirim pesan menghitung
$K_1 = {\alpha_1}^M \circ y \circ {\alpha_2}^N$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \end{pmatrix}^6 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}^2$
$K_1 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix} \right) \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_4 & a_2 & a_3 & a_7 & a_5 & a_6 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_1 & a_2 & a_7 & a_4 & a_5 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_4 & a_2 & a_3 & a_7 & a_5 & a_6 \end{pmatrix}$
$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$</td><td>1. Penerima pesan memilih secara rahasia bilangan asli P dan Q. Pilih: $P = 6$ dan $Q = 1$
2. Penerima pesan menghitung
$y = {\alpha_1}^P \circ {\alpha_2}^Q$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \end{pmatrix}^6 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}^1$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}$
$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}$
3. Penerima pesan mengirim y kepada pengirim pesan
4. Penerima pesan menerima x dari pengirim pesan
5. Penerima pesan menghitung
$K_2 = {\alpha_1}^P \circ y \circ {\alpha_2}^Q$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \end{pmatrix}^6 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_3 & a_1 & a_2 & a_6 & a_4 & a_5 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}^2$
$K_2 = \left(\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_7 & a_3 & a_1 & a_2 & a_6 & a_4 & a_5 \end{pmatrix} \right) \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_2 & a_7 & a_1 & a_5 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_7 & a_5 \end{pmatrix}$
$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu
$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$</td></tr>
</table>

3.5.1 Implementasi Algoritma atas Grup Simetri S_7 untuk Pengamanan Pesan

a. Proses Enkripsi

Plaintext yang ditulis yaitu:

KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

Kunci yang digunakan yaitu:

$$K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$$

Kemudian *plaintext* dienkripsikan terlebih dahulu oleh pengirim pesan. Karena kunci yang digunakan adalah bentuk permutasi P_7, maka *plaintext* dibagi menjadi blok-blok yang terdiri dari 7 huruf. Jika dalam blok ada huruf yang kurang maka dapat ditambah dengan huruf yang disukai, misal $ dan spasi dilambangkan dengan #. Sehingga diperoleh blok-blok sebagai berikut:

KESABAR	AN#ADAL	AH#OBAT	#TERBAI
K#DARI#	SEGALA#	KESULIT	AN$$$$$

Proses enkripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \text{K} & \text{E} & \text{S} & \text{A} & \text{B} & \text{A} & \text{R} \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \text{R} & \text{K} & \text{E} & \text{S} & \text{A} & \text{B} \end{pmatrix}$

$=$ ARKESAB

Blok II : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \text{A} & \text{N} & \# & \text{A} & \text{D} & \text{A} & \text{L} \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ \text{A} & \text{L} & \text{A} & \text{N} & \# & \text{A} & \text{D} \end{pmatrix}$

$$= \boxed{\text{ALAN\#AD}}$$

Blok III : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ A & H & \# & O & B & A & T \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ A & T & A & H & \# & O & B \end{pmatrix}$

$$= \boxed{\text{ATAH\#OB}}$$

Blok IV : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \# & T & E & R & B & A & I \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ A & I & \# & T & E & R & B \end{pmatrix}$

$$= \boxed{\text{AI\#TERB}}$$

Blok V : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ K & \# & D & A & R & I & \# \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ I & \# & K & \# & D & A & R \end{pmatrix}$

$$= \boxed{\text{I\#K\#DAR}}$$

Blok VI : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ S & E & G & A & L & A & \# \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ A & \# & S & E & G & A & L \end{pmatrix}$

$$= \boxed{\text{A\#SEGAL}}$$

Blok VII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ K & E & S & U & L & I & T \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ I & T & K & E & S & U & L \end{pmatrix}$

$$= \boxed{\text{ITKESUL}}$$

Blok VIII : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ A & T & \$ & \$ & \$ & \$ & \$ \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ \$ & \$ & A & T & \$ & \$ & \$ \end{pmatrix}$

$$= \boxed{\text{\$\$AT\$\$\$}}$$

Dari proses enkripsi di atas diperoleh *ciphertext* yang akan dikirim kepada penerima pesan yaitu:

ARKESABALAN#ADATAH#OBAI#TERBI#K#DAR

A#SEGALITKESUL$$AT$$$

b. Proses Dekripsi

Proses selanjutnya adalah proses dekripsi. *Ciphertext* yang diterima yaitu:

ARKESABALAN#ADATAH#OBAI#TERBI#K#DAR A#SEGALITKESUL$$AT$$$

Pada proses ini penerima pesan mendeskripsikan *ciphertext* dengan menginverskan kunci yang telah disepakati yaitu:

$$K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix}$$

Ciphertext terlebih dahulu diubah menjadi blok-blok yang terdiri dari 7 huruf sehingga diperoleh sebagai berikut:

ARKESAB	ALAN#AD	ATAH#OB	AI#TERB
I#K#DAR	A#SEGAL	ITKESUL	$$AT$$$

Proses dekripsi dilakukan satu persatu dari blok tersebut:

Blok I : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ A & R & K & E & S & A & B \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ K & E & S & A & B & A & R \end{pmatrix}$

= KESABAR

Blok II : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ A & L & A & N & \# & A & D \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ A & N & \# & A & D & A & L \end{pmatrix}$

= AN#ADAL

Blok III : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ A & T & A & H & \# & O & B \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ A & H & \# & O & B & A & T \end{pmatrix}$

= AH#OBAT

Blok IV : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \text{A} & \text{I} & \# & \text{T} & \text{E} & \text{R} & \text{B} \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ \# & \text{T} & \text{E} & \text{R} & \text{B} & \text{A} & \text{I} \end{pmatrix}$

= #TERBAI

Blok V : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \text{I} & \# & \text{K} & \# & \text{D} & \text{A} & \text{R} \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ \text{K} & \# & \text{D} & \text{A} & \text{R} & \text{I} & \# \end{pmatrix}$

= K#DARI#

Blok VI : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \text{A} & \# & \text{S} & \text{E} & \text{G} & \text{A} & \text{L} \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ \text{S} & \text{E} & \text{G} & \text{A} & \text{L} & \text{A} & \# \end{pmatrix}$

= SEGALA#

Blok VII: $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \text{I} & \text{T} & \text{K} & \text{E} & \text{S} & \text{U} & \text{L} \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ \text{K} & \text{E} & \text{S} & \text{U} & \text{L} & \text{I} & \text{T} \end{pmatrix}$

= KESULIT

Blok VII: $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ \$ & \$ & \text{A} & \text{T} & \$ & \$ & \$ \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ \text{A} & \text{T} & \$ & \$ & \$ & \$ & \$ \end{pmatrix}$

= AT$$$$$

Dari proses dekripsi di atas diperoleh *plaintext* yaitu:

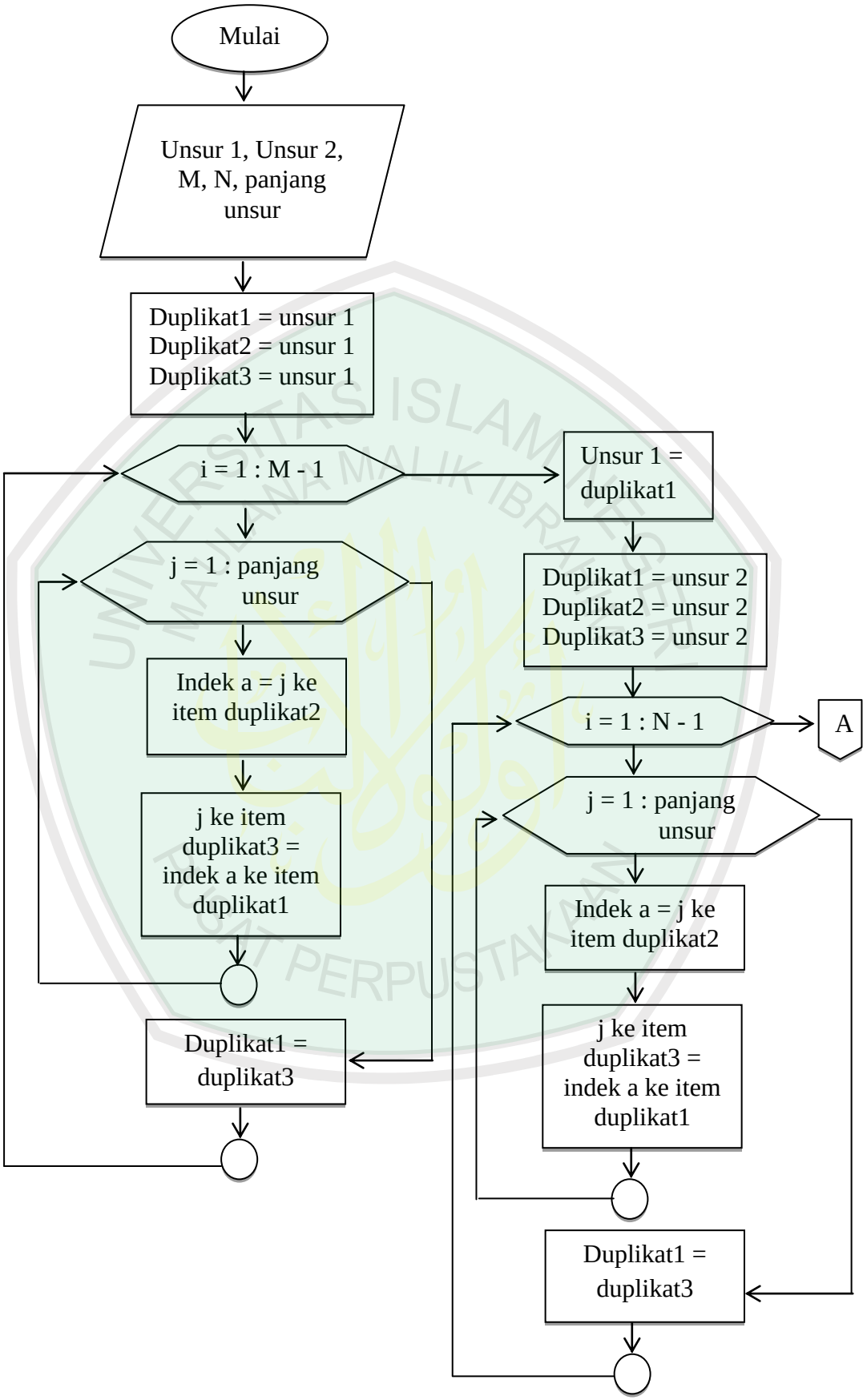
KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN

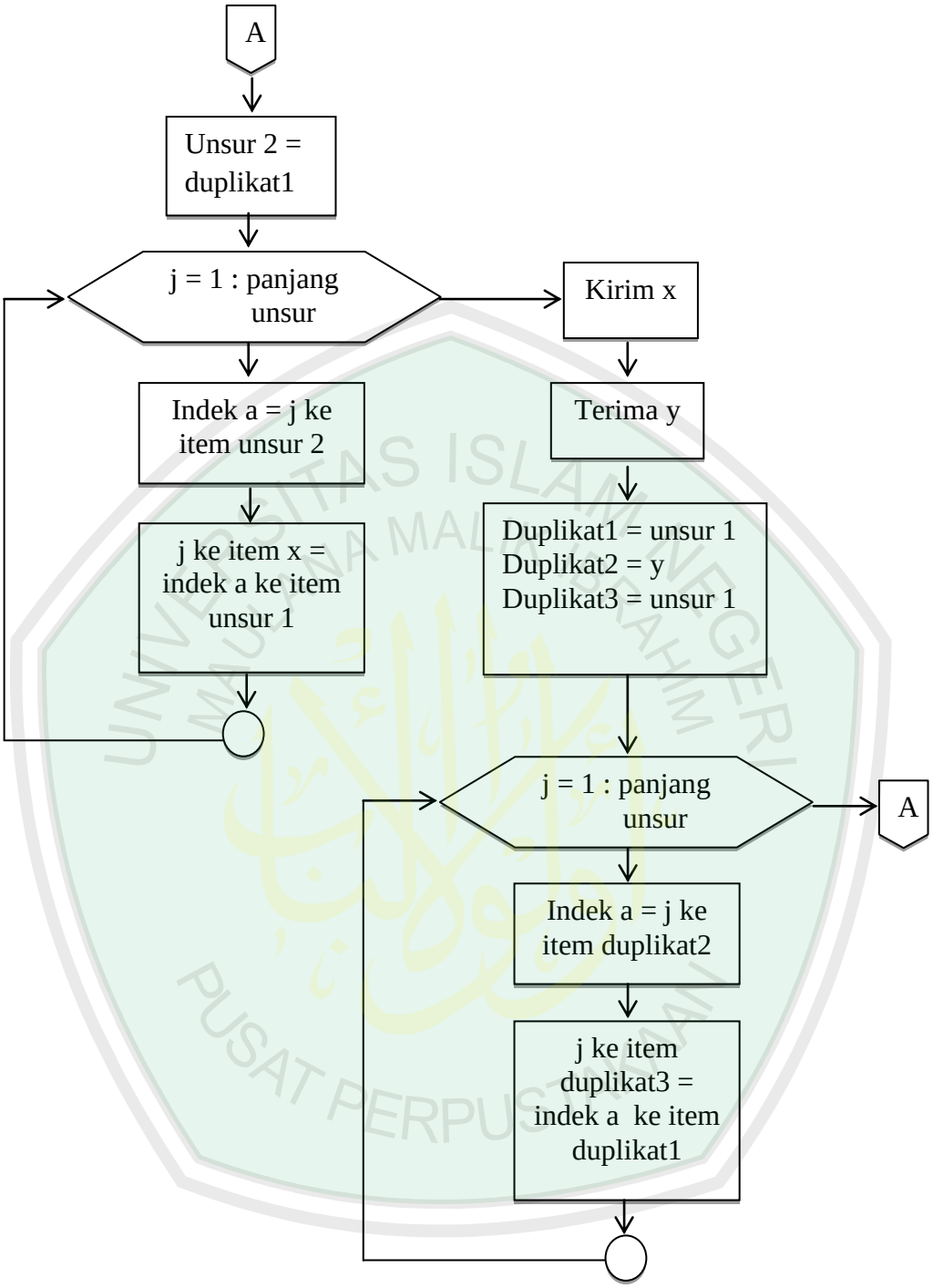
Dari proses enkripsi dan dekripsi di atas yaitu dengan menggunakan kunci yang bentuk permutasi P_4 dimana setiap blok ada 4 huruf, menggunakan kunci yang bentuk permutasi P_5 dimana setiap blok ada 5 huruf, menggunakan kunci

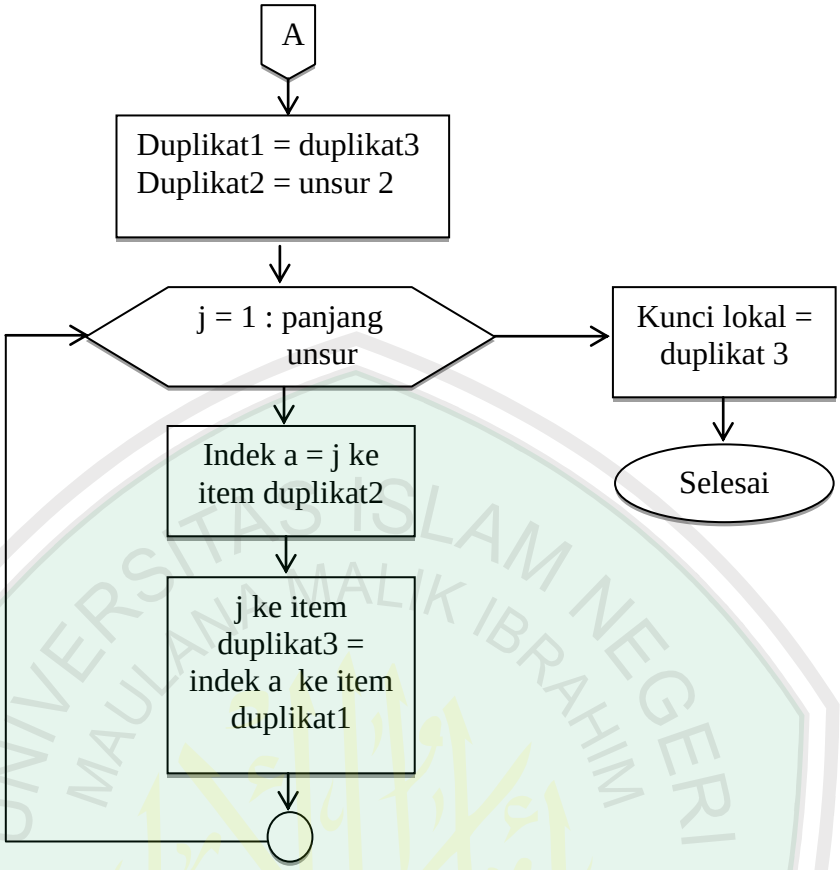
yang bentuk permutasi P_6 dimana setiap blok ada 6 huruf, dan menggunakan kunci yang bentuk permutasi P_7 dimana setiap blok ada 7 huruf, sehingga dapat disimpulkan bahwa dengan menggunakan kunci yang bentuk permutasinya lebih banyak maka peluang keamanan pesan yang dikirim lebih besar.

3.6 Simulasi Proses Pembentukan Kunci, Enkripsi, dan Dekripsi Pesan dengan App Inventor

Pada bab ini simulasi dilakukan dengan menggunakan aplikasi App Inventor. Sebelum membuat program terlebih dahulu dibuat *flowchart*, *flowchart* proses pembentukan kunci oleh pengirim pesan sebagai berikut:


Mulai
Unsur 1, Unsur 2, M, N, panjang unsur
Duplikat1 = unsur 1
Duplikat2 = unsur 1
Duplikat3 = unsur 1
i = 1 : M - 1
j = 1 : panjang unsur
Indek a = j ke item duplikat2
j ke item duplikat3 = indek a ke item duplikat1
Duplikat1 = duplikat3
Unsur 1 = duplikat1
Duplikat1 = unsur 2
Duplikat2 = unsur 2
Duplikat3 = unsur 2
i = 1 : N - 1
A
j = 1 : panjang unsur
Indek a = j ke item duplikat2
j ke item duplikat3 = indek a ke item duplikat1
Duplikat1 = duplikat3


A
Unsur 2 = duplikat1
j = 1 : panjang unsur
Kirim x
Indek a = j ke item unsur 2
Terima y
j ke item x = indek a ke item unsur 1
Duplikat1 = unsur 1
Duplikat2 = y
Duplikat3 = unsur 1
j = 1 : panjang unsur
A
Indek a = j ke item duplikat2
j ke item duplikat3 = indek a ke item duplikat1



Gambar 3.1 *Flowchart* Proses Pembentukan Kunci oleh Pengirim Pesan

Keterangan:

: Permulaan atau akhir program.

: Proses input atau output data, parameter dan informasi.

: Proses perhitungan atau proses pengolahan data.

: Proses inisialisasi atau pemberian harga awal.

