# PENYANDIAN KRIPTOGRAFI METODE HILL CIPHER DAN CAESAR CIPHER DENGAN MENGGUNAKAN APPINVENTOR

**SKRIPSI**

**OLEH**
**KHOIRUN NISAK**
**NIM. 10610041**

**JURUSAN MATEMATIKA**
**FAKULTAS SAINS DAN TEKNOLOGI**
**UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM**
**MALANG**
**2015**

# PENYANDIAN KRIPTOGRAFI METODE HILL CIPHER DAN CAESAR CIPHER DENGAN MENGGUNAKAN APPINVENTOR

**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**
**Khoirun Nisak**
**NIM. 10610041**

**JURUSAN MATEMATIKA**
**FAKULTAS SAINS DAN TEKNOLOGI**
**UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM**
**MALANG**
**2015**

**PENYANDIAN KRIPTOGRAFI METODE HILL CIPHER DAN CAESAR CIPHER DENGAN MENGGUNAKAN APPINVENTOR**

**SKRIPSI**

**Oleh**
**Khoirun Nisak**
**NIM. 10610041**

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 06 Juni 2015

| Pembimbing I, | Pembimbing II, |
|---|---|
| H. Wahyu H. Irawan, M.Pd | Dr. H. Imam Sujarwo, M.Pd |
| NIP. 19710420 200003 1 003 | NIP. 19630502 198703 1 005 |

Mengetahui,
Ketua Jurusan Matematika

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

**PENYANDIAN KRIPTOGRAFI METODE HILL CIPHER DAN CAESAR CIPHER DENGAN MENGGUNAKAN APPINVENTOR**

**SKRIPSI**

**Oleh**
**Khoirun Nisak**
**NIM. 10610041**

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Si)
Tanggal 25 Juni 2015

| | | |
|---|---|---|
| Penguji Utama | : Mohammad Jamhuri, M.Si | ……. |
| Ketua Penguji | : Dr. Abdussakir, M.Pd | ……. |
| Sekretaris Penguji | : H. Wahyu H. Irawan, M.Pd | ……. |
| Anggota Penguji | : Dr. H. Imam Sujarwo, M.Pd | ……..... |

Mengetahui,
Ketua Jurusan Matematika

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

## PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Khoirun Nisak

NIM : 10610041

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Penyandian Kriptografi Metode Hill Cipher dan Caesar Cipher dengan Menggunakan Appinventor.

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 dan 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, 06 Juni 2015
Yang membuat pernyataan,

Khoirun Nisak
NIM. 10610041

**MOTO**

"Jangan tinggalkan membaca al-Quran, semakin banyak membaca al-Quran maka urusanmu semakin mudah" (pesan seorang guru kepada muridnya)

**PERSEMBAHAN**

Dengan rasa syukur *Alhamdulillah* karya ini dipersembahkan untuk kedua orang tua penulis, ayah Sapawi dan ibu Siti Rokayah, dan juga adik-adik tersayang Imro'atul Khasanah dan Muhammad Ali Mustofa yang selalu memberikan do'a dan semangat yang berarti bagi penulis

## KATA PENGANTAR

*Assalamu'alaikum wr.wb.*

Segala puji bagi Allah Swt. yang telah melimpahan rahmat, taufik serta hidayah-Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul **"Penyandian Kriptografi Metode Hill Cipher dan Caesar Cipher dengan Menggunakan Appinventor"** ini dengan baik. Sholawat serta salam semoga tetap tercurahkan kepada Nabi Muhammad Saw. yang telah membimbing dari zaman kegelapan menuju zaman yang terang yakni agama Islam.

Selesainya skripsi ini tak luput dari bantuan dari berbagai pihak, baik secara moril maupun materiil. Ucapan terima kasih penulis sampaikan kepada:

1. Prof. Dr. H. Mudjia Raharjo, M.Si, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. drh. Hj. 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. Dr. Usman Pagalay, M.Si, 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 dan arahannya dengan penuh kesabaran selama penulisan skripsi ini.

6. Dr. H. Imam Sujarwo, M.Pd, selaku dosen pembimbing II yang telah memberikan saran dan bimbingan dengan penuh kesabaran selama penulisan skripsi ini.
7. Seluruh dosen Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang, khususnya dosen Jurusan Matematika dan seluruh staf serta karyawan.
8. Abah Yahya Dja'far dan Ibu Syafiah Yahya, selaku pengasuh Pondok Pesantren Putri Al-Hikmah Al-Fathimiyah yang senantiasa memberi pengarahan kepada penulis selama menjadi santri.
9. Ayah dan Ibu tercinta yang telah memberikan do'a, dukungan, dan semangat kepada penulis.
10. Adik-adik tersayang yang selalu mengajarkan untuk bersabar dan tegas mengambil setiap keputusan.
11. Semua teman-teman seperjuangan selama di bangku perkuliahan yang selalu memberikan semangat, inspirasi, dan kekompakannya yang tak terlupakan.
12. Seluruh keluarga besar santri Pondok Pesantren Putri Al-Hikmah Al-Fathimiyyah yang selalu memberi motivasi apa artinya sebuah kehidupan dan yang selalu ada saat senang maupun sedih.
13. Seluruh keluarga besar anggota Yayasan Baitul Maal BRI yang selalu memberikan arti sebuah perjuangan.
14. Semua pihak yang tidak mungkin penulis sebut satu persatu, penulis ucapkan terimakasih atas bantuannya.

Akhirnya, penulis menyadari masih terdapat banyak kekurangan, sehingga kritik dan saran yang membangun sangat diharapkan untuk penelitian selanjutnya.

Semoga skripsi ini dapat bermanfaat serta menambah wawasan keilmuan khususnya di bidang matematika. Amin.

*Wassalamu'alaikum wr.wb.*

Malang, Juni 2015

Penulis

## DAFTAR ISI

**BAB III METODE PENELITIAN**



**BAB IV PEMBAHASAN**



**BAB V PENUTUP**

## DAFTAR GAMBAR

## DAFTAR LAMPIRAN

# ABSTRAK

Nisak, Khoirun. 2015. **Penyandian Kriptografi Metode Hill Cipher dan Caesar Cipher dengan Menggunakan Appinventor.** Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) H. Wahyu H. Irawan, M.Pd. (II) Dr. H. Imam Sujarwo, M.Pd.

**Kata kunci:** Keamanan, Rahasia, Kriptografi, Hill Cipher, dan Caesar Cipher.

Keamanan dan kerahasiaan suatu data di zaman sekarang ini terutama bagi suatu perusahaan atau organisasi tertentu merupakan hal yang sangat penting. Ada data yang bersifat rahasia dan yang tidak rahasia, artinya data yang bersifat rahasia akan sangat dijaga dan diperhatikan sedangkan data yang bersifat tidak rahasia biasanya tidak terlalu diperhatikan dan akan dengan mudah orang dapat menggandakan. Melihat wacana tersebut untuk menjaga keamanan data yang bersifat rahasia diperlukan suatu sistem yang digunakan untuk menyandikan data-data yang berupa *file* dan membukanya diperlukan kunci rahasia yang sifatnya sulit untuk dideteksi orang yang tidak berhak membukanya. Dalam penelitian ini membahas konsep matematika yang dapat digunakan untuk menjaga keamanan data yaitu ilmu kriptografi. Dalam kriptografi banyak metode untuk mengamankan data, namun penelitian ini membahas metode Hill Cipher dan Caesar Cipher. Simulasi pada penelitian menggunakan aplikasi Appinventor.

Metode yang digunakan dalam penelitian ini adalah deskriptif kualitatif dengan menggunakan metode kepustakaan. Penelitian ini bertujuan untuk mengetahui perbandingan perbedaan pada metode Hill Cipher yang membahas perbedaan kunci matriks $2x2$, $3x3$, dan $4x4$. Sedangkan pada metode Caesar Cipher membahas perbedaan banyak blok, banyak karakter tiap bloknya, dan peracakan kunci yang digunakan.

Berdasarkan penelitian ini dengan perbedaan-perbedaan yang ada pada proses di metode Hill Cipher dan Caesar Cipher diperoleh hasil yang tidak berbeda atau sama. Perintah untuk menjaga rahasia juga sudah dianjurkan dan diperintahkan di dalam al-Quran salah satunya yang terdapat di dalam surat an-Nisa' ayat 58.