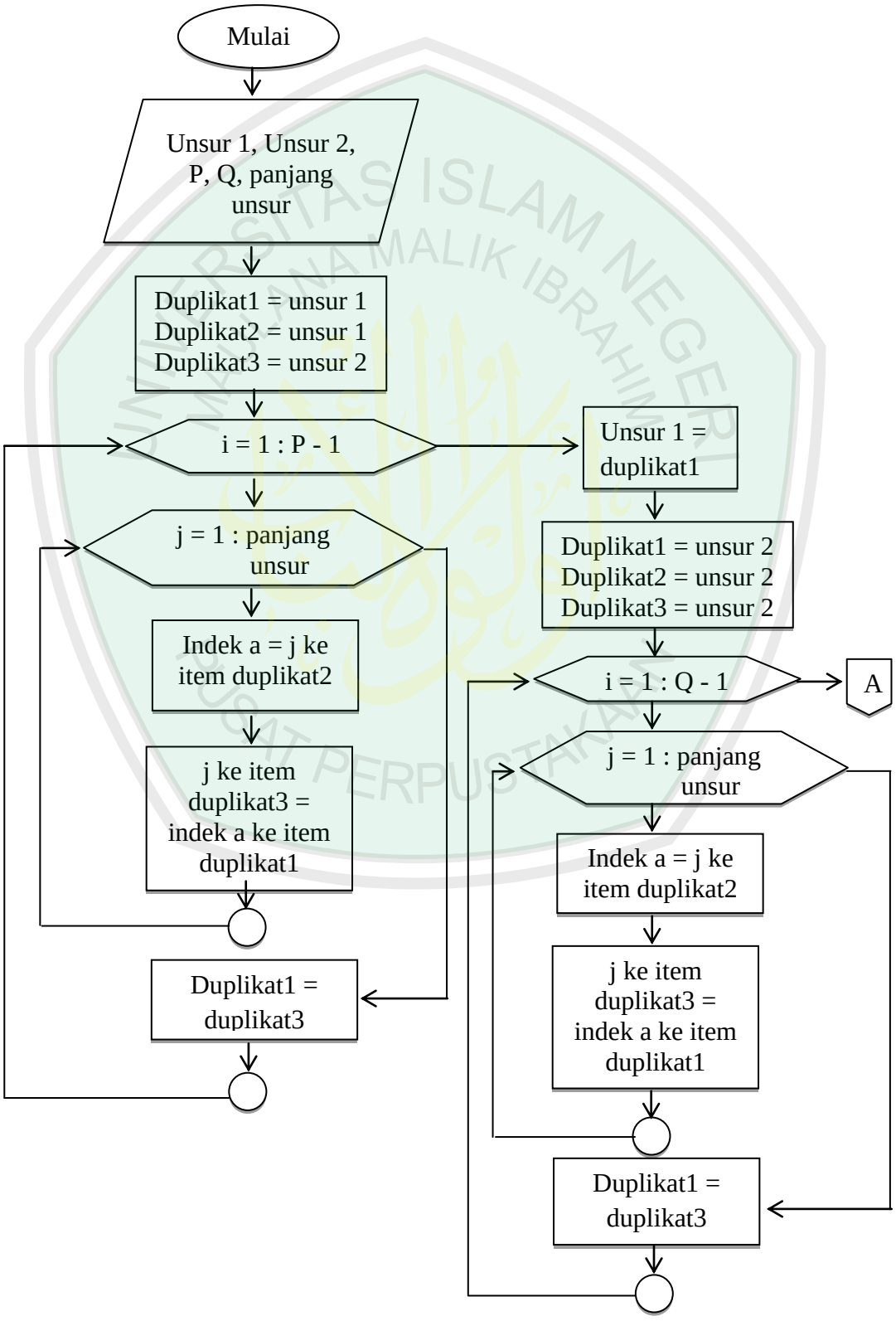
: Perbandingan pernyataan, penyeleksian data yang memberikan pilihan untuk langkah selanjutnya.

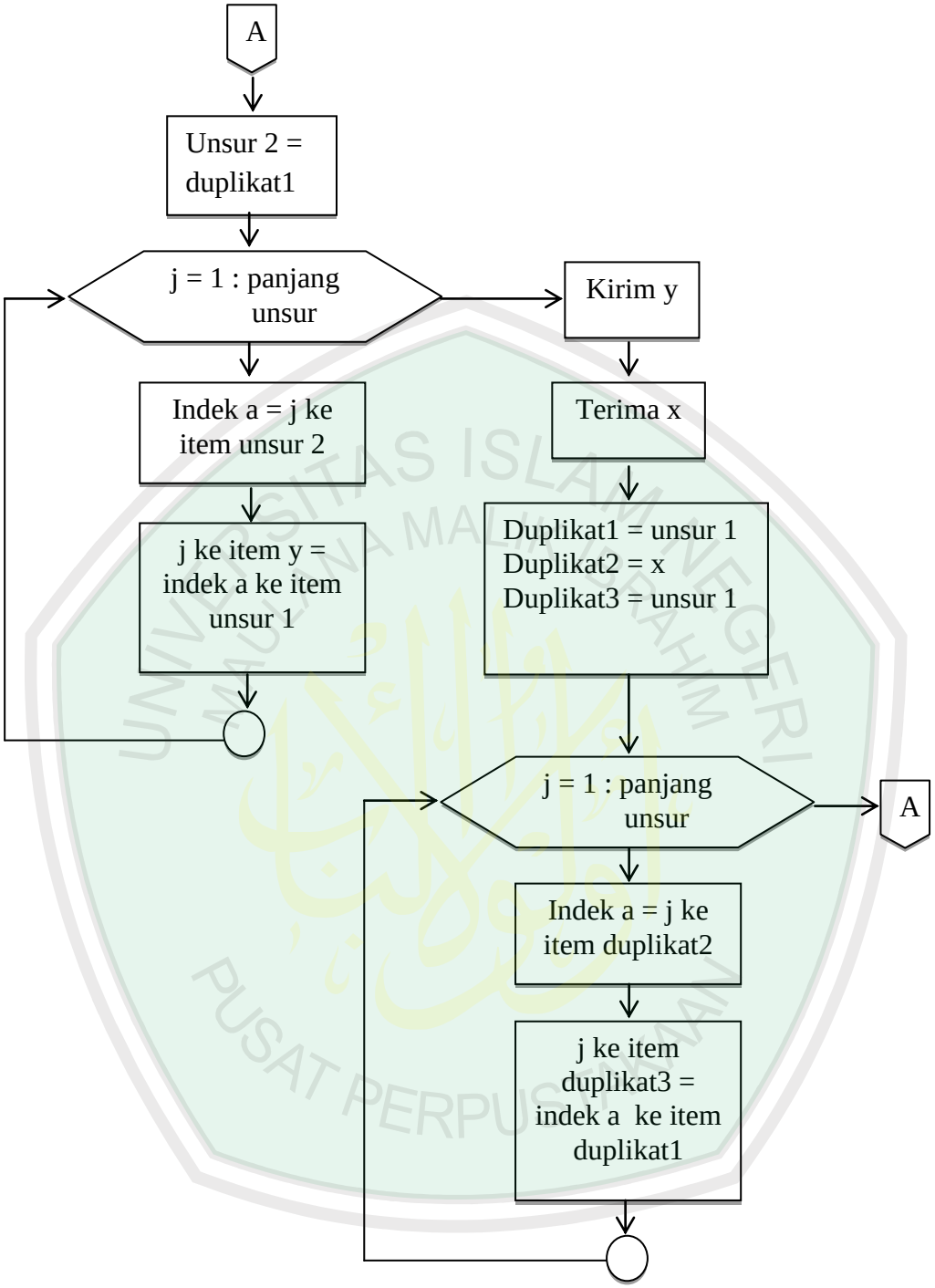
: Penghubung bagian-bagian flowchart yang berada pada satu halaman.

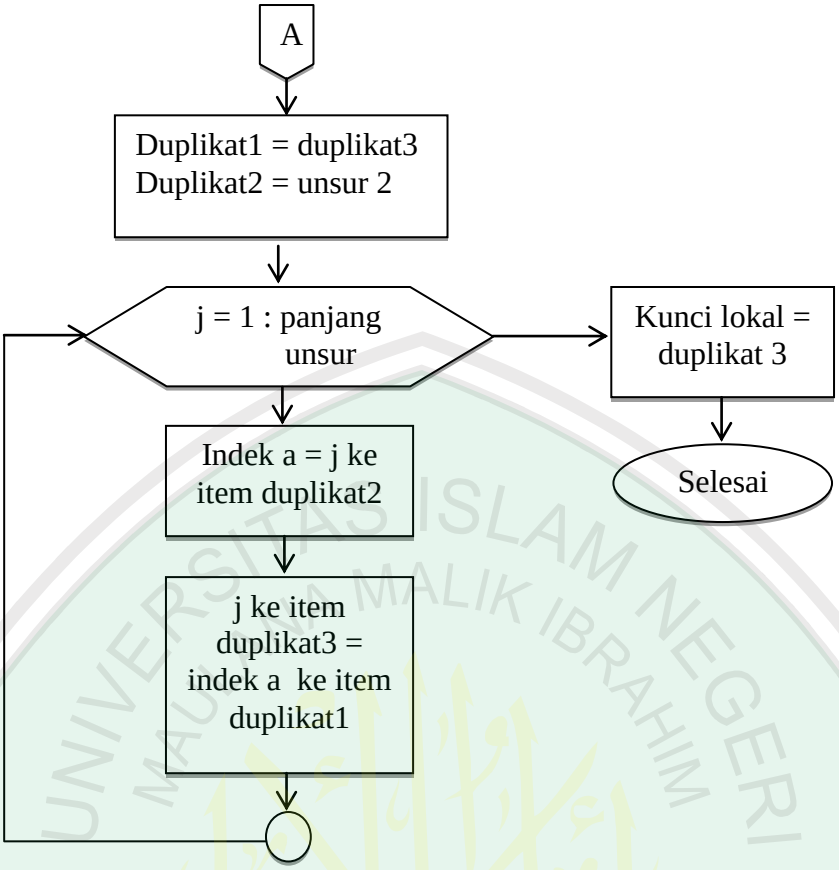
: Penghubung bagian-bagian flowchat yang berada pada halaman berbeda.

: Arah aliran program.

Flowchart proses pembentukan kunci oleh penerima pesan sebagai berikut:




A
Unsur 2 = duplikat1
j = 1 : panjang unsur
Kirim y
Indek a = j ke item unsur 2
Terima x
j ke item y = indek a ke item unsur 1
Duplikat1 = unsur 1
Duplikat2 = x
Duplikat3 = unsur 1
j = 1 : panjang unsur
A
Indek a = j ke item duplikat2
j ke item duplikat3 = indek a ke item duplikat1



Gambar 3.2 *Flowchart* Proses Pembentukan Kunci oleh Penerima Pesan

Form pembentukan kunci oleh pengirim pesan akan ditunjukkan pada Gambar 3.3 dan pembentukan kunci oleh penerima pesan akan ditunjukkan pada Gambar 3.4.

Gambar 3.3 *Form* Pembentukan Kunci oleh Pengirim Pesan

Gambar 3.4 *Form* Pembentukan Kunci oleh Penerima Pesan

Dari *form* di atas dapat dilakukan simulasi proses bentukan kunci sebagai berikut:

Tabel 3.6 Simulasi Proses Pembentukan Kunci

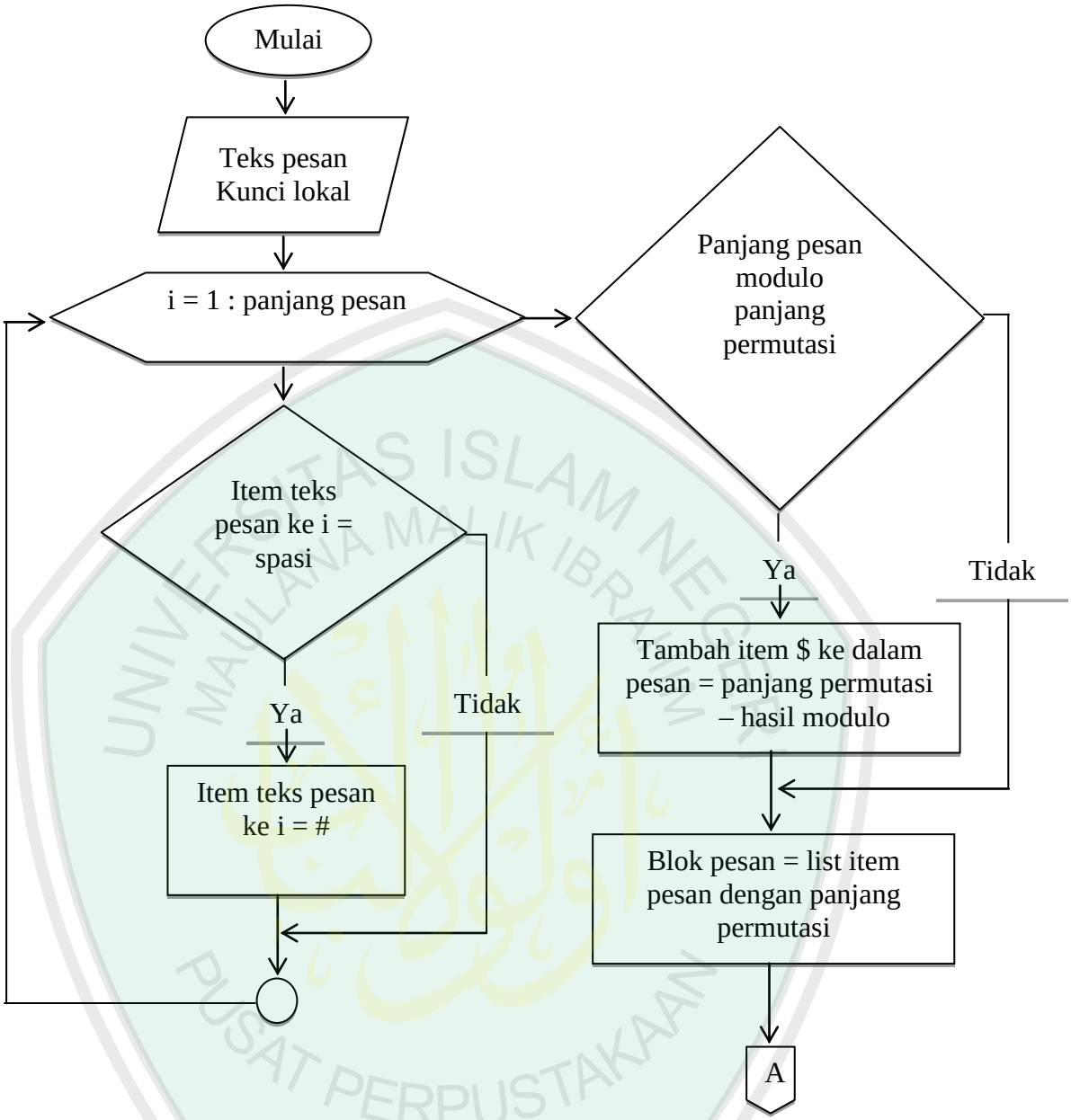
Pengirim pesan	Penerima pesan
1. Pengirim pesan memasukkan nomor HP yang dituju dikotak pertama atau dengan menekan tombol kontak untuk mencari nomor yang tersimpan dikontak. 2. Pengirim pesan memilih grup simetri yang akan digunakan, selanjutnya untuk mengirim grup simetri dengan menekan tombol ok. 3. Pengirim pesan menulis unsur grup simetri di kotak unsur 1, selanjutnya untuk mengirim unsur 1 dengan menekan tombol kirim unsur 1. 4. Pengirim pesan menerima unsur 2 dari penerima pesan. 5. Pengirim pesan menulis nilai M dan N. 6. Pengirim pesan menekan tombol generate x untuk menentukan nilai x, selanjutnya untuk mengirim nilai x dengan menekan tombol kirim x. 7. Pengirim pesan menerima y dari penerima pesan. 8. Pengirim pesan menekan tombol generate K_1.	1. Penerima pesan memasukkan nomor HP yang dituju dikotak pertama atau dengan menekan tombol kontak untuk mencari nomor yang tersimpan dikontak 2. Penerima pesan juga memilih grup simetri yang sama dengan pengirim pesan. 3. Penerima pesan menulis unsur grup simetri di kotak unsur 2, selanjutnya untuk mengirim unsur 2 dengan menekan tombol kirim unsur 2. 4. Penerima pesan menerima unsur 1 dari pengirim pesan. 5. Penerima pesan menulis nilai P dan Q. 6. Penerima pesan menekan tombol generate y untuk menentukan nilai y, selanjutnya untuk mengirim nilai y dengan menekan tombol kirim y. 7. Penerima pesan menerima x dari penerima pesan. 8. Penerima pesan menekan tombol generate K_2.
Pengirim pesan dan penerima pesan berhasil menyepakati kunci rahasia yang sama yaitu $K = K_1 = K_2$	

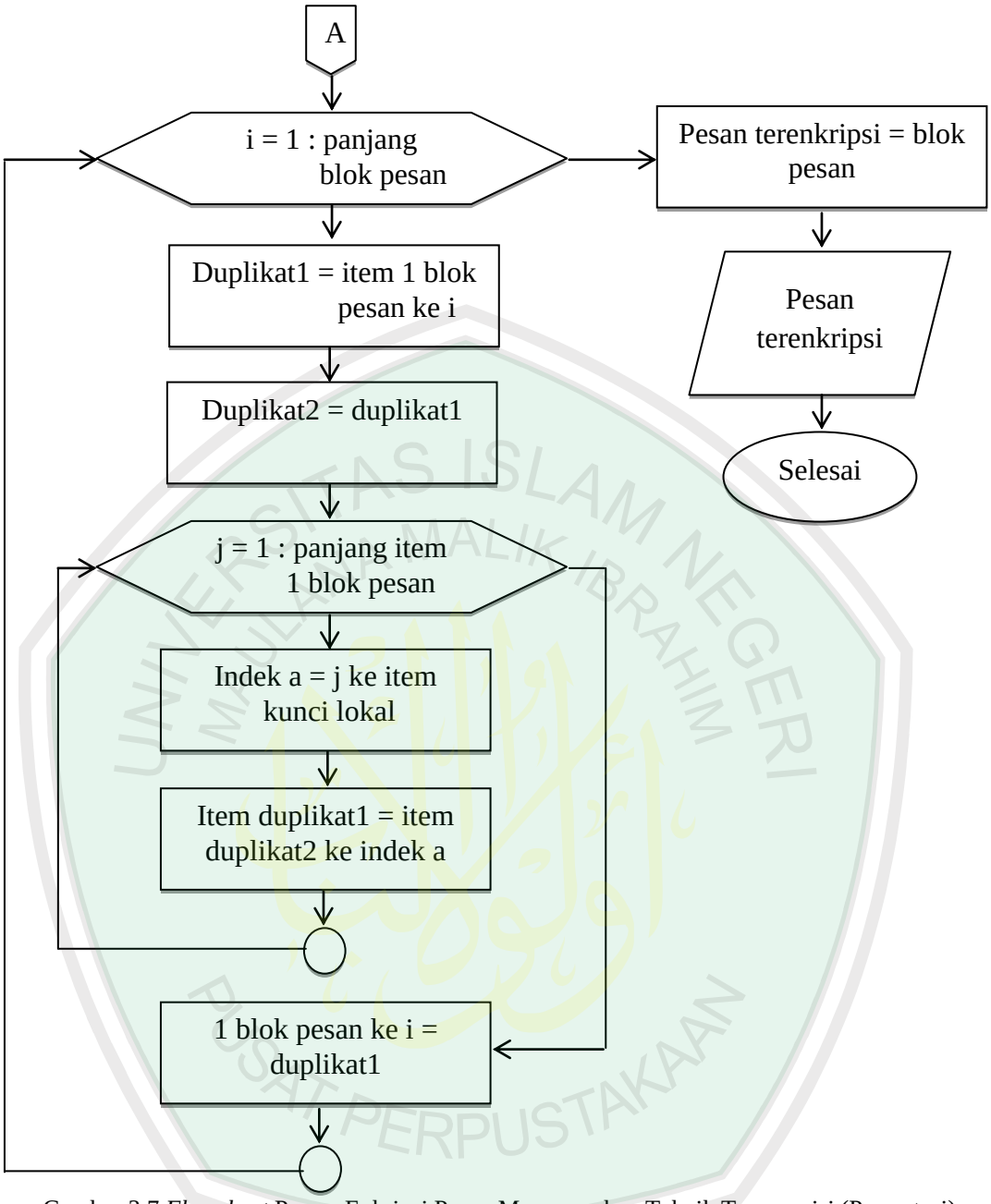
Contoh proses pembentukan kunci oleh pengirim pesan akan ditunjukkan pada Gambar 3.5 dan proses pembentukan kunci oleh penerima pesan akan ditunjukkan pada Gambar 3.6.

Gambar 3.5 Contoh Proses Pembentukan Kunci oleh Pengirim Pesan

Gambar 3.6 Contoh Proses Pembentukan Kunci oleh Penerima Pesan

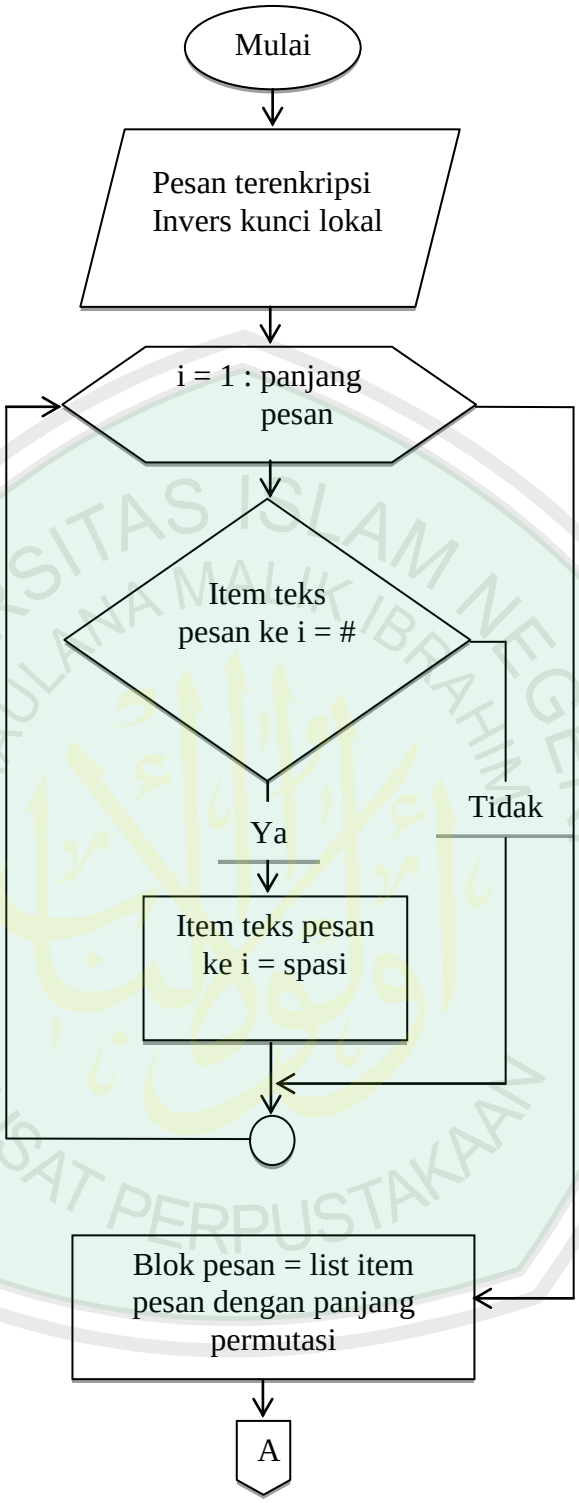
Untuk simulasi proses enkripsi dan dekripsi pesan menggunakan teknik transposisi (permutasi) sama dengan proses pembentukan kunci, terlebih dahulu dibuat *flowchart*, *flowchart* proses enkripsi pesan menggunakan teknik transposisi (permutasi) sebagai berikut:

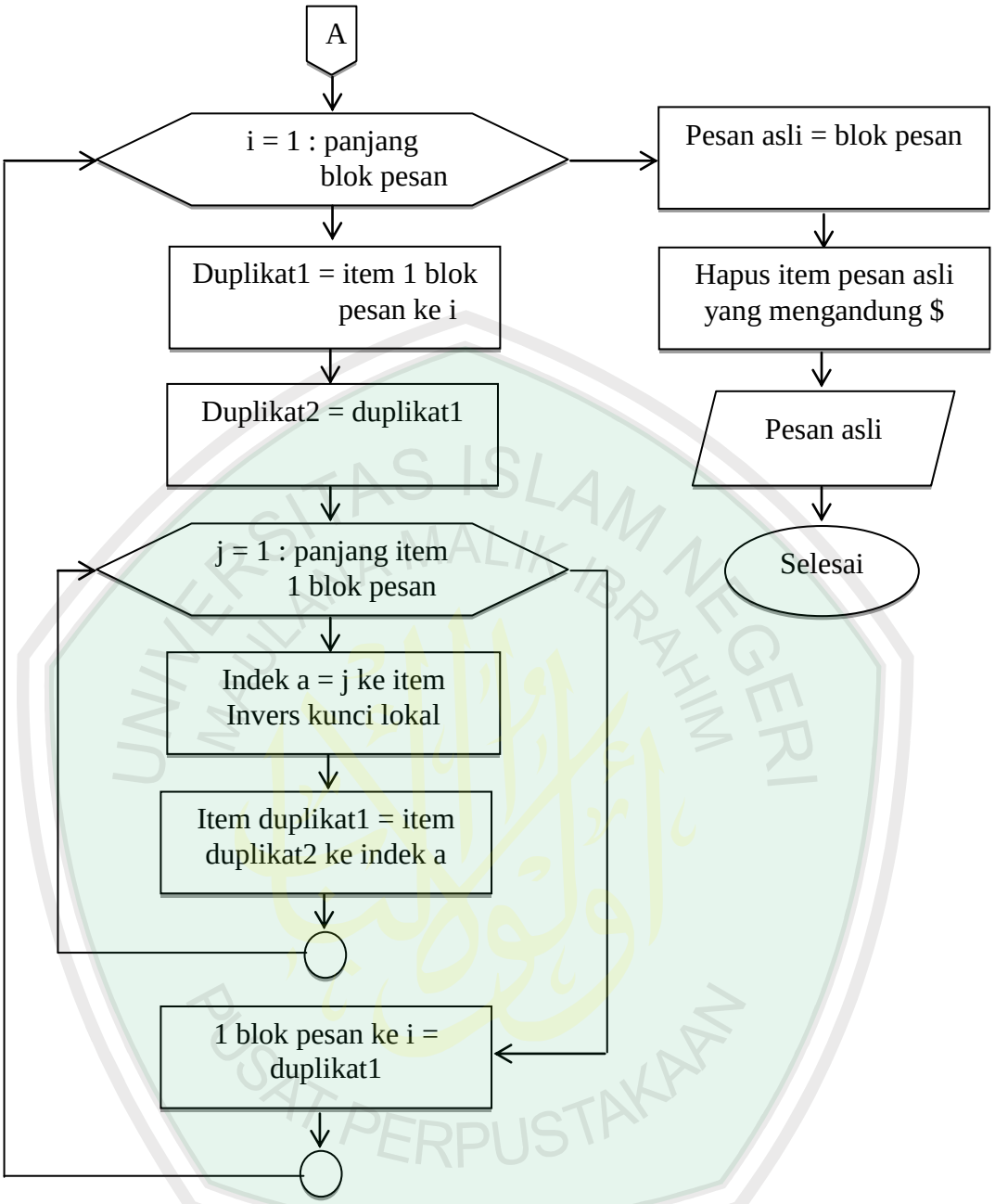

Mulai
Teks pesan
Kunci lokal
i = 1 : panjang pesan
Item teks
pesan ke i =
spasi
Ya
Item teks pesan
ke i = #
Tidak
Panjang pesan
modulo
panjang
permutasi
Ya
Tambah item $ ke dalam
pesan = panjang permutasi
– hasil modulo
Tidak
Blok pesan = list item
pesan dengan panjang
permutasi
A



Gambar 3.7 *Flowchart* Proses Enkripsi Pesan Menggunakan Teknik Transposisi (Permutasi)

flowchart proses dekripsi pesan menggunakan teknik transposisi (permutasi) sebagai berikut:


Mulai
Pesan terenkripsi
Invers kunci lokal
i = 1 : panjang pesan
Item teks pesan ke i = #
Tidak
Ya
Item teks pesan ke i = spasi
Blok pesan = list item pesan dengan panjang permutasi
A



Gambar 3.8 *Flowchart* Proses Dekripsi Pesan Menggunakan Teknik Transposisi (Permutasi)

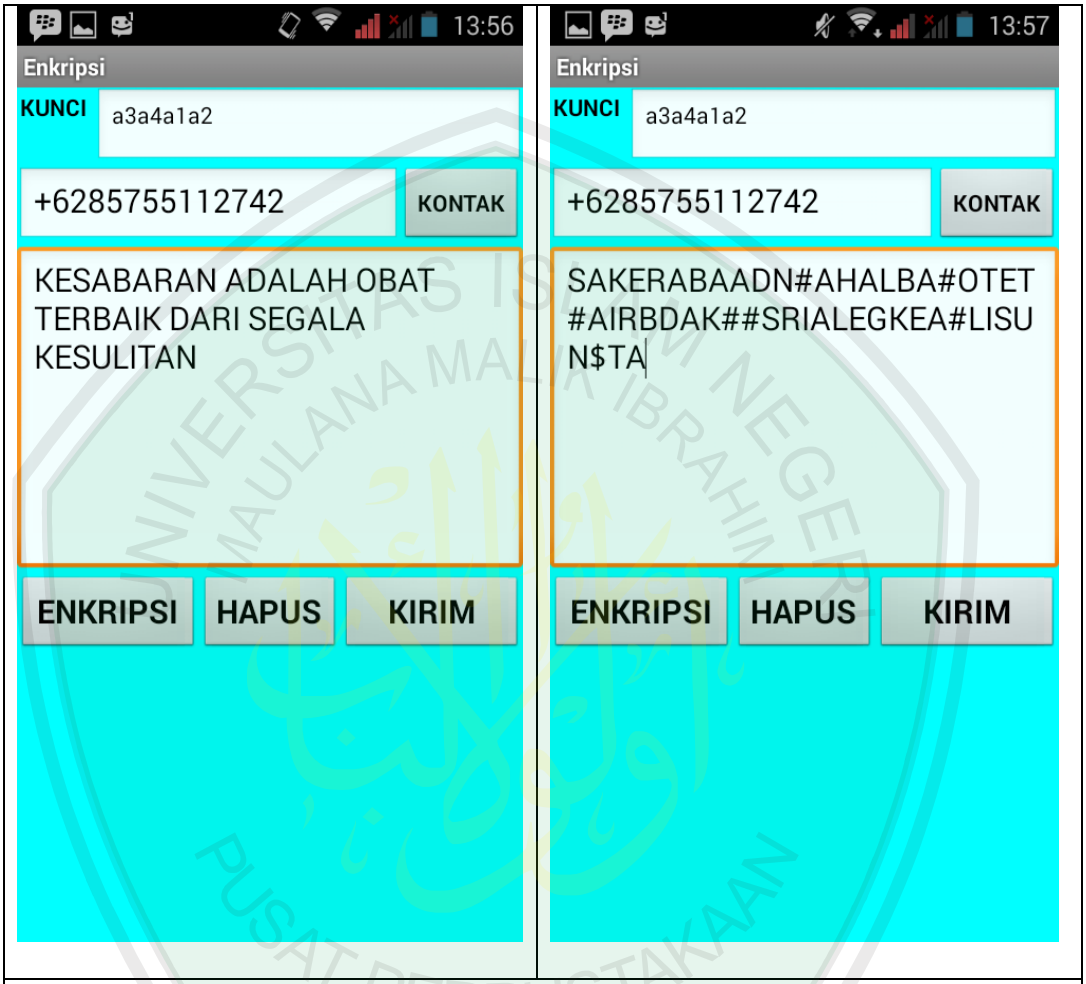
Form enkripsi pesan menggunakan teknik transposisi (permutasi) akan ditunjukkan pada Gambar 3.9 dan dekripsi pesan menggunakan teknik transposisi (permutasi) akan ditunjukkan pada Gambar 3.10.

Gambar 3.9 *Form* Enkripsi Pesan Menggunakan Teknik Transposisi (Permutasi)

Gambar 3.10 *Form* Dekripsi Pesan Menggunakan Teknik Transposisi (Permutasi)

Gambar 3.9 dapat dilakukan simulasi proses enkripsi pesan menggunakan teknik transposisi (permutasi), karena pengirim pesan dan penerima pesan sudah menyepakati kunci rahasia maka kunci yang digunakan secara otomatis akan keluar di kotak kunci. Langkah pertama yang dilakukan pengirim pesan yaitu masukkan nomor HP yang dituju atau dengan menekan tombol kontak untuk mencari nomor HP yang tersimpan di kontak. Langkah kedua tulis *plaintext* di kotak pesan. Langkah ketiga mengenkripsikan *plaintext* dengan menekan tombol enkripsi sehingga menjadi *ciphertext*. langkah keempat kirim *ciphertext* dengan menekan tombol kirim. Contoh akan ditunjukkan pada Gambar 3.11, misal *plaintext* yang ditulis yaitu KESABARAN ADALAH OBAT TERBAIK DARI

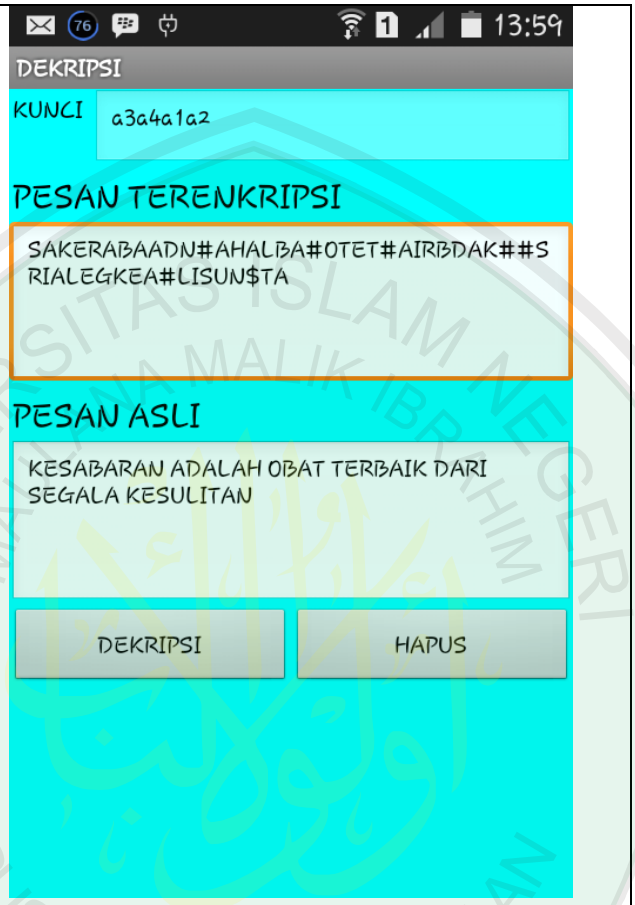
SEGALA KESULITAN kemudian di enkripsi sehingga menjadi *ciphertext* yaitu SAKERABAADN#AHALBA#OTET#AIRBDAK##SRIALEGKEA#LISUN$TA selanjutnya kirim pesan.



Gambar 3.11 Contoh Proses Enkripsi Pesan Menggunakan Teknik Transposisi (Permutasi)

Kemudian penerima pesan menerima *ciphertext* yaitu SAKERABAADN#AHALBA#OTET#AIRBDAK##SRIALEGKEA#LISUN$TA untuk bisa mendekripsikan *ciphertext* berarti penerima pesan harus mempunyai aplikasi yang sama dengan pengirim pesan. sama halnya dengan proses enkripsi, kunci yang digunakan secara otomatis akan keluar di kotak kunci akan tetapi kunci sudah diinverskan. Setelah itu masukkan *ciphertext* tersebut pada kotak

pesan terenkripsi, kemudia tekan tombol dekripsi maka akan keluar di kotak pesan asli kalimat yang semula yaitu KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN. Proses ini akan ditunjukkan pada Gambar 3.12.



Gambar 3.12 Contoh Proses Dekripsi Pesan Menggunakan Teknik Transposisi (Permutasi)

Hasil akhir dari penelitian ini dapat dibuktikan bahwa perhitungan secara manual dan secara program diperoleh hasil yang sama.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan hasil pembahasan, dapat diperoleh kesimpulan sebagai berikut:

1. Proses enkripsi pesan dengan menggunakan grup simetri S_n untuk mengamankan informasi akan menghasilkan *ciphertext* yang tidak dapat dimengerti. Langkah petama pengirim pesan dan penerima pesan menyepakati kunci rahasia menggunakan grup simetri-n. Dalam hal ini diberikan sebuah contoh kasus yaitu "KESABARAN ADALAH OBAT TERBAIK DARI SEGALA KESULITAN" dengan menggunakan kunci bentuk permutasi P_4, misal $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix}$. Pesan terlebih dahulu dibagi menjadi blok-blok yang terdiri dari 4 huruf kemudian proses enkripsi dilakukan satu persatu dari blok tersebut sehingga pesan berubah menjadi *ciphertext* yaitu "SAKERABAADN#AHALBA#OTET#AIRBDAK##SRIALEGKEA#LISUN $TA". Dengan menggunakan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula, meskipun menggunakan *plaintext* yang sama.
2. Proses dekripsi merupakan kebalikan dari proses enkripsi. C*iphertext* yang dihasilkan dari proses enkripsi akan diubah ke bentuk asalnya. Pada dasarnya proses dekripsi sama saja dengan proses enkripsi, akan tetapi kunci yang digunakan diinverskan terlebih dahulu. Sehingga *ciphertext* "SAKERABAADN#AHALBA#OTET#AIRBDAK##SRIALEGKEA#LISN$T A" akan kembali menjadi *plaintext* "KESABARAN ADALAH OBAT

TERBAIK DARI SEGALA KESULITAN". Jika menggunakan kunci yang berbeda pada proses dekripsi maka *ciphertext* tidak dapat kembali ke bentuk pesan *plaintext* dan akan tetap menjadi pesan *ciphertext* yang tidak dapat dibaca dan dimengerti artinya.