Untuk penelitian selanjutnya, disarankan menggunakan program komputer yang lebih baik atau dengan menggunakan metode kriptografi modern yang lebih kompleks.

## ABSTRACT

Nisak, Khoirun. 2014. **Hill Cipher and Caesar Cipher Method of Cryptography Coding Using Appinventor**. Thesis. Department of Mathematic, Faculty of Science and Technology, Islamic State University of Maulana Malik Ibrahim Malang. Advisors: (I) H. Wahyu H. Irawan, M.Pd. (II) Dr. H. Imam Sujarwo, M.Pd.

**Key Words:** Safety, Secret, Cryptography, Hill Cipher, and Caesar Cipher.

Nowadays, safety and confidentiality of data especially for a company or organization are very important. There is data that is confidential and non-confidential, means that the confidential data will be maintained and cared, while the data which is not confidential usually not too concerned and people will be able to duplicate it easily. Bassed on these fact that, to maintain the safety of confidential data we need a system that is used to encode the data in the form of a file and a secret key which is difficult to be detected by unauthorized. This study discusses the mathematical concepts that can be used to maintain the safety of the data, namely cryptography. In cryptographiy, there are some method to secure the data, but this study focuses only on the discussion of the method of Hill Cipher and Caesar Cipher. The simulation of this thesis uses Appinventor aplication.

This study used descriptive qualitative method in the form of literature. This study aimed to compare the difference between the method of Hill Cipher which discusses about difference of key matrix $2x2$, $3x3$, dan $4x4$. with the method of Caesar Cipher which discusses about the differences of number of blocks, the blocks, and the number of each characters and randomization of the key used.

The result of this study stated that the differences of the existing process of Hill Cipher and Caesar Cipher obtained the same result. Related to the safety command, it is also been encouraged and instructed in the holly Quran, surah an-Nisa' 58.

For further researcher, the author suggests to use computer program or use more complex modern cryptographic methods.

# ملخص

**نساء، خير.** ٢٠١٥. **طرق التشفير Hill Cipherو Caesar Cipher باستخدام Appinventor**.بحث جامعي.االشعبة قسم الرياضيات كلية العلوم والتكنولوجية، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشريفين: (١) الحاج وحي هينكي إروان، الماجستير (٢) الدكتور الحاج إمام سوجروواو, الماجستير.

**الكلمات الاساسية:** الأمن، سر، تشفير، هيل جفتير وقيصر جفتير.

أمن وسرية البيانات في عصر اليوم وخاصة بالنسبة للشركة أو المؤسسة مهم جدا. هناك بيانات غير سرية وغير سرية، وهذا يعني البيانات السرية سيتم الحفاظ عليها والعناية بها في حين أن البيانات ليست سرية عادة لا يشعر بقلق كبير، وسوف بسهولة يمكن للناس مكررة.رؤية الخطاب للحفاظ على أمن البيانات السرية التي نحن بحاجة إلى نظام يستخدم لترميز البيانات في شكل ملف وفتحه في حاجة إلى المفتاح السري التي يصعب الكشف عن الأشخاص الذين لا يحق لفتحه. في هذه الدراسة تناقش المفاهيم الرياضية التي يمكن استخدامها للحفاظ على أمن البيانات هو علم التشفير، في العديد من وسائل التشفير لتأمين البيانات، ولكن يناقش هذه الدراسة طريقة Hill Cipherو Caesar Cipher. المحاكة في هذا البحث باستخدام تطبيقAppinventor.

الطريقة المستخدمة في هذا البحث هو النوعية باستخدام أساليب الأدب وصفية. هدفت هذه الدراسة إلى مقارنة الفرق هو في طريقة Hill Cipher مناقشة رئيسيا ٢x٢الفرق المصفوفة، ٣x٣و ٤x٤، في حين أن أسلوب Caesar Cipher مناقشة الاختلافات في عدد من كتل، والكتل وعدد من الشخصيات في نطق مفتاح المستخدمة.

نتائج هذه الدراسة ويتم الحصول على الخلافات القائمة في عملية وطريقة Hill Cipher وCaesar Cipher كانت النتائج لا تختلف أو نفس. كما تم تشجيع الأوامر لالسرية وتعليمات في القرآن الوارد في الرسالة سورة النساء "الآية ٥٨".

لمزيد من البحث، فمن المستحسن استخدام برنامج كمبيوتر أفضل أو باستخدام طرق التشفير الحديثة هي أكثر تعقيدا.

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Masalah keamanan dan kerahasiaan data di zaman sekarang ini terutama bagi suatu perusahaan atau organisasi tertentu sangat penting. Karena data dibagi dua jenis yaitu data yang bersifat rahasia dan data yang bersifat tidak rahasia, artinya data yang bersifat rahasia akan sangat dijaga dan diperhatikan sedangkan data yang bersifat tidak rahasia biasanya tidak terlalu diperhatikan dan akan dengan mudah orang dapat menggandakan. Melihat wacana tersebut untuk menjaga keamanan data yang bersifat rahasia diperlukan suatu sistem yang digunakan untuk menyandikan data-data yang berupa *file* dan membukanya diperlukan kunci rahasia yang sifatnya sulit untuk dideteksi orang yang tidak berhak membukanya.

Al-Quran juga menganjurkan untuk menjaga rahasia yang harus disimpan yaitu terdapat di dalam surat an-Nisa' ayat 58 yang berbunyi:

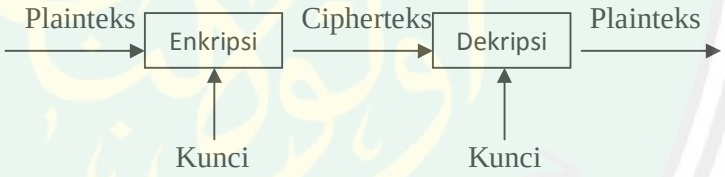
إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

*"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-Nisa'/4:58).*

Keamanan data pada lalu lintas jaringan adalah suatu hal yang diinginkan semua orang untuk menjaga *privacy*. Supaya data yang dikirim aman dari orang yang tidak bertanggung jawab dengan menyembunyikan data memakai algoritma

kriptografi. Dalam ilmu matematika terdapat konsep yang disebut kriptografi. Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua *kripto* dan *graphia*, kripto 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 ke tempat yang lain (Ariyus, 2006:9).

Di dalam buku Rinaldi Munir (2012) disebutkan bahwa pesan yang dapat dibaca dinamakan plainteks (teks asli yang bisa dibaca), sedangkan teks yang sudah disandikan dinamakan cipherteks (teks yang disamarkan atau tidak dapat dibaca). Kemudian proses untuk mengubah dari plainteks ke cipherteks disebut enkripsi sedangkan proses kebalikannya yaitu mengembalikan teks ke bentuk semula atau bentuk asli disebut dekripsi. Di bawah ini akan ditunjukkan gambaran proses penyandian enkripsi dekripsi:




Gambar 1.1 Proses Penyandian
(sumber: Munir, 2012)

Menurut Ariyus (2008) berdasarkan kunci yang dipakai, algoritma kriptografi dibagi menjadi tiga yaitu algoritma simetri, algoritma asimetri, dan fungsi hash. Kemudian kriptografi ada dua jenis yaitu kriptografi klasik dan kriptografi modern. Di dalam kriptografi klasik ada beberapa teknik yaitu: teknik substitusi, teknik permutasi, teknik *blocking*, teknik ekspansi, dan teknik perampatan. Di dalam teknik substitusi juga dibagi beberapa macam cara yaitu: Caesar Cipher, Playfair Cipher, Shift Cipher, Hill Cipher, dan Vinegere Cipher. Kriptografi klasik merupakan awal dari kriptografi modern, jadi untuk memahami

lebih dalam tentang kriptografi modern lebih baik memahami konsep dasar terlebih dahulu tentang kriptografi klasik.

Berdasarkan dari latar belakang tersebut maka peneliti mengangkat judul skripsi yang berjudul "Penyandian Kriptografi Metode Hill Cipher dan Caesar Cipher dengan Menggunakan Appinventor."