3. Penyandian dengan menggunakan teknik transposisi (permutasi) dapat dibuat simulasi dengan menggunakan aplikasi App Inventor. Aplikasi ini dapat digunakan oleh orang lain untuk mengamankan pesan rahasia dengan mudah.

4.2 Saran

Pada penelitian ini membahas tentang proses enkripsi dan dekripsi pesan menggunakan grup simetri S_n untuk mengamankan pesan. Teknik yang digunakan yaitu teknik transposisi (pemutasi). Untuk penelitian selanjutnya, disarankan untuk menggunakan teknik lain yang tingkat keamanannya lebih tinggi atau menggunakan metode kriptografi modern yang lebih kompleks dan menggunakan aplikasi program komputer yang lain.

DAFTAR PUSTAKA

Ad-Dimasyqi. 2001. *Tafsir Ibnu Katsir*. Bandung: Sinar Baru Algensindo.

Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi.* Yogyakarta: C.V ANDI OFFSET.

Dummit, D.S dan Foote, R.M. 2004. *Abstract Algebra Third Edition*. New York: Prentice-Hall International, Inc.

Prasetiyo, A.F. 2014. *App Inventor untuk Pemula*. Tangerang: Surya University.

Muhsetyo, G. 1997. *Dasar-Dasar Teori Bilangan*. Jakarta: PGSM.

Myasnikov, A., Shpilrain, A., dan Ushakov, A. 2008. *Group-based Cryptography*. Basel Switzerland: Birkhauser Verlag.

Raisinghania, M.D. dan Aggarwal, R.S. 1980. *Modern Algebra*. New Delhi: S. Chand & Company LTD.

Riyanto, M.Z. 2010. *Sistem Kriptografi Kunci Publik Multivariat*. Makalah Seminar Nasional Matematika dan Pendidikan Matematika. Yogyakarta: Lembaga Penelitian UNY. 27 November 2010.

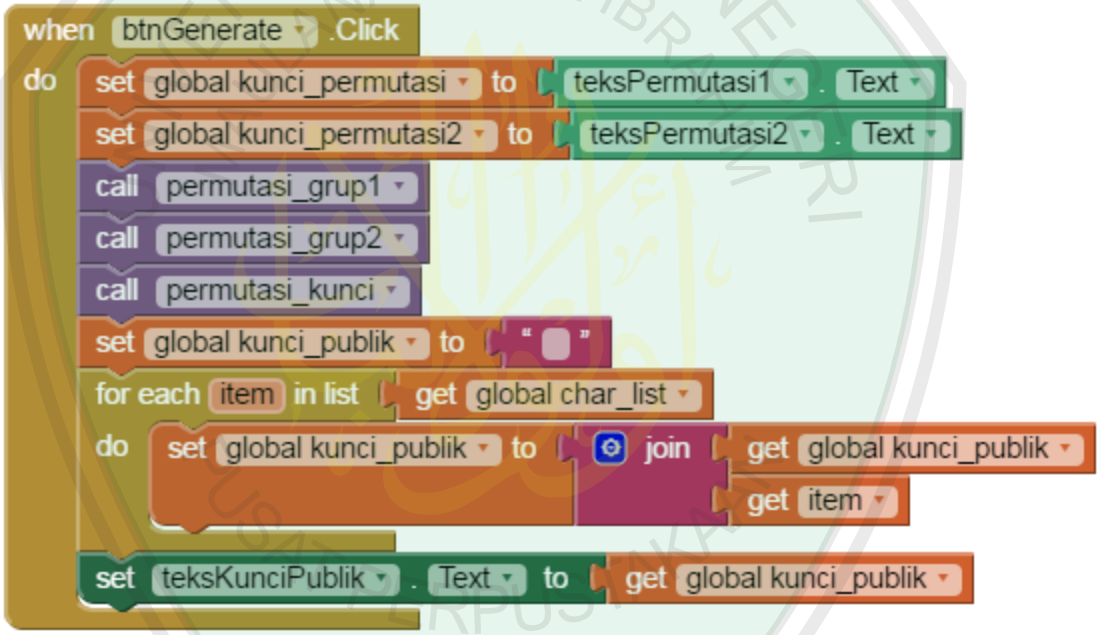
Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: C.V ANDI OFFSET.

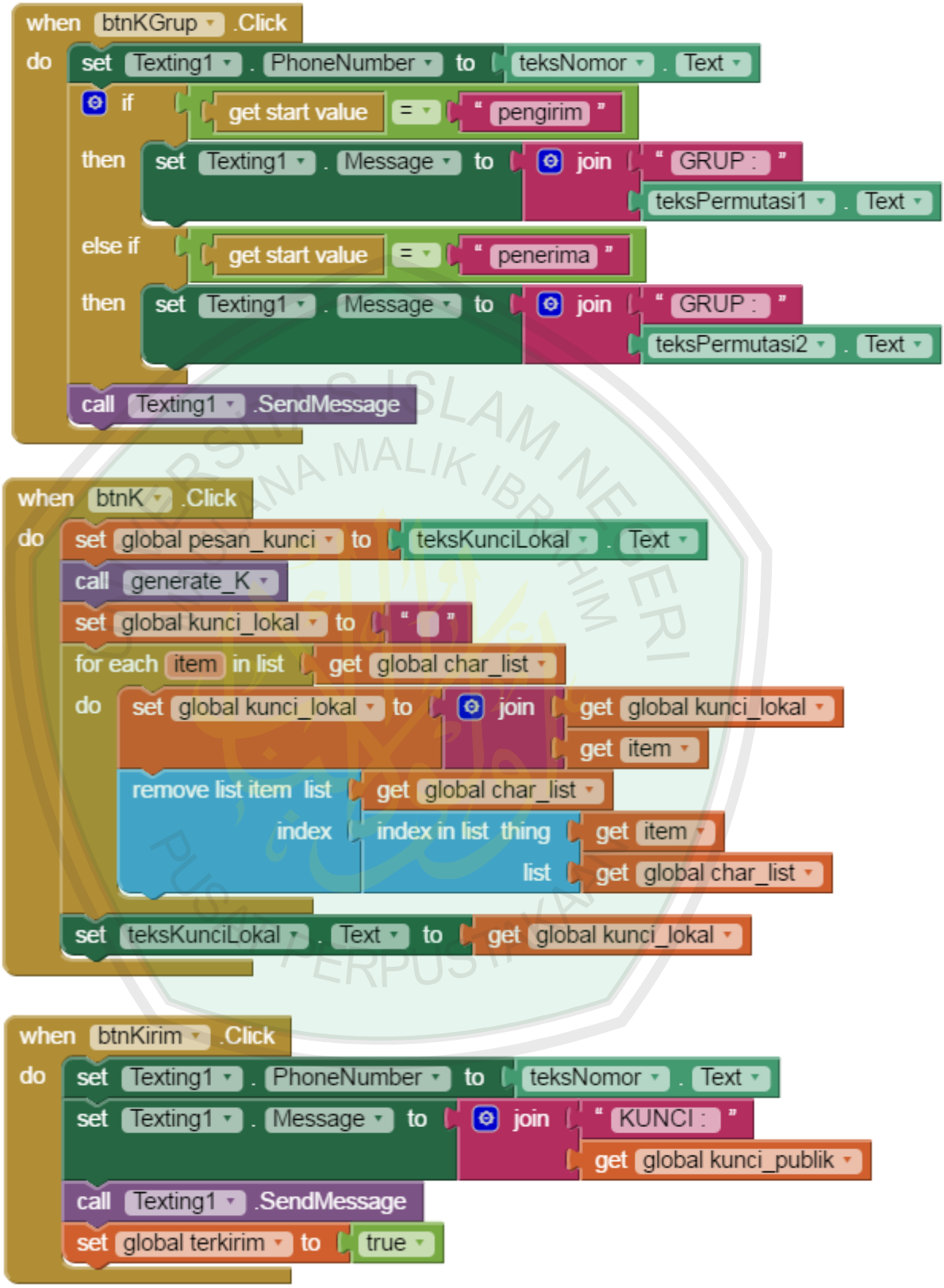
Wicaksono, D.R. 2014. *Aplikasi Aljabar Min-Plus untuk Mengamankan Informasi Rahasia*. Skripsi tidak diterbitkan. Yogyakarta: Universitas Negeri Yogyakarta.

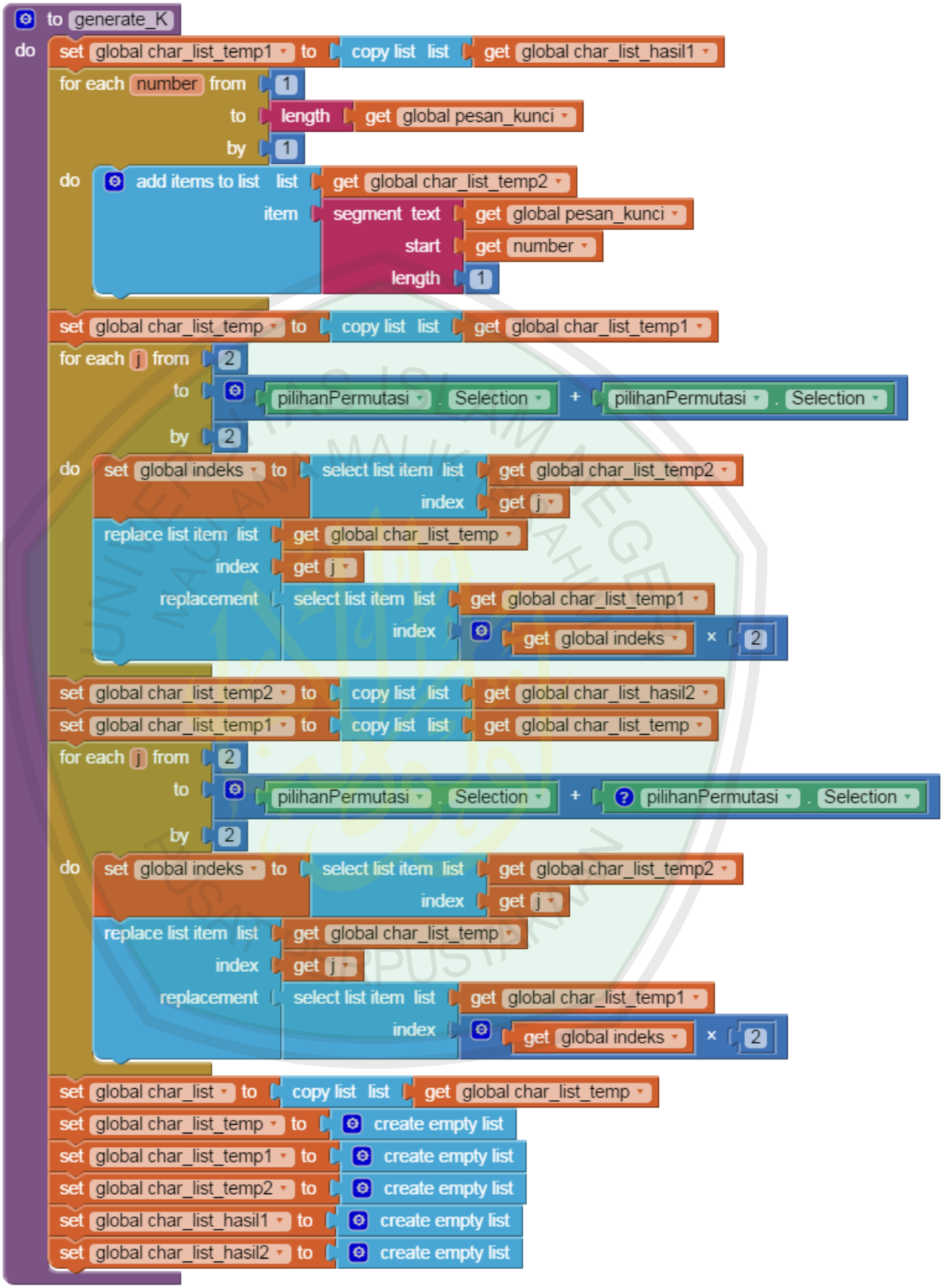
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM
PUSAT PERPUSTAKAAN