## 1.1 Rumusan Masalah

Berdasarkan dari latar belakang tersebut peneliti membuat rumusan masalah sebagai berikut:

1. Bagaimana deskripsi Hill Cipher dengan perbedaan kunci matriks?
2. Bagaimana deskripsi Caesar Cipher dengan perbedaan jumlah blok, karakter, dan peracakan kunci?
3. Bagaimana program Hill Cipher dan Caesar Cipher dalam mengolah pesan?
4. Bagaimana keterkaitan antara agama dengan penyandian?

## 1.2 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat peneliti maka tujuan dari penelitian ini adalah

1. Untuk mengetahui deskripsi Hill Cipher dengan perbedaan kunci matriks.
2. Untuk mengetahui deskripsi Caesar Cipher dengan perbedaan jumlah blok, karakter, dan peracakan kunci
3. Untuk membuat program Hill Cipher dan Caesar Cipher untuk mengolah pesan.
4. Untuk mengetahui keterkaitan antara agama dengan penyandian.

### 1.3 Manfaat Penelitian

Peneliti berharap bahwa dalam melakukan penelitian ini dapat memberi manfaat antara lain:

a. Bagi peneliti:
   1. Dapat menambah wawasan tentang penyandian dan kajian agamanya di dalam al-Quran.
   2. Dapat memperkaya sumber pengetahuan tentang kriptografi khususnya sesuai penelitian ini yaitu masalah Hill Cipher dan Caesar Cipher selanjutnya akan dapat berguna dalam menjaga keamanan data khususnya yang bersifat rahasia.
   3. Dapat mengimplementasikan Hill Cipher dan Cesar Cipher dengan program.
b. Bagi pembaca:

   Dapat digunakan sebagai bahan perbandingan bagi peneliti selanjutnya yang ingin membahas lebih lanjut.
c. Bagi lembaga:

   Dapat digunakan sebagai rujukan untuk penelitian selanjutnya.

### 1.4 Batasan Masalah

Peneliti membatasi masalah dalam penelitian ini agar tidak bias dalam masalah yang akan dibahas yaitu:

1. Pada metode Hill Cipher hanya membahas perbedaan hasil yang menggunakan kunci matriks $2x2$, $3x3$, dan $4x4$. Karena kunci pada metode Hill Cipher ini berupa matriks nxn, maka dari itu peneliti membatasi dengan memberi contoh hanya menggunakan matriks $2x2$, $3x3$, dan $4x4$.

2. Pada metode Caesar Cipher ada tiga bagian yaitu blok, karakter, dan zig-zag, namun dalam penelitian ini hanya membahas bagian blok saja.

### 1.5 Sistematika Penulisan

Dalam penelitian ini sistematika penulisannya terdiri dari empat bab dan masing-masing dari empat bab akan dibagi ke dalam subbab dengan rumusan sebagai berikut:

Bab I Pendahuluan

Pendahuluan ini terdapat latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Bagian kajian pustaka ini terdiri dari teori-teori atau konsep-konsep yang dapat mendukung di dalam penelitian ini. Teori atau konsep tersebut meliputi konsep kriptografi, konsep matriks, operasi matriks, invers matriks, dan konsep modulo.

Bab III Metode Penelitian

Bagian metode penelitian ini menjelaskan tentang urutan dan langkah-langkah penulis melakukan penelitian yaitu meliputi proses pengambilan data, analisis data, dan menarik kesimpulan.

Bab IV Pembahasan

Bagian pembahasan ini akan menjelaskan dan menguraikan secara keseluruhan langkah-langkah yang disebutkan dalam metode penelitian dan menjawab rumusan masalah.

Bab V Penutup

Bagian penutup ini berisi kesimpulan hasil pembahasan dan saran yang ingin disampaikan peneliti.

# BAB II

# KAJIAN PUSTAKA

## 2.1 Kriptografi

### 2.1.1 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang Mesir untuk mengirim pesan ke pasukan militer yang berada di lapangan agar pesan tersebut tidak terbaca oleh pihak musuh walaupun kurir pembawa pesan tertangkap oleh musuh. Dikisahkan, pada zaman Romawi kuno pada suatu saat, ketika Julius Caesar ingin mengirimkan pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir, karena pesan tersebut bersifat rahasia, Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka di jalan. 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 yang teracak tersebut, yang dilakukan Julius Caesar adalah mengganti semua susunan alfabet dari a,b,c yaitu a menjadi d, b menjadi e, c menjadi f, dan seterusnya (Ariyus, 2006:9).

Dari ilustrasi tersebut, beberapa istilah kriptografi dipergunakan untuk menandai aktivitas-aktivitas rahasia dalam mengirim pesan. Apa yang dilakukan Julius Caesar yang mengacak pesan, disebut dengan enkripsi. Pada saat sang jenderal merapikan pesan yang teracak itu, proses itu disebut dekripsi. Pesan awal

yang belum diacak dan pesan yang telah dirapikan disebut plainteks, sedangkan pesan yang telah diacak disebut cipherteks (Ariyus, 2006:10).

### 2.1.2 Komponen Kriptografi

Pada dasarnya komponen kriptografi 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. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
3. *Kunci* adalah 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-karakter 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, dsb) atau yang disimpan di dalam media perekaman (kertas, *storage*, dsb).
7. *Cryptanalysis* bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks asli tanpa harus 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 kripnatalis. 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).

### 2.1.3 Macam-macam Algoritma Kriptografi

Ariyus (2008) menyatakan bahwa algoritma kriptografi dibagi menjadi tiga bagian berdasarkan 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.

**1. Algoritma Simetri**

Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Algoritma ini sudah ada

sejak 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. Algoritma yang memakai kunci simetri di antaranya adalah:

1. Data Encryption Standard (DES).
2. RC2, RC4, RC5, RC6.
3. International Data Encryption Algorithm (IDEA).
4. Advanced Encryption Standard (AES).
5. One Time Pad (OTP).
6. A5, dan lain sebagainya (Ariyus, 2008:44).

**2. Algoritma Asimetri**

Algoritma asimetri sering juga disebut dengan algoritma kunci *public*, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi adalah 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 mendekripsikannya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut (Ariyus, 2008:45).

**3. Fungsi Hash**

Fungsi hash sering disebut fungsi hash satu arah *(one-way function), message 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 tetap. Fungsi hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang yang diinginkan (Ariyus, 2008:46).

### 2.1.4 Kriptografi Klasik dan Modern

Kriptografi klasik merupakan suatu algoritma yang menggunakan satu 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).

### 2.1.6 Kriptografi Klasik Teknik Substitusi

Kriptografi klasik teknik substitusi ada beberapa macam, antara lain:

**1. Caesar Cipher**

Substitusi kode yang pertama dalam dunia penyandian terjadi pada pemerintah Julius Caesar yang dikenal dengan kode Kaisar, dengan mengganti posisi huruf awal dari alfabet atau disebut juga dengan algoritma ROT3.

**Caesar Cipher (ROT3)**

| Plain Text | Encoded Text |
|---|---|
| ABC | DEF |
| Hello | Khoor |
| Attack | Dwwdfn |

Perhatikan contoh berikut:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | q | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Menjadi:

| D | E | F | G | H | I | J | K | L | M | N | O | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

| Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 |

Jika penggeseran yang dilakukan sebanyak tiga kali maka kunci untuk dekripsinya adalah 3. Penggeseran kunci yang dilakukan tergantung keinginan pengirim pesan (Ariyus, 2008:50).

Kemudian pada perkembangannya algoritma kode caesar memberikan suatu gagasan baru untuk menggunakan kunci lain yang disebut *polyalphabetic*. Kunci bisa jadi nama, alamat atau apa saja yang diinginkan oleh pengirim pesan. Caesar Cipher dengan menggunakan satu kunci atau bisa disebut dengan

substitusi deret campur kata kunci, yang perlu diingat adalah tidak ada perulangan huruf (Ariyus, 2006:20).

Menggunakan satu kunci:

K1

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | O | N | Y | A | R | I | U | S | B | C | E | F | G | H | J | K | L | M | P | Q | T | V | W | X | Z |

Plainteks : KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA

Kunci : DONY ARIYUS

Proses :

| Plainteks | K | E |
|---|---|---|
| Kunci | C | A |

Dan seterusnya

Cipherteks : CAGDSCDGUDLIDOOFFAFOQDPLDCXDPCANSEFAGYAL SPD

Menggunakan dua kunci:

K1

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | O | N | Y | A | R | I | U | S | B | C | E | F | G | H | J | K | L | M | P | Q | T | V | W | X | Z |

K2

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | H | I | L | D | V | A | N | B | E | F | G | J | K | M | O | P | Q | R | S | T | U | W | X | Y | Z |

Plainteks : KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA

Kunci 1 : DONY ARIYUS

Kunci 2 : CHILDVANIA

Proses :

| Plainteks | K | E |
|---|---|---|
| Kunci 1 | C | A |
| Kunci 2 | I | C |

Dan seterusnya

Cipherteks : ICALRILTTIGBLMMVVCUMPLOGLIYLOICKRDVCAYCG ROL

Menggunakan lebih dari satu kunci:

K1

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | O | N | Y | A | R | I | U | S | B | C | E | F | G | H | J | K | L | M | P | Q | T | V | W | X | Z |

K2

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | H | I | L | D | V | A | N | B | E | F | G | J | K | M | O | P | Q | R | S | T | U | W | X | Y | Z |

K3

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M | U | T | H | I | A | C | R | B | D | E | F | G | J | K | L | N | O | P | Q | S | V | W | X | Y | Z |

Plainteks : KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA

Kunci 1 : DONY ARIYUS

Kunci 2 : CHILDVANIA

Kunci 3 : MUTHIA CITRA

Proses :

| Plainteks | K | E |
|---|---|---|
| Kunci 1 | C | A |
| Kunci 2 | I | C |
| Kunci 3 | B | T |

Dan seterusnya

Cipherteks : CAGDSCCKNCQAMUVGGIFOQDPLCFYCSF ITBFGIGYAL SPCXXXX (Ariyus, 2006:20).

Dengan menggunakan lebih dari satu kunci, bisa menggunakan metode pendistribusian kunci-kunci yang ada. Metode ini terdiri dari tiga bagian, yaitu blok, karakter, dan zig-zag.

a. Blok

Metode untuk mengenkripsi dengan menggunakan blok adalah dengan membagi jumlah teks asli menjadi blok-blok yang ditentukan, tergantung dari keinginan pengirim pesan.

Contoh:

Teks asli: BANJIR MERENDAM JAKARTA HARGA BAHAN POKOK NAIK.

Teks asli di atas dibagi menjadi 7 blok. Setiap blok berisi 6 karakter. Karena blok yang ketujuh tidak mencukupi maka ditambah dengan karakter “X” atau karakter lain yang diinginkan.

| BANJIR | MEREND | AMJAKA | RTAHAR | GAHABA | NPOKOK |
|---|---|---|---|---|---|
| Blok 1 | Blok 2 | Blok 3 | Blok 4 | Blok 5 | Blok 6 |

| NAIKXX |
|---|
| Blok 7 |

Kunci 1: DONY ARIYUS

Kunci 2: YOGYAKARTA

Kunci 3: KRIPTOGRAFI

K1

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | O | N | Y | A | R | I | U | S | B | C | E | F | G | H | J | K | L | M | P | Q | T | V | W | X | Z |

K2

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Y | O | G | A | K | R | T | B | C | D | E | F | H | I | J | L | M | N | P | Q | S | U | V | W | X | Z |

K3

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K | R | I | P | T | O | G | A | F | B | C | D | E | H | J | L | M | N | Q | S | U | V | W | X | Y | Z |

Dengan aturan K1 digunakan pada blok pertama, K2 blok kedua, K3 blok ketiga, dan seterusnya. Atau juga bisa dipakai untuk mengenkripsi dua blok sekaligus.

Dari contoh di atas diperoleh teks kode berikut:

ODGBSI HKNKIA KEBKCK LPDUDL TYOYBY HLJCJC
K1 K2 K3 K1 K2 K3

GDSCWW
K1

Dari contoh tersebut diperoleh teks kode:

" ODGBSIHKNKIAKEBKCKLPDUDLTYOYBYHLJCJCGDSCWW"

b. Karakter

Metode ini menggunakan pendistribusian perkarakter, hampir sama dengan metode blok. Metode ini enkripsi dan dekripsi sama.

Contoh:

Teks asli: BANJIR MERENDAM JAKARTA HARGA BAHAN POKOK NAIK.

Kunci 1: DONY ARIYUS

Kunci 2: YOGYAKARTA

Kunci 3: KRIPTOGRAFI

K1

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | O | N | Y | A | R | I | U | S | B | C | E | F | G | H | J | K | L | M | P | Q | T | V | W | X | Z |

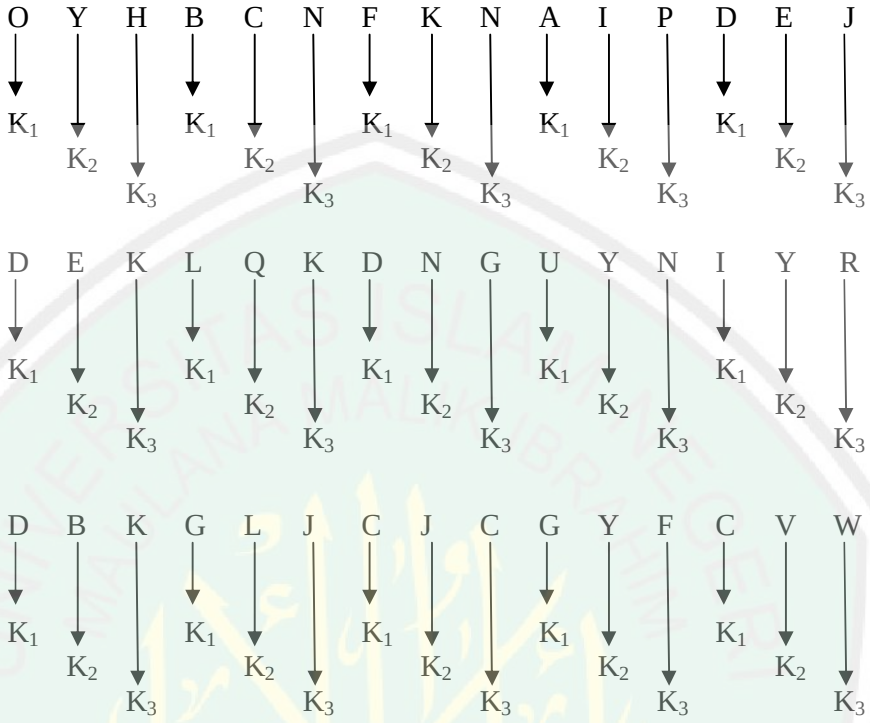
K2

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Y | O | G | A | K | R | T | B | C | D | E | F | H | I | J | L | M | N | P | Q | S | U | V | W | X | Z |

K3

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K | R | I | P | T | O | G | A | F | B | C | D | E | H | J | L | M | N | Q | S | U | V | W | X | Y | Z |

Setiap karakter memakai kunci berbeda yaitu K1, K2, K3, K1, K2, dan seterusnya. Sehingga diperoleh hasil sebagai berikut:




c. Zig-zag

Pendistribusian dengan metode zig-zag dilakukan dengan menukarkan huruf asli dengan huruf yang sudah memakai kunci (K1) dan mencari huruf yang sama pada K2 dan K3, sehingga huruf yang menjadi teks kode adalah huruf dari persamaan C = K3 dan sebaliknya. Pada metode ini enkripsi dan dekripsi sama.