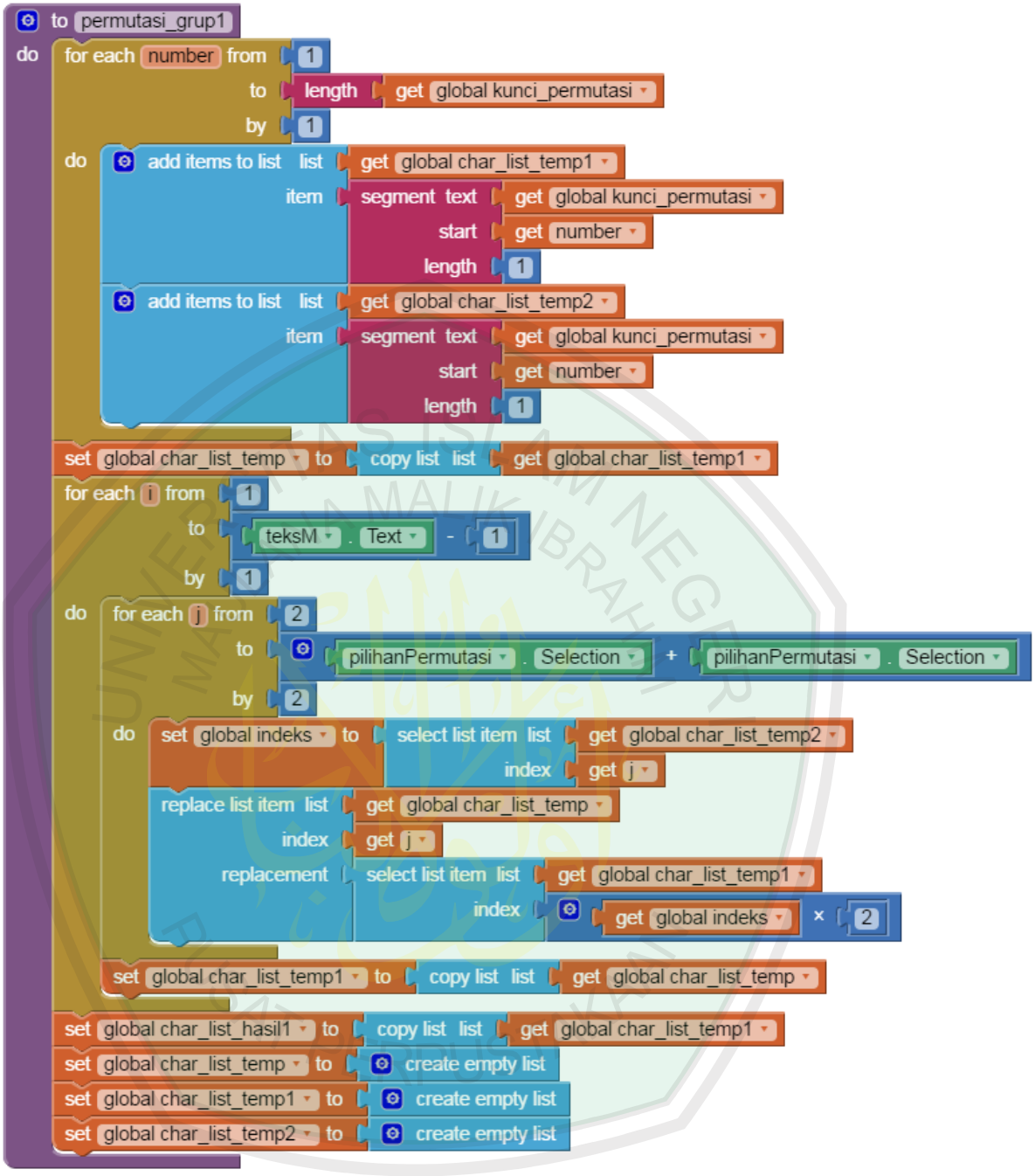
LAMPIRAN

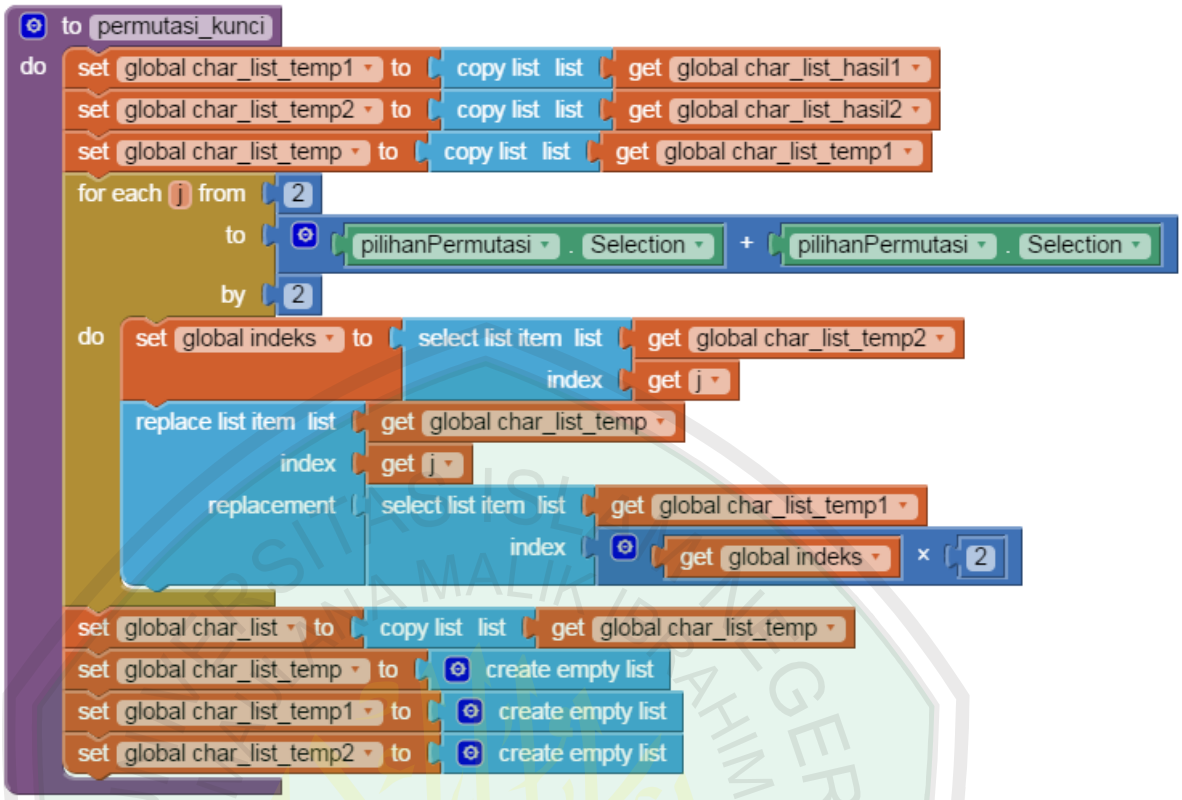
1. Proses Pembentukan Kunci

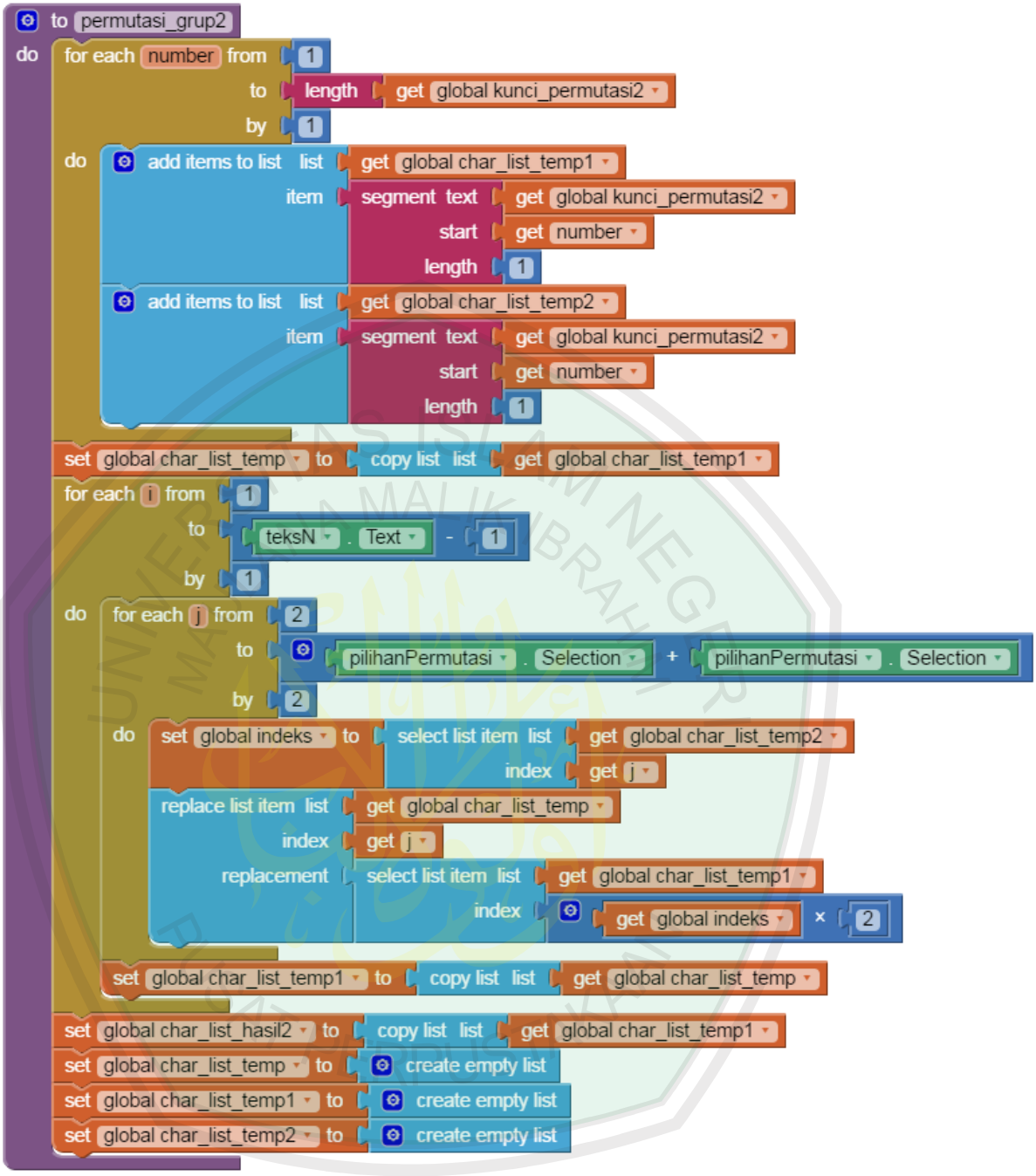


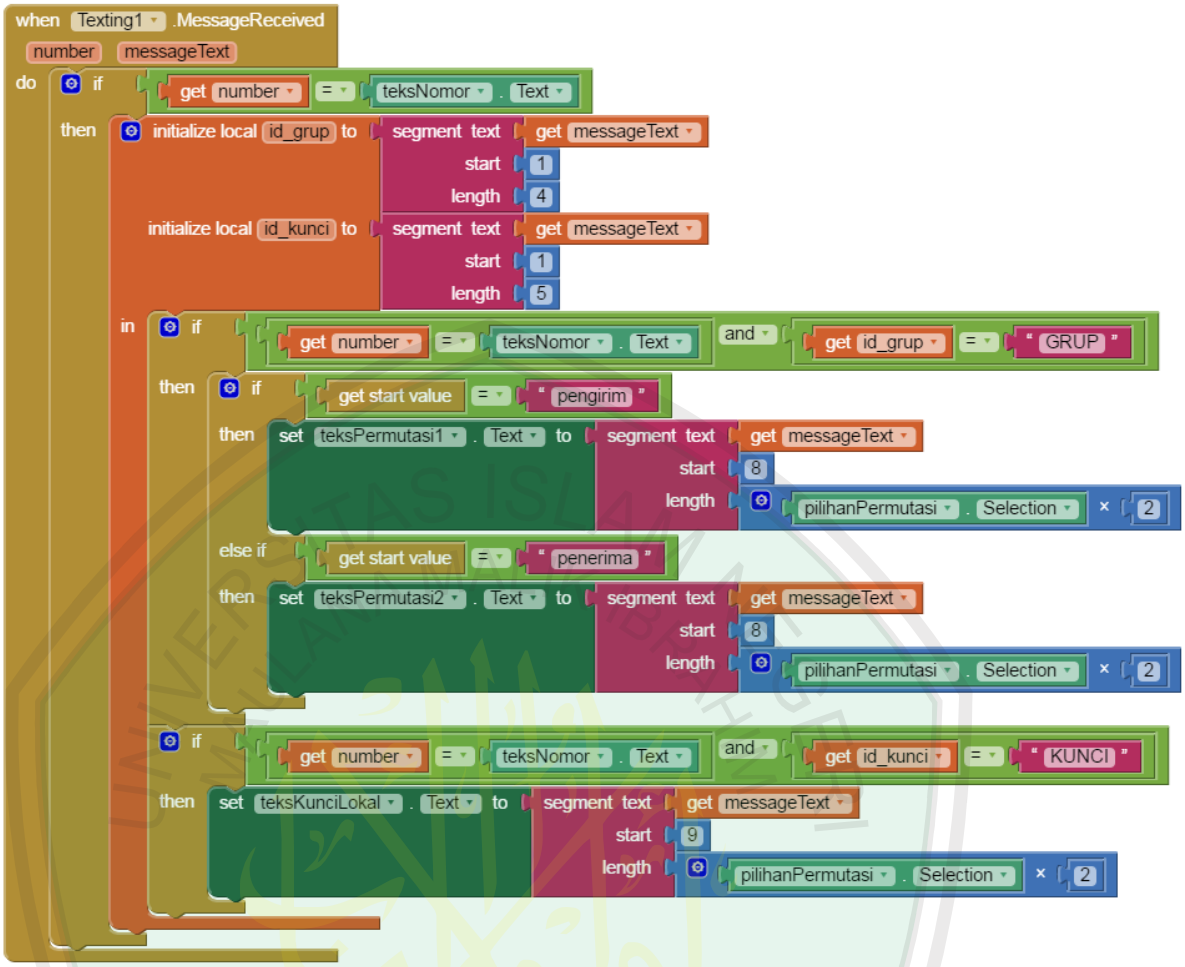

when btnKGrup .Click
do set Texting1 . PhoneNumber to teksNomor . Text
if get start value = " pengirim "
then set Texting1 . Message to join " GRUP : " teksPermutasi1 . Text
else if get start value = " penerima "
then set Texting1 . Message to join " GRUP : " teksPermutasi2 . Text
call Texting1 .SendMessage
when btnK .Click
do set global pesan_kunci to teksKunciLokal . Text
call generate_K
set global kunci_lokal to " "
for each item in list get global char_list
do set global kunci_lokal to join get global kunci_lokal get item
remove list item list get global char_list index index in list thing get item list get global char_list
set teksKunciLokal . Text to get global kunci_lokal
when btnKirim .Click
do set Texting1 . PhoneNumber to teksNomor . Text
set Texting1 . Message to join " KUNCI : " get global kunci_publik
call Texting1 .SendMessage
set global terkirim to true

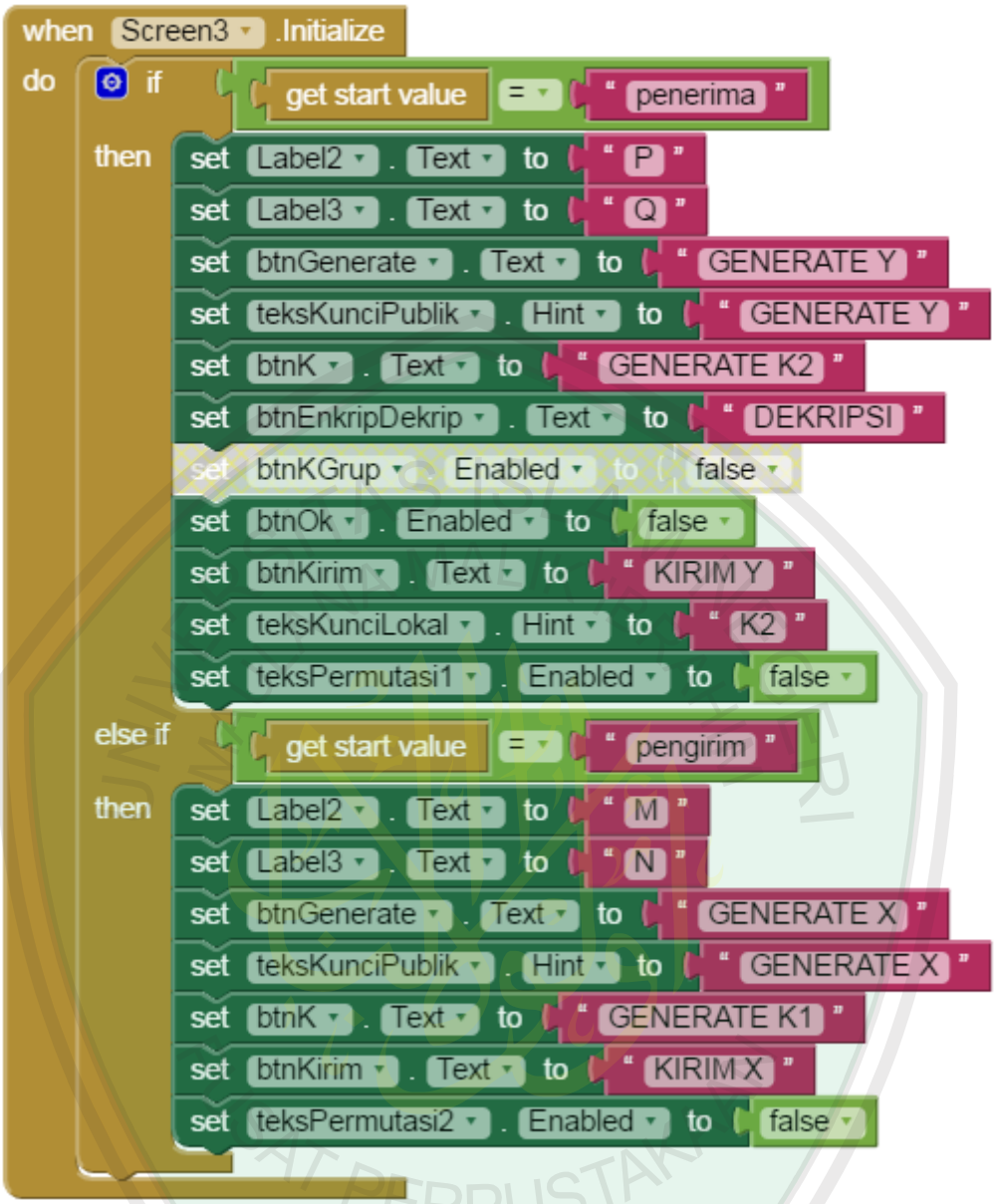

to generate_K
do
set global char_list_temp1 to copy list list get global char_list_hasil1
for each number from 1
to length get global pesan_kunci
by 1
do add items to list list get global char_list_temp2
item segment text get global pesan_kunci
start get number
length 1
set global char_list_temp to copy list list get global char_list_temp1
for each j from 2
to pilihanPermutasi . Selection + pilihanPermutasi . Selection
by 2
do set global indeks to select list item list get global char_list_temp2
index get j
replace list item list get global char_list_temp
index get j
replacement select list item list get global char_list_temp1
index get global indeks × 2
set global char_list_temp2 to copy list list get global char_list_hasil2
set global char_list_temp1 to copy list list get global char_list_temp
for each j from 2
to pilihanPermutasi . Selection + pilihanPermutasi . Selection
by 2
do set global indeks to select list item list get global char_list_temp2
index get j
replace list item list get global char_list_temp
index get j
replacement select list item list get global char_list_temp1
index get global indeks × 2
set global char_list to copy list list get global char_list_temp
set global char_list_temp to create empty list
set global char_list_temp1 to create empty list
set global char_list_temp2 to create empty list
set global char_list_hasil1 to create empty list
set global char_list_hasil2 to create empty list

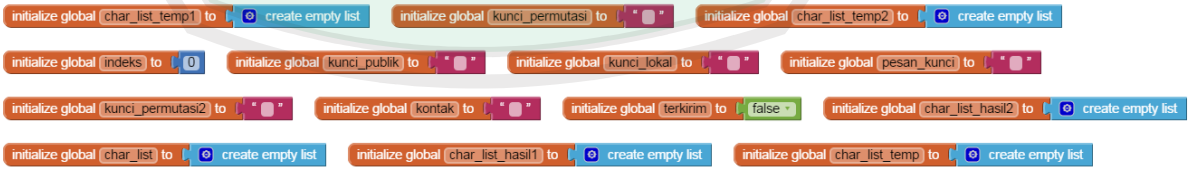

to permutasi_grup1
do
for each number from 1
to length get global kunci_permutasi
by 1
do add items to list list get global char_list_temp1
item segment text get global kunci_permutasi
start get number
length 1
add items to list list get global char_list_temp2
item segment text get global kunci_permutasi
start get number
length 1
set global char_list_temp to copy list list get global char_list_temp1
for each i from 1
to teksM . Text - 1
by 1
do for each j from 2
to pilihanPermutasi . Selection + pilihanPermutasi . Selection
by 2
do set global indeks to select list item list get global char_list_temp2
index get j
replace list item list get global char_list_temp
index get j
replacement select list item list get global char_list_temp1
index get global indeks × 2
set global char_list_temp1 to copy list list get global char_list_temp
set global char_list_hasil1 to copy list list get global char_list_temp1
set global char_list_temp to create empty list
set global char_list_temp1 to create empty list
set global char_list_temp2 to create empty list


to permutasi_kunci
do
set global char_list_temp1 to copy list list get global char_list_hasil1
set global char_list_temp2 to copy list list get global char_list_hasil2
set global char_list_temp to copy list list get global char_list_temp1
for each j from 2
to pilihanPermutasi . Selection + pilihanPermutasi . Selection
by 2
do set global indeks to select list item list get global char_list_temp2
index get j
replace list item list get global char_list_temp
index get j
replacement select list item list get global char_list_temp1
index get global indeks × 2
set global char_list to copy list list get global char_list_temp
set global char_list_temp to create empty list
set global char_list_temp1 to create empty list
set global char_list_temp2 to create empty list


to permutasi_grup2
do
for each number from 1
to length get global kunci_permutasi2
by 1
do add items to list list get global char_list_temp1
item segment text get global kunci_permutasi2
start get number
length 1
add items to list list get global char_list_temp2
item segment text get global kunci_permutasi2
start get number
length 1
set global char_list_temp to copy list list get global char_list_temp1
for each i from 1
to teksN . Text - 1
by 1
do for each j from 2
to pilihanPermutasi . Selection + pilihanPermutasi . Selection
by 2
do set global indeks to select list item list get global char_list_temp2
index get j
replace list item list get global char_list_temp
index get j
replacement select list item list get global char_list_temp1
index get global indeks × 2
set global char_list_temp1 to copy list list get global char_list_temp
set global char_list_hasil2 to copy list list get global char_list_temp1
set global char_list_temp to create empty list
set global char_list_temp1 to create empty list
set global char_list_temp2 to create empty list

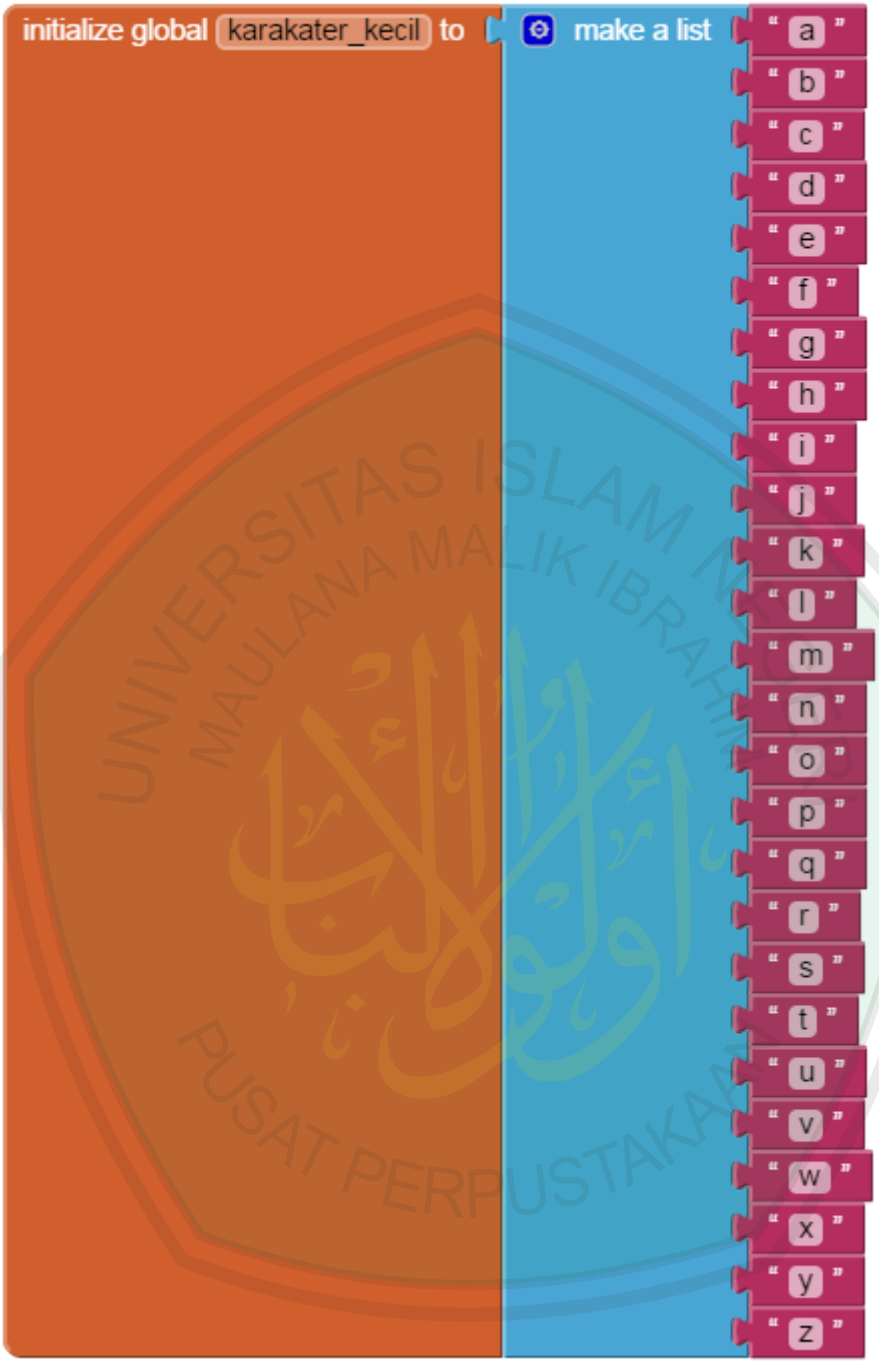

when Texting1 .MessageReceived
number
messageText
do
if
get number = teksNomor . Text
then
initialize local id_grup to
segment text get messageText
start 1
length 4
initialize local id_kunci to
segment text get messageText
start 1
length 5
in
if
get number = teksNomor . Text
and
get id_grup = " GRUP "
then
if
get start value = " pengirim "
then
set teksPermutasi1 . Text to
segment text get messageText
start 8
length
pilihanPermutasi . Selection × 2
else if
get start value = " penerima "
then
set teksPermutasi2 . Text to
segment text get messageText
start 8
length
pilihanPermutasi . Selection × 2
if
get number = teksNomor . Text
and
get id_kunci = " KUNCI "
then
set teksKunciLokal . Text to
segment text get messageText
start 9
length
pilihanPermutasi . Selection × 2

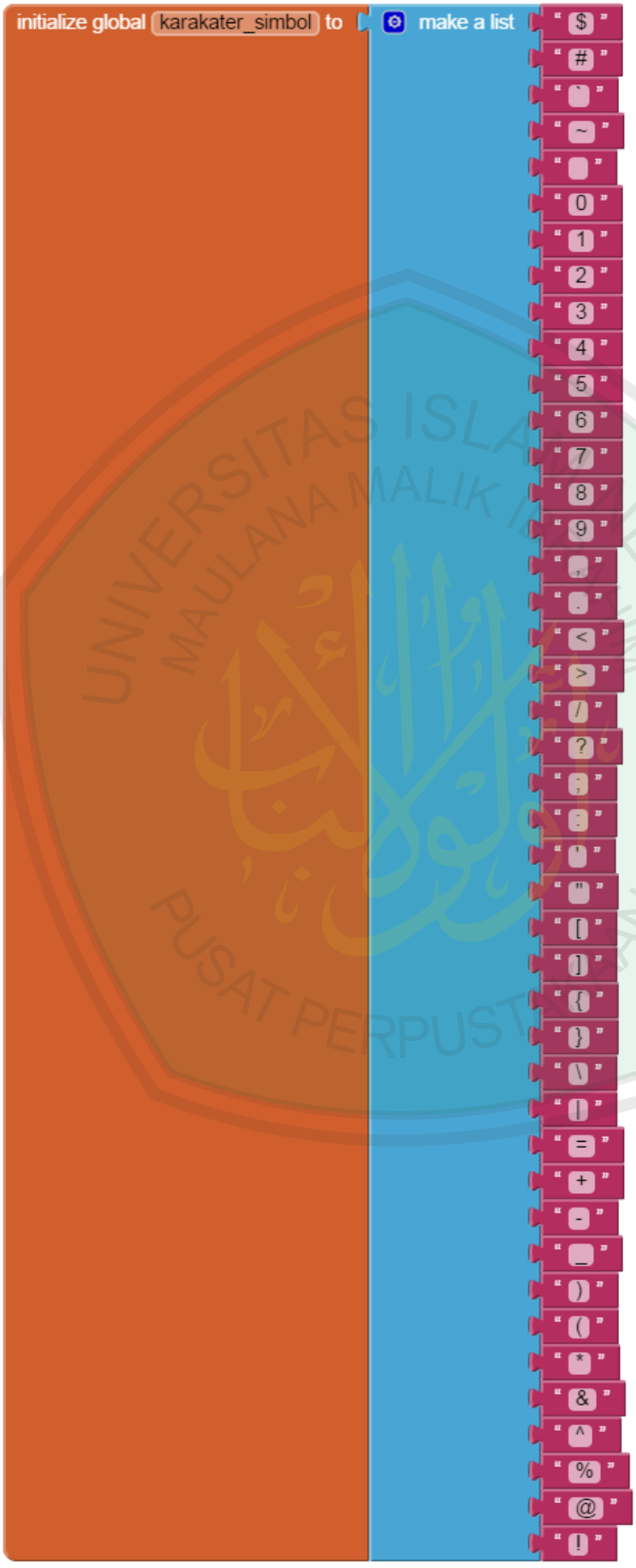

when Screen3 .Initialize
do if get start value = " penerima "
then set Label2 . Text to " P "
set Label3 . Text to " Q "
set btnGenerate . Text to " GENERATE Y "
set teksKunciPublik . Hint to " GENERATE Y "
set btnK . Text to " GENERATE K2 "
set btnEnkripDekrip . Text to " DEKRIPSI "
set btnKGrup . Enabled to false
set btnOk . Enabled to false
set btnKirim . Text to " KIRIM Y "
set teksKunciLokal . Hint to " K2 "
set teksPermutasi1 . Enabled to false
else if get start value = " pengirim "
then set Label2 . Text to " M "
set Label3 . Text to " N "
set btnGenerate . Text to " GENERATE X "
set teksKunciPublik . Hint to " GENERATE X "
set btnK . Text to " GENERATE K1 "
set btnKirim . Text to " KIRIM X "
set teksPermutasi2 . Enabled to false

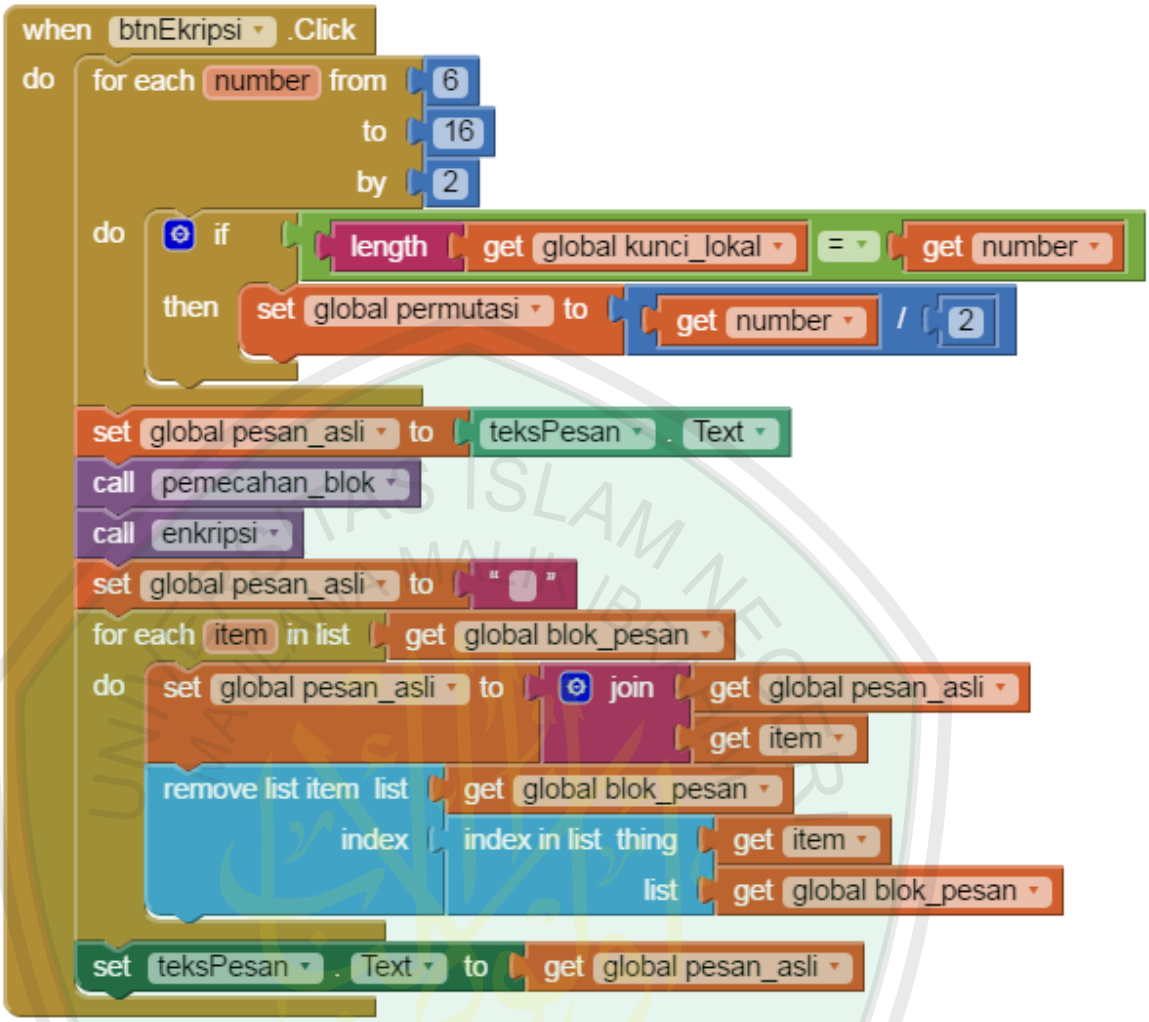

initialize global char_list_temp1 to create empty list
initialize global kunci_permutasi to " "
initialize global char_list_temp2 to create empty list
initialize global indeks to 0
initialize global kunci_publik to " "
initialize global kunci_lokal to " "
initialize global pesan_kunci to " "
initialize global kunci_permutasi2 to " "
initialize global kontak to " "
initialize global terkirim to false
initialize global char_list_hasil2 to create empty list
initialize global char_list to create empty list
initialize global char_list_hasil1 to create empty list
initialize global char_list_temp to create empty list

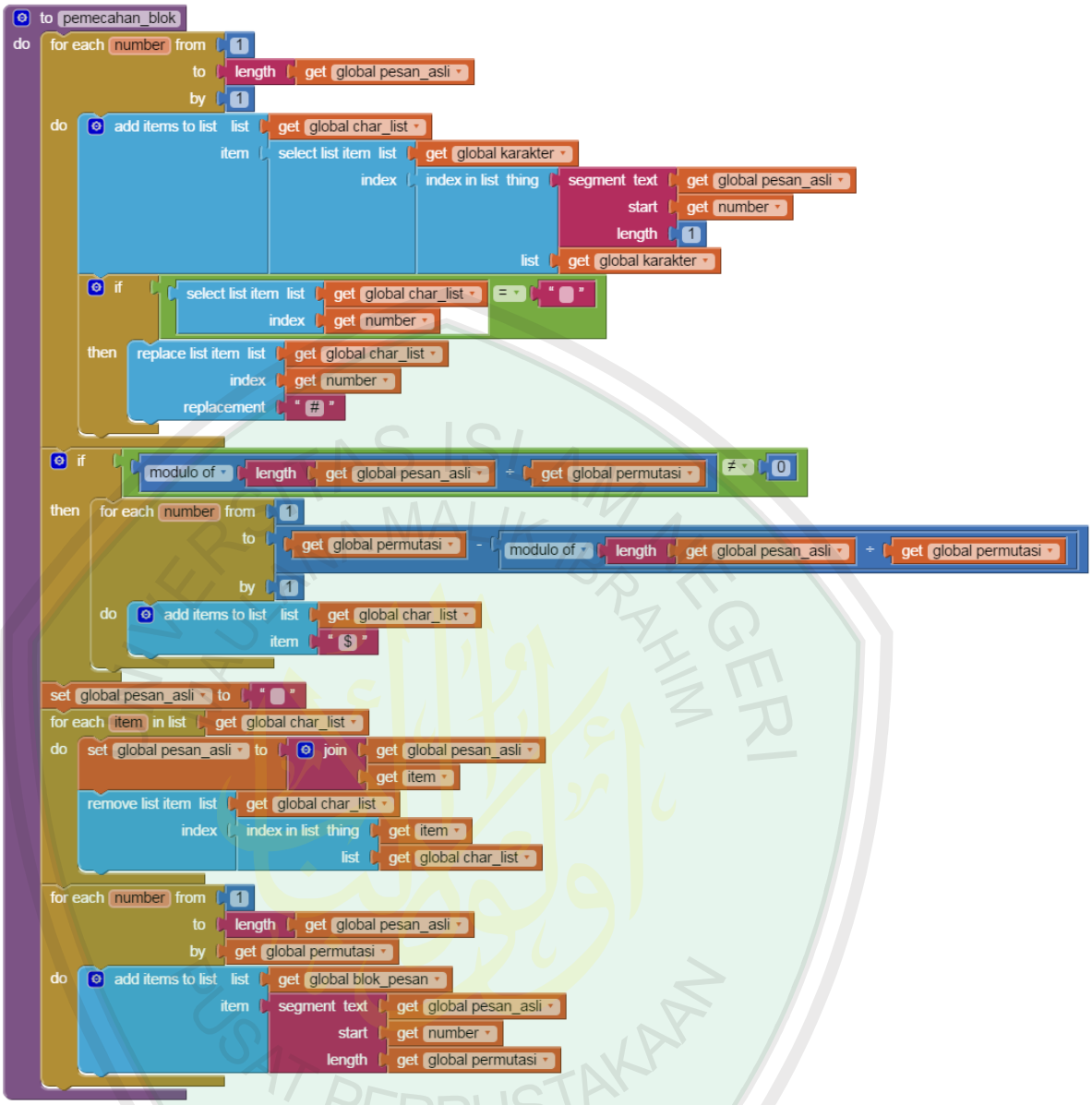
2. Proses Enkripsi Pesan

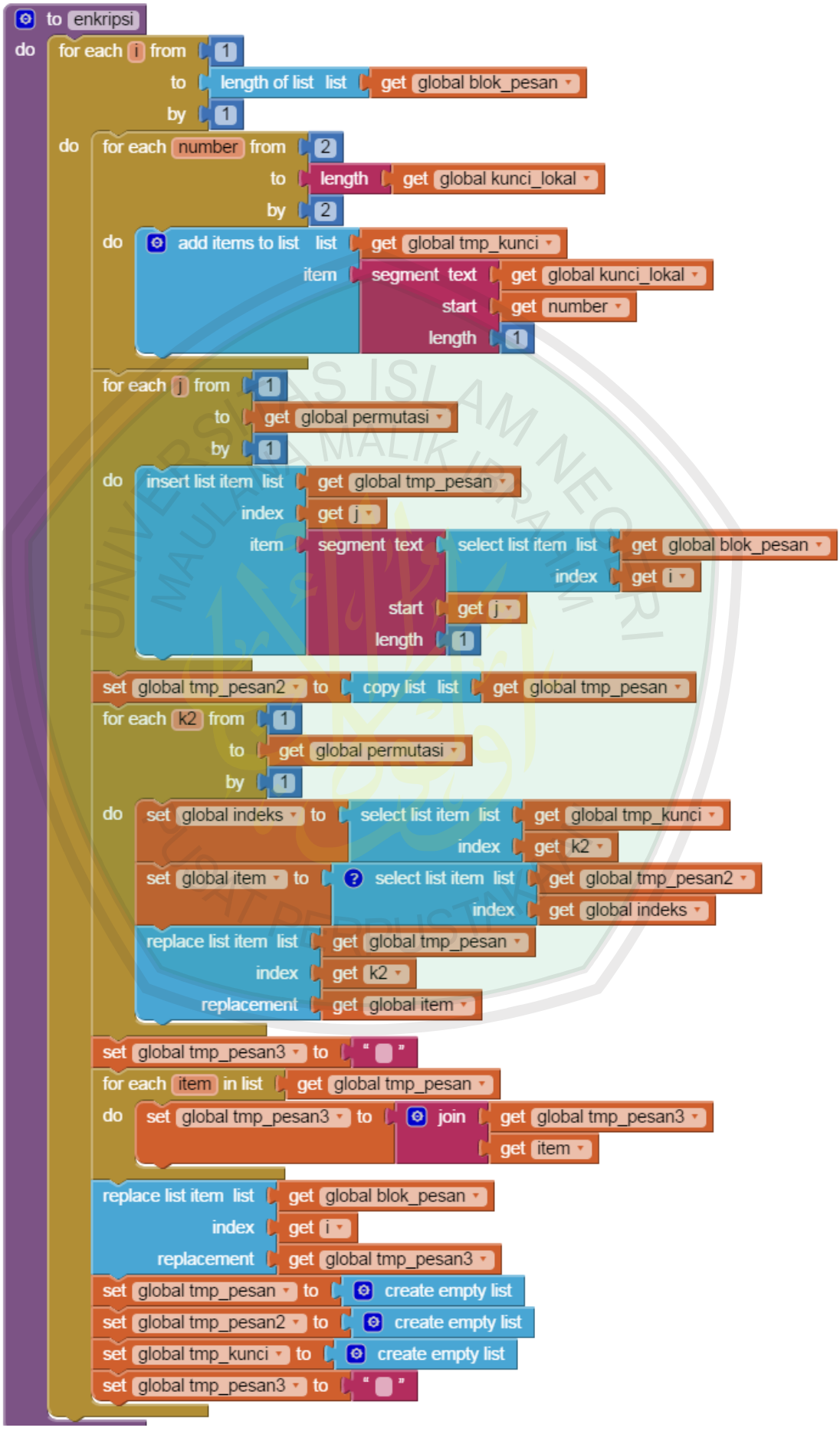

initialize global karakater_besar to
make a list
" A "
" B "
" C "
" D "
" E "
" F "
" G "
" H "
" I "
" J "
" K "
" L "
" M "
" N "
" O "
" P "
" Q "
" R "
" S "
" T "
" U "
" V "
" W "
" X "
" Y "
" Z "


initialize global karakater_kecil to
make a list
" a "
" b "
" c "
" d "
" e "
" f "
" g "
" h "
" i "
" j "
" k "
" l "
" m "
" n "
" o "
" p "
" q "
" r "
" s "
" t "
" u "
" v "
" w "
" x "
" y "
" z "


initialize global karakater_simbol to
make a list
" $ "
" # "
" ` "
" ~ "
" "
" 0 "
" 1 "
" 2 "
" 3 "
" 4 "
" 5 "
" 6 "
" 7 "
" 8 "
" 9 "
" , "
" . "
" < "
" > "
" / "
" ? "
" ; "
" : "
" ' "
" " "
" ["
"] "
" { "
" } "
" \ "
" | "
" = "
" + "
" - "
" _ "
") "
" ("
" * "
" & "
" ^ "
" % "
" @ "
" ! "