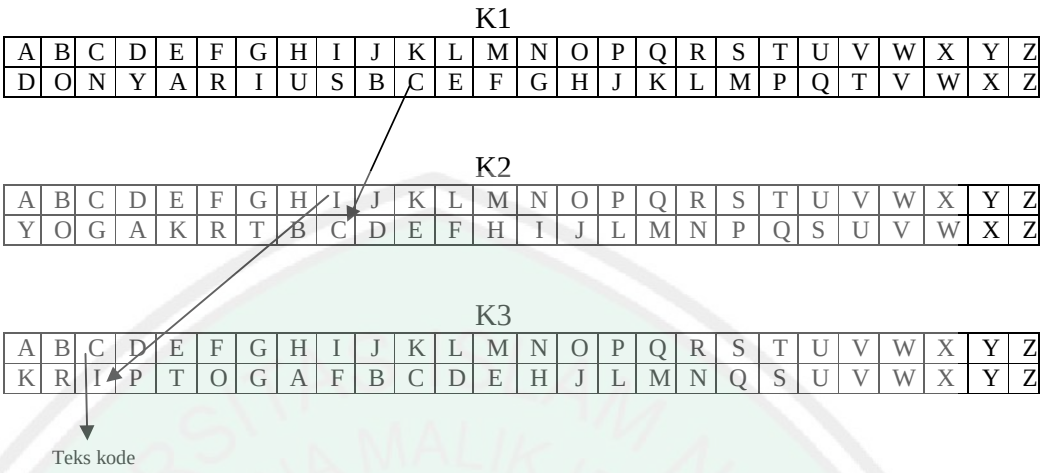
Contoh:

Teks asli: KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA.

Kunci 1: DONY ARIYUS

Kunci 2: YOGYAKARTA

Kunci 3: KRIPTOGRAFI




Sehingga dari teks asli:

KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA.

Diperoleh teks kode:

CLKOUCOK VODRO JJP PLPJEOT DOCYOT CLBUA PLKHLDUTO

(Ariyus, 2008:56).

**2. Hill Cipher**

Hill cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula (Widyanarko, 2009). Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks n x n

dengan n merupakan ukuran blok. Matriks K yang menjadi kunci harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse* $K^{-1}$ sehingga: $K \cdot K^{-1} = K^{-1} \cdot K = I$

Kunci harus memiliki invers karena matriks $K^{-1}$ tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

Contoh:

**Proses Enkripsi**

Dapat dilihat bahwa matriks enkripsi pada contoh sebelumnya memiliki invers pada $Z_{26}$:

$$\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}^{-1} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$$

Karena

$$\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} = \begin{bmatrix} 11 \cdot 7 + 8 \cdot 23 & 11 \cdot 18 + 8 \cdot 11 \\ 3 \cdot 7 + 7 \cdot 23 & 3 \cdot 18 + 7 \cdot 11 \end{bmatrix}$$

$$= \begin{bmatrix} 261 & 286 \\ 182 & 131 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Dengan semua operasi aritmatika di atas dilakukan pada modulo 26.

Teks asli: JULY

Kunci : $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$ $K^{-1} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$

Kata JULY ditukarkan ke dalam bilangan menjadi 9, 20, 11, 24. Ada 2 elemen teks asli untuk dienkripsi. Selanjutnya lakukan perhitungan sebagai berikut:

$$(9, 20) \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = (99 + 60, 72 + 140) = (3, 4) \rightarrow \text{DE}$$

$$(11, 24) \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = (121 + 72, 88 + 168) = (11, 22) \rightarrow \text{LW}$$

Sehingga diperoleh teks kode: DELW

**Proses Dekripsi**

Teks kode: DELW

Kunci : $K^{-1} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$

DELW → 3 4 11 22

$(3,4)\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} = (9,20)$ dan

$(11,22)\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} = (11,24)$

Didapatkan teks asli seperti semula yaitu JULY.

Dekripsi hanya mungkin dilakukan jika matriks K memiliki invers. Suatu matriks K memikili invers jika dan hanya jika determinannya tidak nol.

**3. Playfair Cipher**

Kunci dari Playfair Cipher adalah penggunaan matriks 5 x 5 (dengan masukan terdiri dari 25 karakter dan membuang J yang ada di dalam alfabet). Dengan begitu kunci yang digunakan ada 25 alfabet. Jumlah kemungkinan kunci pada kode playfair: 25!=15.511.210.043.330.985.984.000.000 (Ariyus, 2008:72).

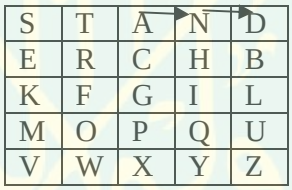
| | | | | |
|---|---|---|---|---|
| S | T | A | N | D |
| E | R | C | H | B |
| K | F | G | I | L |
| M | O | P | Q | U |
| V | W | X | Y | Z |

Algoritma enkripsi/dekripsi:

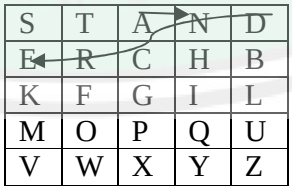
1. Aturan enkripsi dan dekripsi mengikuti aturan segiempat dan karakter yang ada terlebih dahulu dibagi menjadi dua karakter setiap bagiannya. Bila kedua huruf (karakter) tidak terletak pada satu baris atau kolom maka pergerakan karakter dimulai dari huruf kedua secara vertikal menuju karakter teks kode

yang pertama. Misalnya teks asli “di” huruf keduanya adalah “i”, maka dari “i” yang di dalam matriks bergerak vertikal mencari huruf yang sebaris dengan “d”, maka akan dijumpai karakter “n” (sebagai teks kode). Untuk karakter yang kedua, “d” mencari sisi lain seperti cara karakter “i” sehingga dijumpai karakter “i”. Jadi teks kode dari “di” adalah “nl” (Ariyus, 2008:73).


2. Bila karakter-karakter yang dienkripsi atau didekripsi berada pada kolom atau baris yang sama dan saling berdekatan maka digunakan prinsip enkripsi atau dekripsi ke bawah atau ke samping “n” adalah “d” dan karakter di samping “a” adalah “n” sehingga teks kodenya menjadi “dn”.




3. Bila karakter-karakter yang dienkripsi berada pada akhir baris maka diikuti aturan seperti nomor 2 di atas, tetapi pada kasus baris terakhir, karakter yang diambil untuk teks kodenya adalah karakter yang berada di samping (yang berarti baris pertama setelah baris tersebut).




4. Jika terdapat karakter yang kembar untuk penggunaan kode playfair maka disisipkan satu karakter di antara karakter tersebut. Sebagai contoh “aa”, “ii” menjadi “aza”, “izi” tergantung kesepakatan.

5. Untuk kepentingan analisis dari kode playfair, aturan satu, aturan dua, dan aturan tiga diberi singkatan. Aturan satu ERDL *(encipher right, decipher left)* sedangkan aturan dua dan tiga EBDA *(encipher below, decipher above)* (Ariyus, 2008:73).

Jadi dari teks asli di atas akan didapat teks kode di bawah ini:

| Plaintext | Di | da | La | Mj | iw | Ay | an | gs | eh | At |
|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | Ln | ne | Gd | Kq | fy | Nx | dn | ak | br | Na |

| Plaintext | Te | rd | Ap | At | ak | Al | ya | ng | se | ha | Tz |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | Rs | bt | Cx | Na | sg | dg | xn | ai | ek | cn | Dw |

Teks asli : DI DALAM JIWA YANG SEHAT TERDAPAT AKAL YANG SEHAT

Teks kode : LNNEGDKQFYNXDNAK BRNARSBTCXNASGDGXNAIEKCN DW (Ariyus, 2008:74).

**4. Shift Cipher**

Teknik substitusi kode shift (geser) dengan modulo 26 memasangkan bilangan ke setiap alfabet seperti a <- -> 0, B <- -> 1.... Z <- -> 25.

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | q | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**5. Vinegere**

Kode vinegere termasuk kode abjad majemuk *(polyalphabetic substitution cipher).* Teknik dari substitusi vinegere dapat dilakukan dengan dua cara, yaitu angka dan huruf.

1. Angka yaitu teknik substitusi vinegere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

2. Huruf yaitu teknik substitusi vinegere dengan menggunakan huruf dan menggunakan tabel (Ariyus, 2008:75).

## 2.2 Kajian Matematika

### 2.2.1 Pengertian Modulo

**Definisi 2.1: (Modulo)**

Misalkan *a* adalah bilangan bulat dan *m* adalah bilangan bulat > 0. Operasi a **mod** m (dibaca "*a* modulo *m*") memberikan sisa jika r dibagi dengan m. dengan kata lain, $a$ **mod** $m = r$ sedemikian hingga $a = mq + r$, dengan $0 \leq r < m$ (Munir, 2002:191).

Aritmatika modulo *(modular arithmetic)* memainkan peranan yang penting dalam perhitungan bilangan bulat, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmatika modulo adalah **mod**. Operator mod memberikan sisa pembagian. Misalnya 23 dibagi 5 memberikan hasil 4 dan sisa 3, sehingga ditulis 23 **mod** 5 = 3 (Munir, 2012:191).

### 2.2.2 Pengertian Matriks

**Definisi 2.2: (Pengertian Matriks)**

Matriks didefinisikan sebagai susunan persegi panjang dari bilangan-bilangan yang diatur dalam baris dan kolom. Susunan sebuah matriks m kali n (ditulis $mxn$) karena memiliki m baris dan n kolom (Hadley, 1992:51).

Bentuk umum dari matriks $A_{mxn}$ adalah:

$$A_{mxn} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Contoh:

Matriks $A_{3x3} = \begin{bmatrix} 2 & 4 & -5 \\ 1 & 0 & 4 \\ 8 & 6 & 1 \end{bmatrix}$

Matriks $A_{1x3} = [4 \quad 6 \quad 8]$

Matriks $A_{2x2} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

**Definisi 2.2 (Kesamaan Matriks)**

Dua matriks dikatakan sama jika kedua matriks tersebut mempunyai ukuran yang sama dan entri-entri yang bersesuaian dalam kedua matriks tersebut sama (Anton, 1987:23).

Contoh:

Jika $A = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \quad B = \begin{bmatrix} 2 & 1 \\ 3 & 5 \end{bmatrix}$

Maka $A = B$

### 2.2.3 Operasi Matriks

**Definisi 2.2 (Penjumlahan Matriks)**

Jika $A$ dan $B$ adalah sebarang dua matriks yang ukurannya sama, maka jumlah $A+B$ adalah matriks yang diperoleh dengan menambahkan bersama-sama entri yang bersesuaian dalam kedua matriks tersebut. Matriks-matriks yang ukurannya berbeda tidak dapat ditambahkan (Anton, 1987:23).

Contoh: $A = \begin{bmatrix} 2 & 1 & 0 & 3 \\ -1 & 0 & 2 & 4 \\ 4 & -2 & 7 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 4 & 3 & 5 & 1 \\ 2 & 2 & 0 & -1 \\ 3 & 2 & -5 & 5 \end{bmatrix}$

Maka $A + B = \begin{bmatrix} 2 & 1 & 0 & 3 \\ -1 & 0 & 2 & 4 \\ 4 & -2 & 7 & 0 \end{bmatrix} + \begin{bmatrix} 4 & 3 & 5 & 1 \\ 2 & 2 & 0 & -1 \\ 3 & 2 & -5 & 5 \end{bmatrix}$

$$= \begin{bmatrix} 2+4 & 1+3 & 0+5 & 3+1 \\ -1+2 & 0+2 & 2+0 & 4+(-1) \\ 4+3 & -2+2 & 7+(-5) & 0+5 \end{bmatrix} = \begin{bmatrix} 6 & 4 & 5 & 4 \\ 1 & 2 & 2 & 3 \\ 7 & 0 & 2 & 5 \end{bmatrix}$$

**Definisi 2.3 (Perkalian Matriks)**

Jika $A$ adalah suatu matriks dan $c$ adalah suatu skalar, maka hasil kali *(product)* $cA$ adalah matriks yang diperoleh dengan mengalikan masing-masing entri dari A oleh c (Anton, 1987:24).

Contoh: $A = \begin{bmatrix} 4 & 2 \\ 1 & 3 \\ -1 & 0 \end{bmatrix}$ maka $2A = \begin{bmatrix} 8 & 4 \\ 2 & 6 \\ -2 & 0 \end{bmatrix}$

dan $(-1)A = \begin{bmatrix} -4 & -2 \\ -1 & -3 \\ 1 & 0 \end{bmatrix}$

**Definisi 2.4 (Perkalian Matriks)**

Jika $A$ adalah matriks $mxr$ dan $i$ adalah matriks $rxn$, maka hasil kali $AB$ adalah matriks $mxn$ yang entri-entrinya ditentukan sebagai berikut. Untuk mencari entri dalam baris $i$ dan kolom $j$ dari $AB$, pilihlah baris $i$ dari matriks $A$ dan kolom $j$ dari matriks $B$, kalikanlah entri-entri yang bersesuaian dari baris dan kolom tersebut bersama-sama dan kemudian tambahkanlah hasil kali yang dihasilkan (Anton, 1987:25).

Contoh: $A = \begin{bmatrix} 1 & 2 & 4 \\ 2 & 6 & 0 \end{bmatrix}$ dan $B = \begin{bmatrix} 4 & 1 & 4 & 3 \\ 0 & -1 & 3 & 1 \\ 2 & 7 & 5 & 2 \end{bmatrix}$

Karena $A$ dalah matriks $2x3$ dan $B$ adalah matriks $3x4$, maka hasil kali $AB$ adalah matriks $2x4$. Misalnya entri dalam baris 2 dan kolom 3 dari $AB$, kita dapat memilih baris 2 dari $A\,A$ dan kolom 3 dari $B$. Maka, seperti yang dilukiskan di bawah, kita dapat mengalikan entri-entri yang bersesuaian bersama-sama dan menambah hasil kali (Anton, 1987:25).

Perhitungan-perhitungan untuk hasil kalinya adalah sebagai berikut:

$$A=\begin{bmatrix}1 & 2 & 4\\ 2 & 6 & 0\end{bmatrix} \text{ dan } B=\begin{bmatrix}4 & 1 & 4 & 3\\ 0 & -1 & 3 & 1\\ 2 & 7 & 5 & 2\end{bmatrix}$$

$$\text{Hasilnya adalah } AB=\begin{bmatrix}12 & 27 & 30 & 13\\ 8 & -4 & 26 & 12\end{bmatrix}$$

### 2.2.4 Invers dan Transpos Matriks

**Definisi 2.5 (Invers Matriks)**

Misalkan *A* merupakan suatu matriks kuadrat dengan *n* baris dan *n* kolom dan $I_n$ suatu *identity* matriks. Apabila ada *square* matriks $A^{-1}$ sedemikian rupa sehingga berlaku hubungan sebagai berikut: $AA^{-1} = A^{-1}A = I$, maka $A^{-1}$ ini disebut *inverse matriks A* (Supranto, 2003:130).

Contoh: $B=\begin{bmatrix}3 & 5\\ 1 & 2\end{bmatrix}$ invers dari $A=\begin{bmatrix}2 & -5\\ -1 & 3\end{bmatrix}$

Karena $AB=\begin{bmatrix}2 & -5\\ -1 & 3\end{bmatrix}\begin{bmatrix}3 & 5\\ 1 & 2\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=I$

Dan $BA=\begin{bmatrix}3 & 5\\ 1 & 2\end{bmatrix}\begin{bmatrix}2 & -5\\ -1 & 3\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=I$

**Definisi 2.5 (Transpos Matriks)**

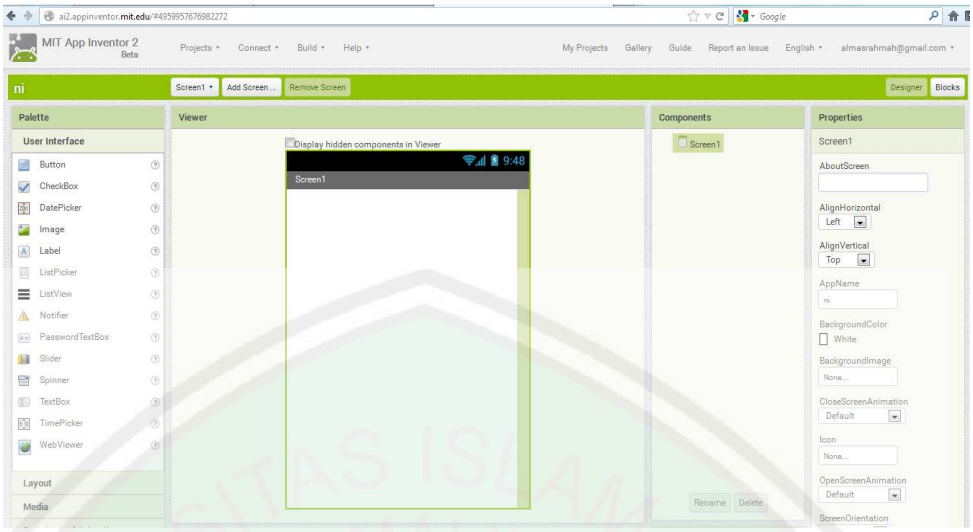
Matriks transpos diperoleh dengan menukar elemen-elemen baris menjadi elemen-elemen kolom atau sebaliknya (Gazali, 2005:18)