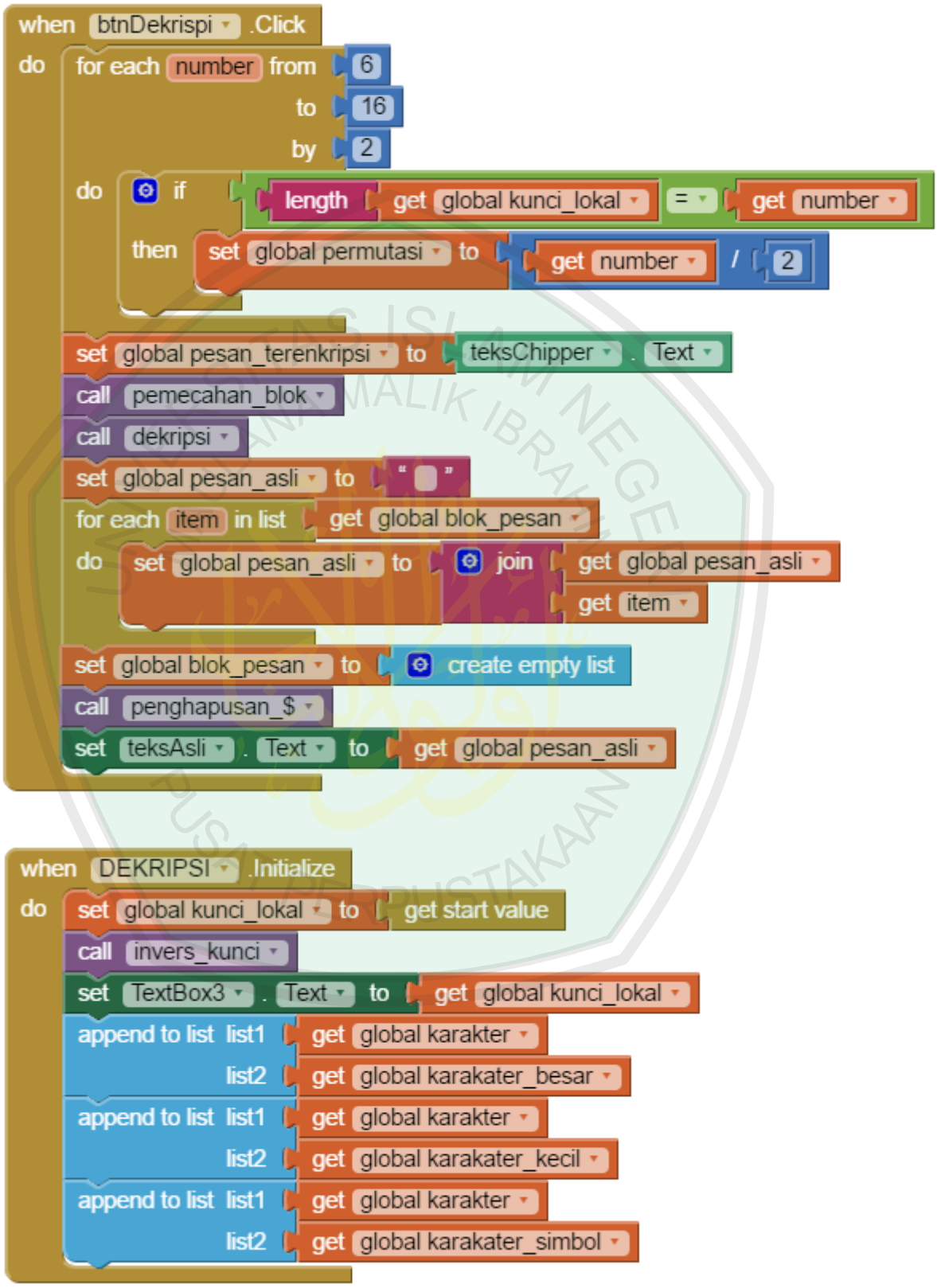

when btnEkripsi .Click
do
for each number from 6
to 16
by 2
do if length get global kunci_lokal = get number
then set global permutasi to get number / 2
set global pesan_asli to teksPesan . Text
call pemecahan_blok
call enkripsi
set global pesan_asli to " "
for each item in list get global blok_pesan
do set global pesan_asli to join get global pesan_asli
get item
remove list item list get global blok_pesan
index index in list thing get item
list get global blok_pesan
set teksPesan . Text to get global pesan_asli

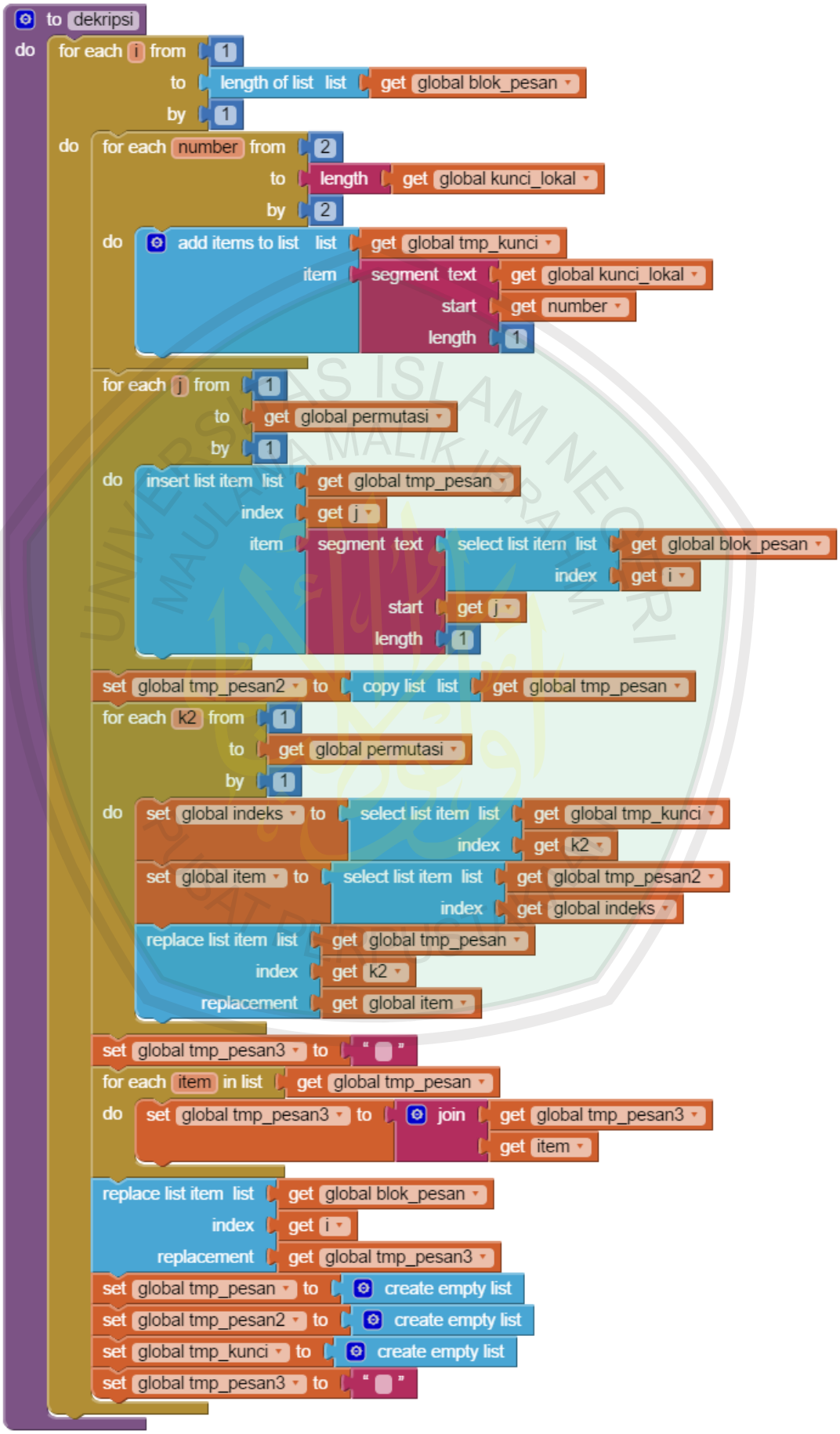

to pemecahan_blok
do
for each number from 1
to length get global pesan_asli
by 1
do add items to list list get global char_list
item select list item list get global karakter
index index in list thing segment text get global pesan_asli
start get number
length 1
list get global karakter
if select list item list get global char_list = " "
index get number
then replace list item list get global char_list
index get number
replacement " # "
if modulo of length get global pesan_asli ÷ get global permutasi ≠ 0
then for each number from 1
to get global permutasi - modulo of length get global pesan_asli ÷ get global permutasi
by 1
do add items to list list get global char_list
item " $ "
set global pesan_asli to " "
for each item in list get global char_list
do set global pesan_asli to join get global pesan_asli
get item
remove list item list get global char_list
index index in list thing get item
list get global char_list
for each number from 1
to length get global pesan_asli
by get global permutasi
do add items to list list get global blok_pesan
item segment text get global pesan_asli
start get number
length get global permutasi

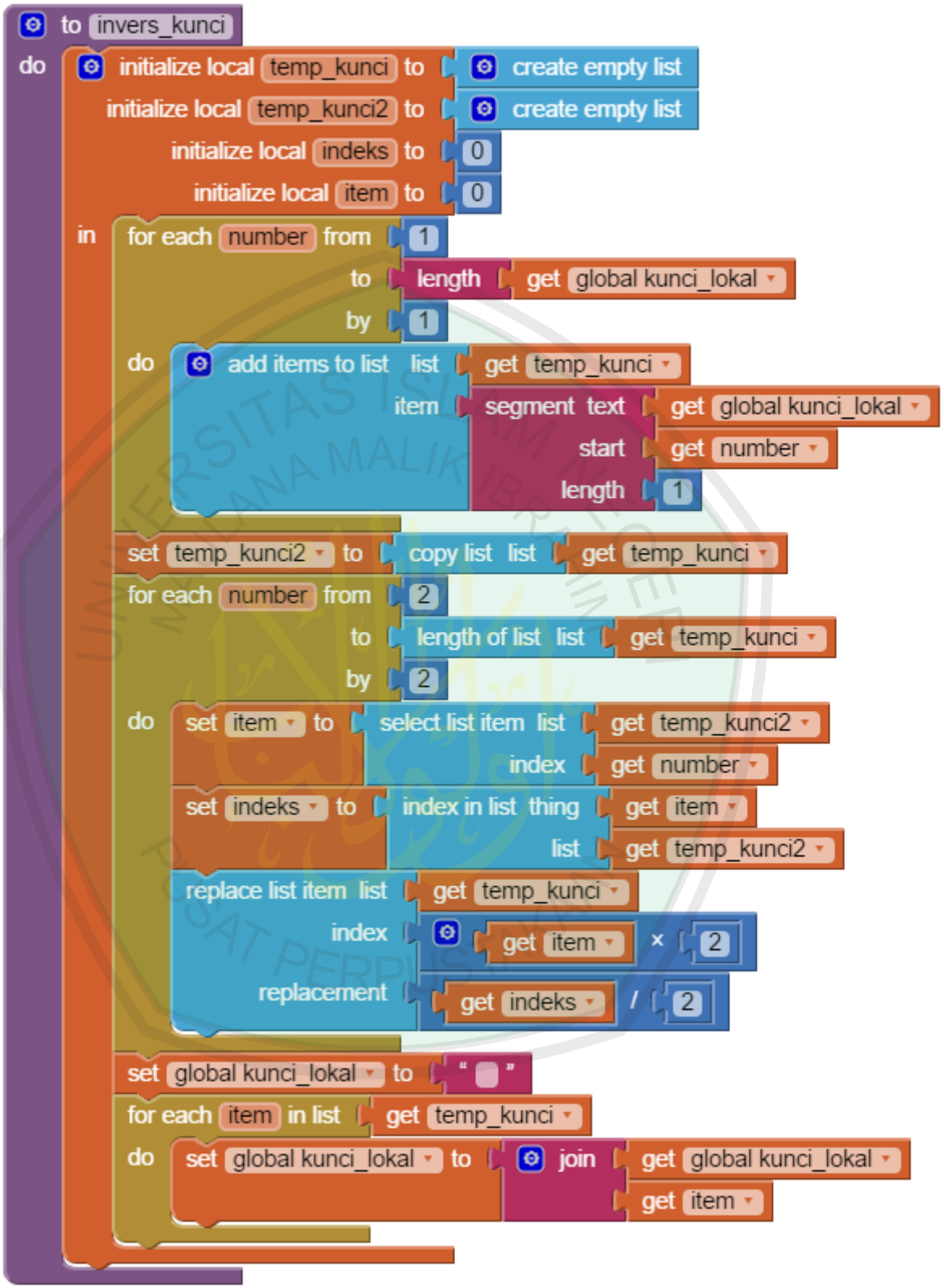

to enkripsi
do
for each i from 1
to length of list list get global blok_pesan
by 1
do
for each number from 2
to length get global kunci_lokal
by 2
do
add items to list list get global tmp_kunci
item segment text get global kunci_lokal
start get number
length 1
for each j from 1
to get global permutasi
by 1
do
insert list item list get global tmp_pesan
index get j
item segment text select list item list get global blok_pesan
index get i
start get j
length 1
set global tmp_pesan2 to copy list list get global tmp_pesan
for each k2 from 1
to get global permutasi
by 1
do
set global indeks to select list item list get global tmp_kunci
index get k2
set global item to select list item list get global tmp_pesan2
index get global indeks
replace list item list get global tmp_pesan
index get k2
replacement get global item
set global tmp_pesan3 to
for each item in list get global tmp_pesan
do
set global tmp_pesan3 to join get global tmp_pesan3
get item
replace list item list get global blok_pesan
index get i
replacement get global tmp_pesan3
set global tmp_pesan to create empty list
set global tmp_pesan2 to create empty list
set global tmp_kunci to create empty list
set global tmp_pesan3 to

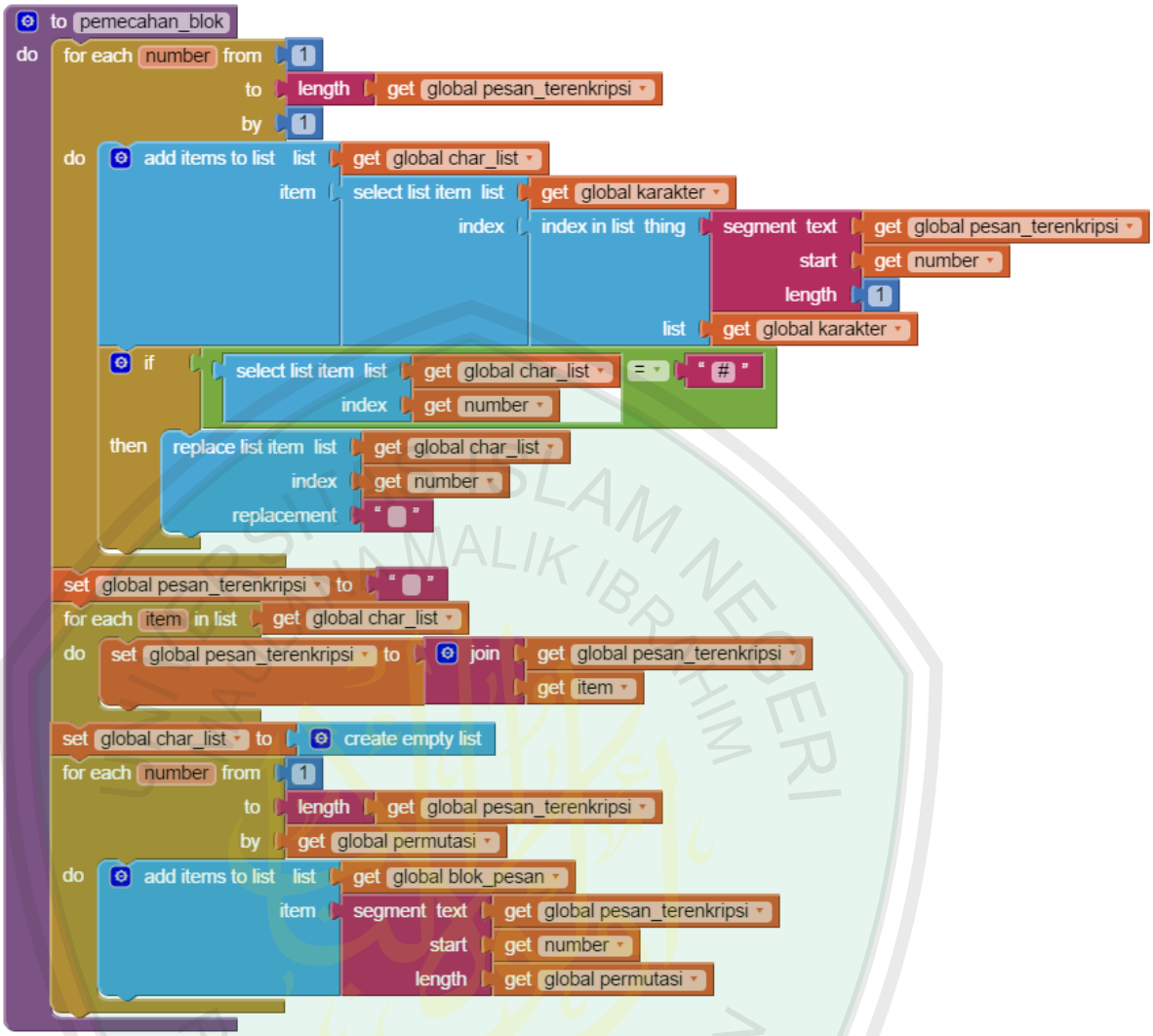

initialize global permutasi to 0
initialize global pesan_asli to ""
initialize global char_list to create empty list
initialize global blok_pesan to create empty list
initialize global tmp_pesan to create empty list
initialize global tmp_pesan2 to create empty list
initialize global tmp_kunci to create empty list
initialize global tmp_pesan3 to ""
initialize global indeks to 1
initialize global indeks2 to ""
initialize global item to ""