Contoh: $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$, maka transpos dari A adalah $A^t = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$

## 2.3 Pengertian Appinventor

Seiring dengan kemajuan zaman, banyak teknologi baru yang ditemukan. Salah satu teknologi yang sedang populer adalah *smartphone*. Android merupakan jenis *smartphone* yang paling banyak digunakan. Appinventor adalah program yang sangat bagus yang dibuat oleh *Google* dan sekarang dikembangkan oleh MIT. Program ini dapat digunakan untuk membuat dan mendesain aplikasi Android yang berbasis *Web Page* dan *Java Interface*. Hanya dengan pengetahuan pemrograman yang sedikit kita sudah bisa membuat sebuah aplikasi Android yang sederhana. Jika kita sudah berpengalaman menggunakan Appinventor kita juga bisa membuat program yang sangat rumit dan berguna hanya dengan menggunakan Appinventor (Prasetiyo, 2014:2).

Appinventor merupakan aplikasi untuk membuat program yang terdiri dari dua bagian yaitu: *Design View* dan *Block Editor*. Membuat program dengan menggunakan Appinventor sangatlah seru karena kita mendesain sebuah program dengan cara menyusun *puzzle* atau *block-block* yang warna-warni. Untuk masuk ke dalam *Block Editor* tekan *block* yang berada pada sisi kanan atas. *Block* dalam Appinventor itu seperti sebuah *statement* atau instruksi yang berada dalam bahasa pemrograman. Jadi dalam membuat aplikasi Android dengan menggunakan Appinventor lebih menyenangkan (Prasetiyo, 2014:5). Berikut ini akan ditunjukkan gambar Appinventor:

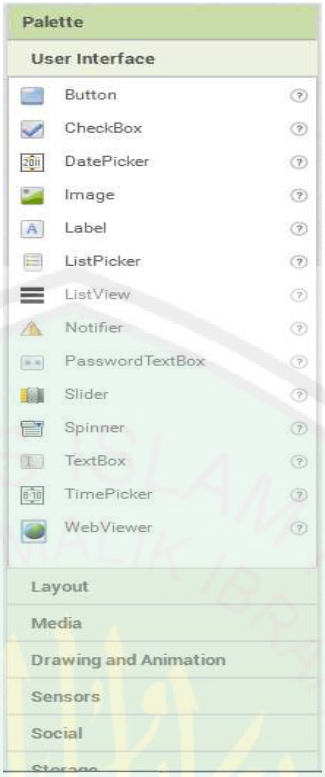



Gambar 2.1 Tampilan Aplikasi Appinventor

*Design View* terdiri dari lima komponen dasar:

a. *Palette*

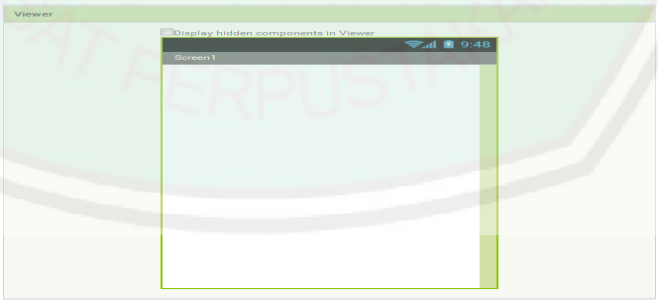
*Palette* terdiri dari objek apa saja yang bisa anda gunakan ke dalam aplikasi anda. *Palette* terdiri dari beberapa grup semuanya dikelompokkan ke dalam satu grup jika memiliki tema/fungsi yang sama. Contohnya *User Interface* yang memiliki fungsi digunakan untuk mengatur interaksi aplikasi dengan si pengguna yang terdiri dari *button, check box, clock, image, label,* dan sebagainya. Cara untuk menampilkan atau menyembunyikan anggota dari suatu kelompok kita perlu mengklik pada kelompok itu.




Gambar 2.2 *Pallete*

*b. Viewer*

Terdiri dari tampilan *handphone* dan komponen–komponen yang bisa diklik. Di situ juga kita bisa melihat komponen yang tidak bisa kita lihat dengan *handphone*.




Gambar 2.3 *Viewer*

*c. Component*

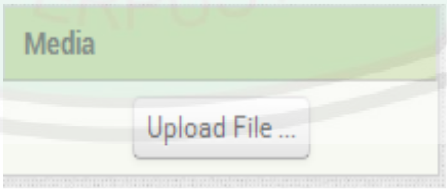
Terdiri dari daftar komponen apa saja yang telah kita tambahkan ke dalam projek kita baik secara terlihat maupun tidak terlihat dalam *handphone*.

Tampilannya berupa susunan atau daftar yang memudahkan kita untuk mengatur komponen atau melihat apa saja yang berbentuk seperti direktori.


Gambar 2.4 *Component*

d. Media

Kolom Media terletak di bawah dari kolom *Component*. Kolom ini digunakan untuk mengatur semua media komponen untuk mendukung aplikasi yang telah anda buat.

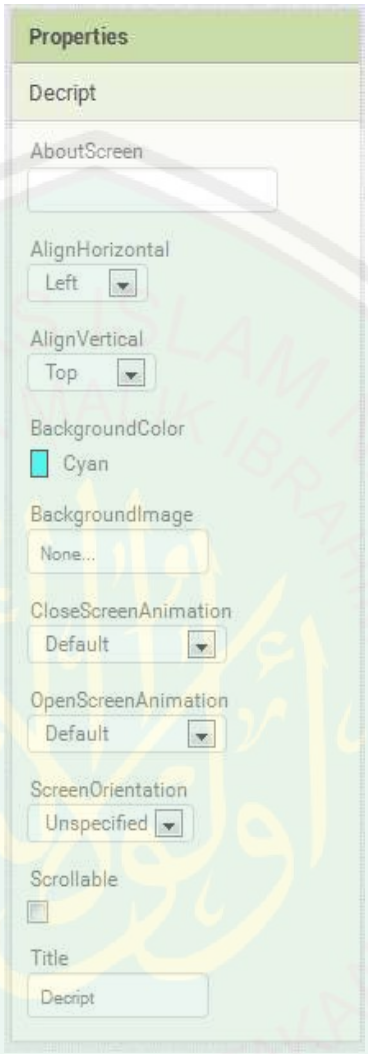



Gambar 2.5 Media

*e. Properties*

Setiap komponen yang anda tambahkan ke dalam projek, anda dapat mengatur komponen itu bagaimana dia berinteraksi dengan pengguna maupun dengan

komponen lain, atau bagaimana tampilannya. Setiap komponen memiliki kolom *properties* yang berbeda-beda (Prasetiyo, 2014:7).




Gambar 2.6 *Properties*

## 2.4 Kajian Keagamaan

Al-Quran juga menjelaskan anjuran untuk menjaga pesan yang bersifat rahasia supaya tidak diketahui oleh orang yang tidak berhak, yaitu terdapat di dalam surat an-Nisa' ayat 58 yang berbunyi:

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-Nisa'/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. bersabda:

اَدِّالْاَمَانَةَ إِلَى مَنِ ائْتَمَنَكَ, وَلَاتَخُنْ مَنْ خَانَكَ

*"Sampaikanlah 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 menyampaikannya (Ibnu Katsir, 2000:251).

Selain surat an-Nisa' ayat 58 al-Quran juga menjelaskan anjuran untuk menjaga pesan bersifat rahasia yang terdapat dalam surat al-Anfal ayat 27 yaitu:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

*"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui" (QS. al-Anfal/8:27).*

As-Saddi mengatakan, apabila mereka mengkhianati Allah dan Rasul-Nya, berarti mereka mengkhianati amanat-amanat yang dipercayakan kepada diri mereka. Selanjutnya ia mengatakan pula bahwa dahulu mereka mendengar pembicaraan dari Nabi Saw., lalu mereka membocorkannya kepada kaum

musyrik. Abdur Rahman Ibnu Zaid mengatakan, Allah melarang kalian berbuat khianat terhadap Allah dan Rasul-Nya, janganlah kalian berbuat seperti apa yang dilakukan oleh orang-orang munafik (Ibnu Katsir, 2001:407).