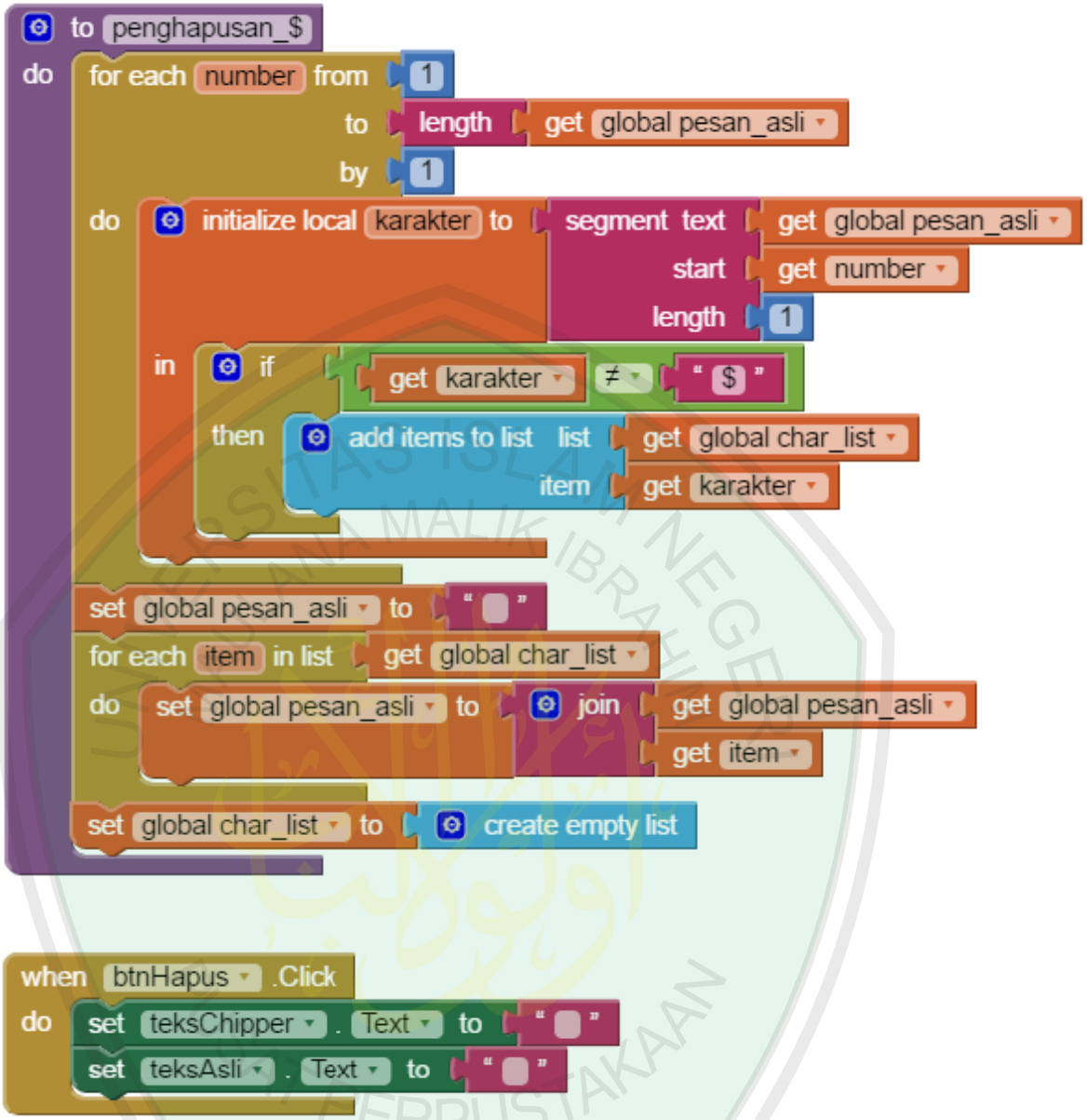
3. Proses Dekripsi Pesan

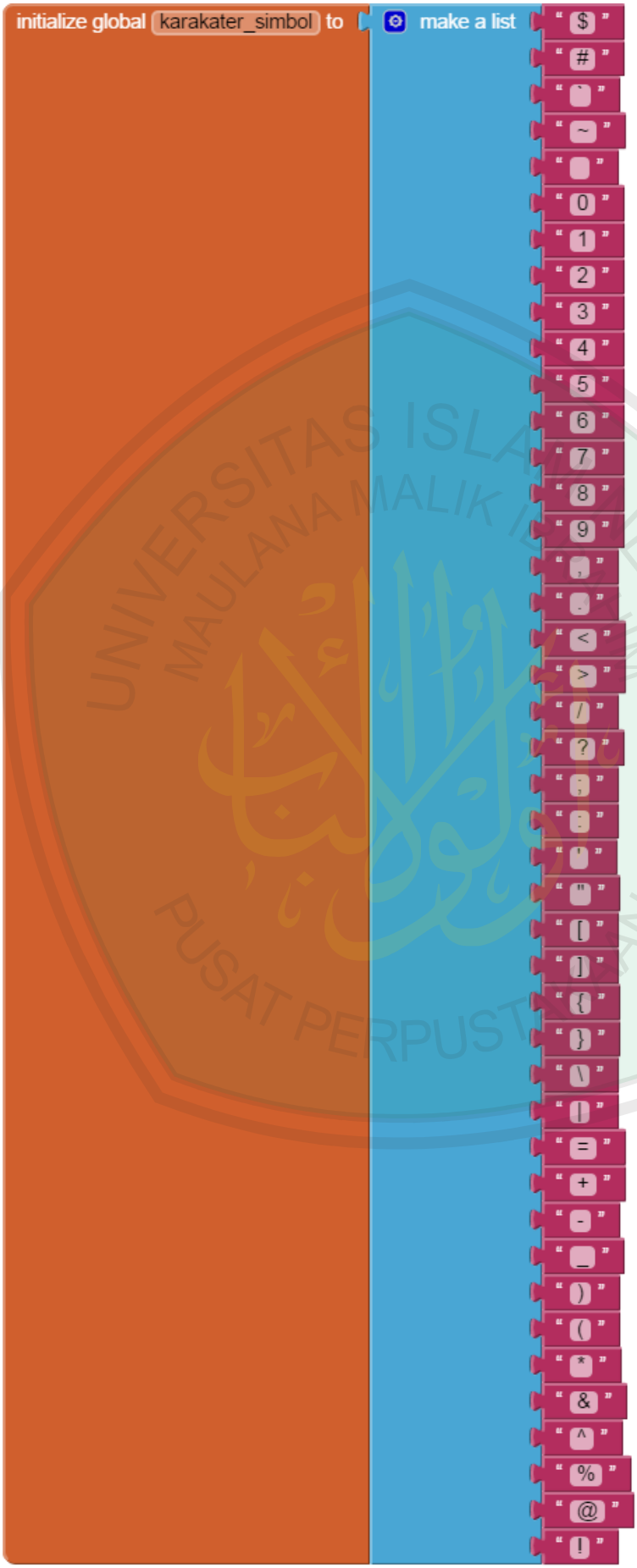


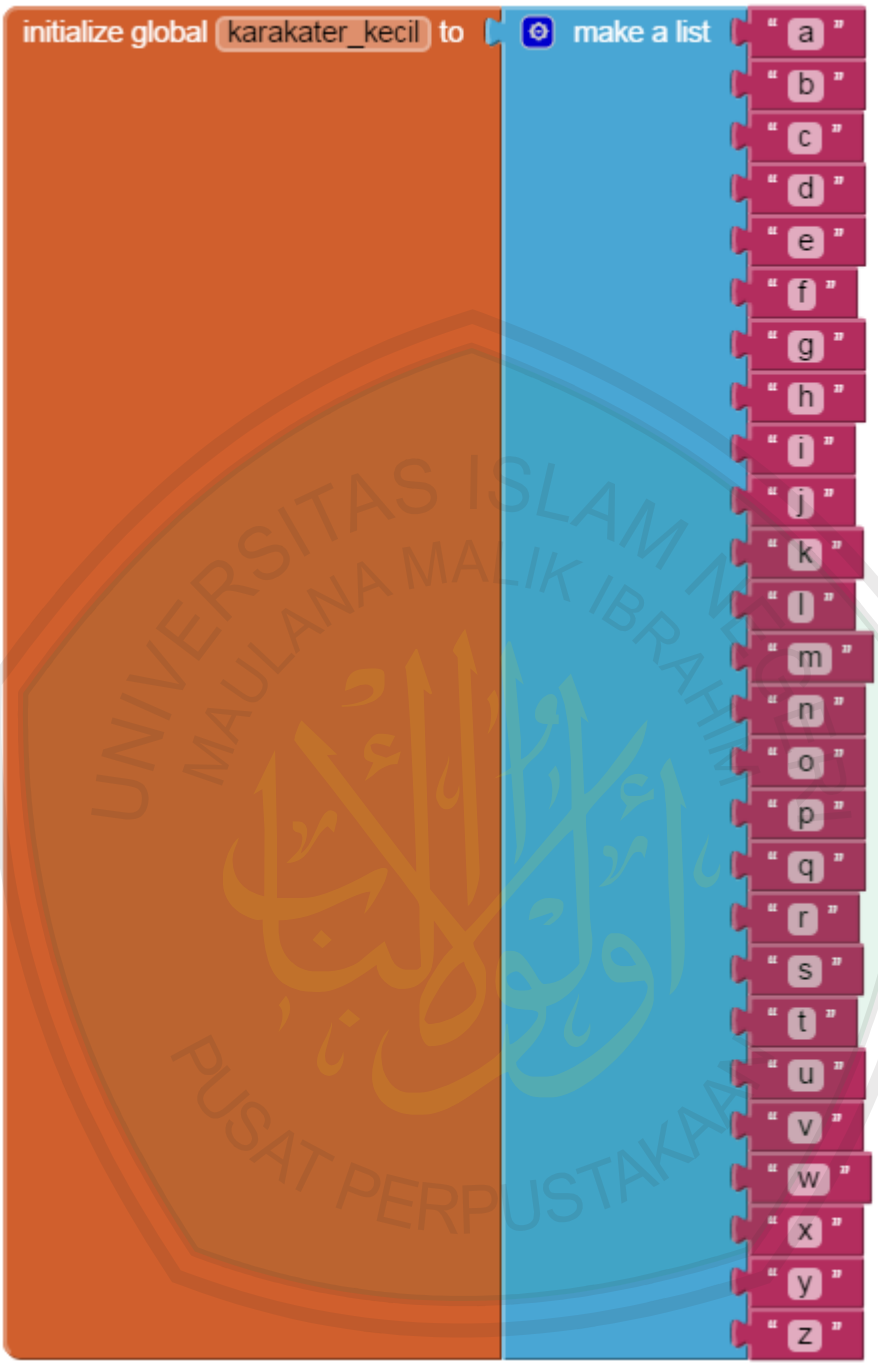

to dekripsi
do
for each i from 1
to length of list list get global blok_pesan
by 1
do
for each number from 2
to length get global kunci_lokal
by 2
do
add items to list list get global tmp_kunci
item segment text get global kunci_lokal
start get number
length 1
for each j from 1
to get global permutasi
by 1
do
insert list item list get global tmp_pesan
index get j
item segment text select list item list get global blok_pesan
index get i
start get j
length 1
set global tmp_pesan2 to copy list list get global tmp_pesan
for each k2 from 1
to get global permutasi
by 1
do
set global indeks to select list item list get global tmp_kunci
index get k2
set global item to select list item list get global tmp_pesan2
index get global indeks
replace list item list get global tmp_pesan
index get k2
replacement get global item
set global tmp_pesan3 to
for each item in list get global tmp_pesan
do
set global tmp_pesan3 to join get global tmp_pesan3
get item
replace list item list get global blok_pesan
index get i
replacement get global tmp_pesan3
set global tmp_pesan to create empty list
set global tmp_pesan2 to create empty list
set global tmp_kunci to create empty list
set global tmp_pesan3 to

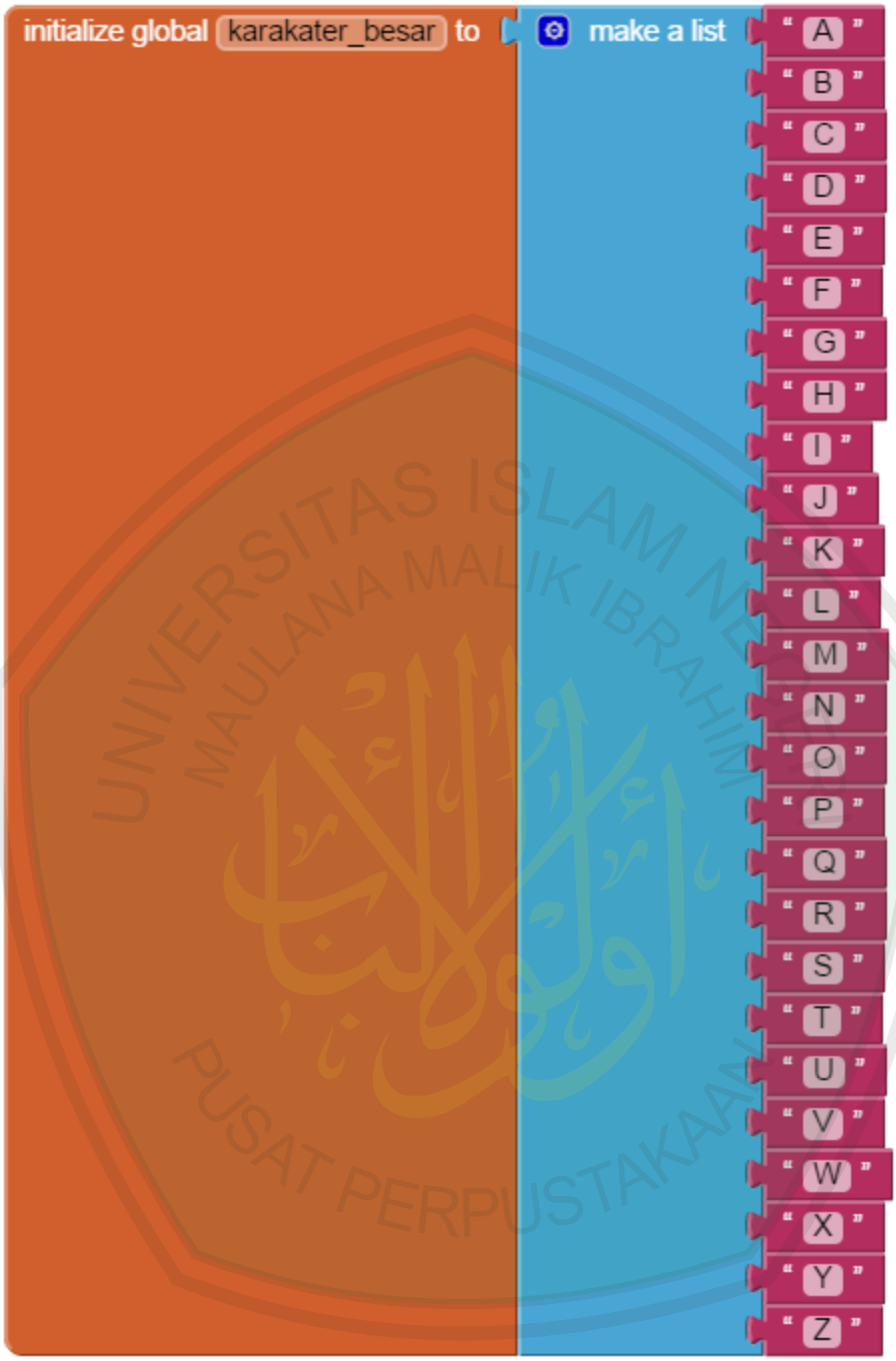

to invers_kunci
do
initialize local temp_kunci to create empty list
initialize local temp_kunci2 to create empty list
initialize local indeks to 0
initialize local item to 0
in
for each number from 1
to length get global kunci_lokal
by 1
do
add items to list list get temp_kunci
item segment text get global kunci_lokal
start get number
length 1
set temp_kunci2 to copy list list get temp_kunci
for each number from 2
to length of list list get temp_kunci
by 2
do
set item to select list item list get temp_kunci2
index get number
set indeks to index in list thing get item
list get temp_kunci2
replace list item list get temp_kunci
index get item × 2
replacement get indeks / 2
set global kunci_lokal to " "
for each item in list get temp_kunci
do
set global kunci_lokal to join get global kunci_lokal
get item


to pemecahan_blok
do
for each number from 1
to length get global pesan_terenkripsi
by 1
do add items to list list get global char_list
item select list item list get global karakter
index index in list thing segment text get global pesan_terenkripsi
start get number
length 1
list get global karakter
if select list item list get global char_list = " # "
index get number
then replace list item list get global char_list
index get number
replacement " "
set global pesan_terenkripsi to " "
for each item in list get global char_list
do set global pesan_terenkripsi to join get global pesan_terenkripsi
get item
set global char_list to create empty list
for each number from 1
to length get global pesan_terenkripsi
by get global permutasi
do add items to list list get global blok_pesan
item segment text get global pesan_terenkripsi
start get number
length get global permutasi


to penghapusan_$
do
for each number from 1
to length get global pesan_asli
by 1
do initialize local karakter to segment text get global pesan_asli
start get number
length 1
in if get karakter ≠ " $ "
then add items to list list get global char_list
item get karakter
set global pesan_asli to " "
for each item in list get global char_list
do set global pesan_asli to join get global pesan_asli
get item
set global char_list to create empty list
when btnHapus .Click
do set teksChipper . Text to " "
set teksAsli . Text to " "


initialize global karakater_simbol to
make a list
" $ "
" # "
" ` "
" ~ "
" "
" 0 "
" 1 "
" 2 "
" 3 "
" 4 "
" 5 "
" 6 "
" 7 "
" 8 "
" 9 "
" , "
" . "
" < "
" > "
" / "
" ? "
" ; "
" : "
" ' "
" " "
" ["
"] "
" { "
" } "
" \ "
" | "
" = "
" + "
" - "
" _ "
") "
" ("
" * "
" & "
" ^ "
" % "
" @ "
" ! "


initialize global karakater_kecil to
make a list
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z


initialize global karakater_besar to
make a list
" A "
" B "
" C "
" D "
" E "
" F "
" G "
" H "
" I "
" J "
" K "
" L "
" M "
" N "
" O "
" P "
" Q "
" R "
" S "
" T "
" U "
" V "
" W "
" X "
" Y "
" Z "


initialize global tmp_kunci to create empty list
initialize global permutasi to 0
initialize global pesan_asli to " "
initialize global char_list to create empty list
initialize global karakter to create empty list
initialize global tmp_pesan to create empty list
initialize global tmp_pesan2 to create empty list

RIWAYAT HIDUP

Wasiatun Riskiyah, lahir di kabupaten Probolinggo pada tanggal 07 April 1994, biasa dipanggil Acik, tinggal di Dusun Jurangdalam, Desa Kedung Rejoso RT 21 RW 10, Kecamatan Kotaanyar, Kabupaten Probolinggo. Anak pertama dari Bapak Marsuki dan Ibu Musliatin.

Pendidikan dasarnya ditempuh di SDN 1 Sumbercenteng, Kotannyar, Probolinggo dan lulus pada tahun 2006, setelah itu melanjutkan ke SMPN 1 Paiton, Paiton, Probolinggo dan lulus pada tahun 2009. Kemudian dia melanjutkan pendidikan SMAN 1 Paiton, Paiton, Probolinggo dan lulus pada tahun 2012. Pada tahun 2012 menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil jurusan Matematika.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp./Fax.(0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Wasiatun Riskiyah
NIM : 12610009
Fakultas/Jurusan: Sains dan Teknologi/Matematika
Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi
Pembimbing I : H. Wahyu H. Irawan, M.Pd
Pembimbing II : Mohammad Jamhuri, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	01 Februari 2016	Konsultasi Bab I, Bab II & Bab III	1.
2.	09 Februari 2016	Revisi Bab I, Bab II & Bab III	2.
3.	15 Februari 2016	ACC Bab I, Bab II & Bab III	3.
4.	26 Februari 2016	Konsultasi Bab I Kajian Keagamaan	4.
5.	03 Maret 2016	Konsultasi Bab II Kajian Keagamaan	5.
6.	04 April 2016	Konsultasi Bab I, Bab II & Bab III	6.
7.	07 April 2016	Konsultasi Bab I & Bab II Kajian Keagamaan	7.
8.	18 April 2016	Revisi Bab III	8.
9.	11 Mei 2016	Konsultasi Bab I, Bab II, Bab III & Bab IV	9.
10.	17 Mei 2016	Revisi Bab I, Bab II, Bab III & Bab IV	10.
11.	25 Mei 2016	ACC Kajian Keagamaan	11.
12.	26 Mei 2016	ACC Keseluruhan	12.

Malang, 26 Mei 2016
Mengetahui,
Ketua Jurusan Matematika

Dr. Abdussakir, M.Pd
NIP. 19751006 200312 1 001