Penyandian pesan juga sudah diterapkan pada saat turunnya wahyu kepada Nabi Muhammad Saw., yaitu di dalam buku Ringkasan Shahih Bukhori hadits yang artinya:

> *Dari Aisyah Ummul Mukminin RA, bahwa Al Harits bin Hisyam RA bertanya kepada Rasulullah Saw., "Wahai Rasulullah, bagaimana caranya wahyu datang kepadamu?" Rasulullah Saw. menjawab, "kadang-kadang wahyu itu datang kepadaku seperti bunyi lonceng, itulah yang paling berat bagiku. Setelah bunyi itu berhenti, aku pun memahami apa yang dikatakan. Adakalanya malaikat menampakkan diri kepadaku dalam bentuk seorang laki-laki lalu berbicara kepadaku, maka aku memahami apa yang diucapkan. "Aisyah RA berkata, "aku pernah melihat beliau ketika wahyu turun kepadanya di suatu hari yang sangat dingin, yang mana setelah wahyu itu selesai turun, kelihatan dahi beliau bersimpah peluh."*

# BAB III

# METODE PENELITIAN

## 3.1 Jenis dan Metode Penelitian

Sebelum melakukan penelitian, peneliti harus menentukan terlebih dahulu metode yang akan dilakukan untuk penelitian tersebut sebagai cara agar mencapai tujuan dari penelitian. Dalam penelitian ini jenis penelitian yang digunakan adalah deskriptif kualitatif. Metode penelitian kualitatif dan jenis penelitian deskriptif yaitu dengan metode kepustakaan dengan cara mengumpulkan data-data atau informasi dari berbagai buku, jurnal, internet, dan lainnya yang berkaitan dengan masalah yang akan digunakan dalam pembahasan masalah dalam penelitian ini. Metode penelitian kepustakaan juga sering disebut dengan *library research*.

## 3.2 Teknik Pengumpulan Data

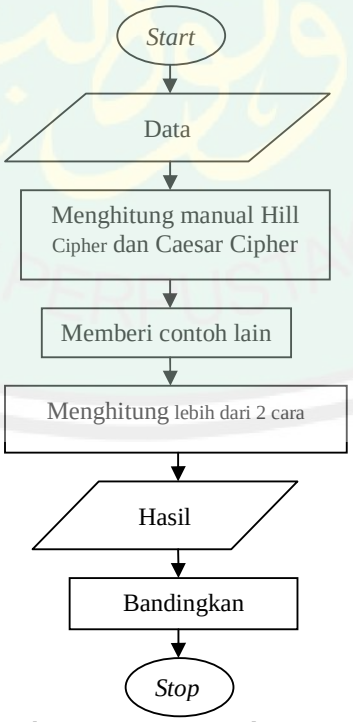
Teknik pengumpulan data merupakan langkah yang paling utama dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data. Tanpa mengetahui teknik pengumpulan data, maka peneliti tidak akan mendapatkan data yang memenuhi standar data yang ditetapkan (Sugiono, 2010:308). Karena di dalam penelitian ini menggunakan metode kepustakaan maka teknik pengumpulan data atau informasi berasal dari berbagai pustaka yaitu berupa buku-buku, jurnal, artikel, majalah, dan lain-lain. Oleh karena itu pada penelitian ini peneliti mengumpulkan data dan sumber informasi dari beberapa literatur yang menjadi bahan sebagai landasan untuk menjawab rumusan masalah.

### 3.3 Analisis Data

Informasi yang telah diperoleh dari berbagai literatur kemudian dianalisis dan diolah dalam bentuk laporan penelitian kepustakaan. Berikut akan dijelaskan langkah-langkah dalam menganalisis informasi yang sudah terkumpul. Langkah-langkah analisis adalah

1. Memberi contoh pesan yang berkaitan dengan masalah yang akan dibahas kemudian mempelajari dan menelaahnya.
2. Mencoba mencari dan menghitung proses penyandian secara manual dari Hill Cipher dan Caesar Cipher.
3. Memberi contoh lain dan menerapkannya dalam proses no 2.
4. Menghitung dengan Hill Cipher dan Caesar Cipher dengan lebih dari 2 cara.
5. Hasil proses penyandian dari masing-masing cara sudah didapatkan.
6. Mendeskripsikan dan membandingkan hasil dari masing-masing cara.

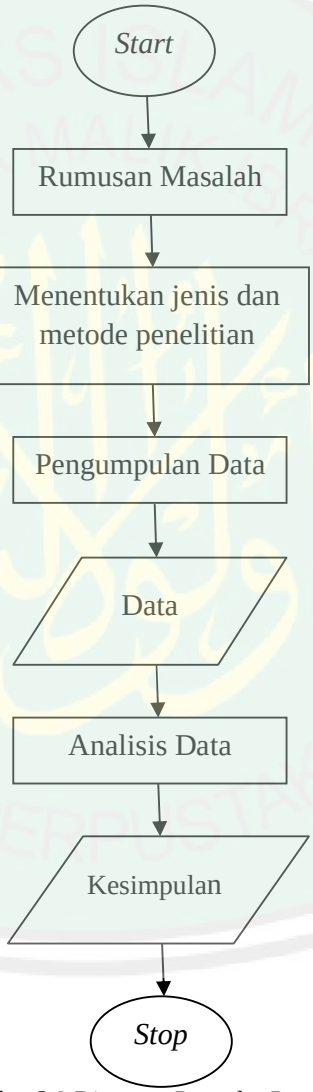
Analisis di atas dapat ditampilkan dalam bentuk *flowchart* di bawah ini:




Gambar 3.1 Diagram Analisis Data

### 3.4 Prosedur Penelitian

Prosedur penelitian merupakan langkah-langkah penelitian yang akan dilakukan peneliti agar penelitian lebih terfokus dan tidak bias. Di dalam penelitian ini langkah awal adalah merumuskan masalah, menentukan jenis dan metode penelitian, pengumpulan data, analisis data kemudian diakhiri dengan kesimpulan. Berikut akan ditampilkan *flowchart* tentang prosedur di dalam penelitian ini:




Gambar 3.2 Diagram Prosedur Penelitian

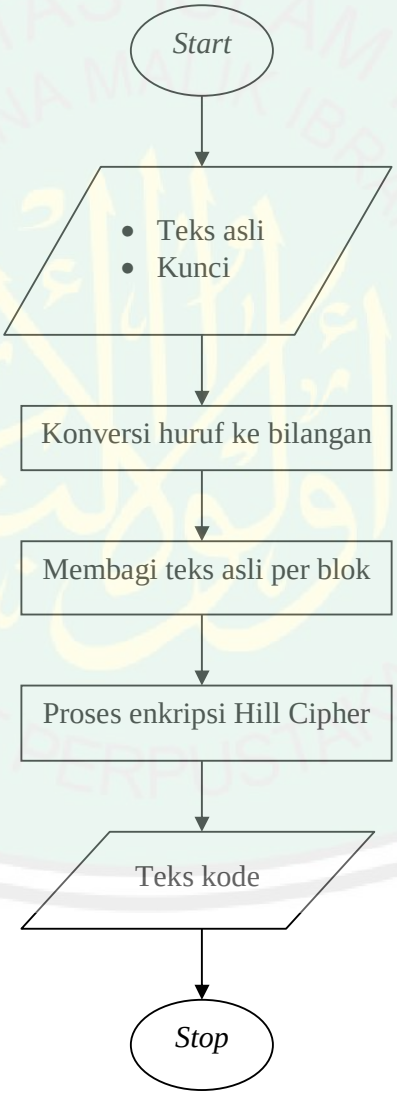
# BAB IV

# PEMBAHASAN

## 4.1 Proses Penyandian Hill Cipher

### 4.1.1 Proses Enkripsi Hill Cipher

Proses enkripsi dengan metode Hill Cipher ini dapat dijelaskan dalam *flowchart* di bawah ini:




Gambar 4.1 Proses Enkripsi Hill Cipher

Langkah awal dari proses enkripsi dengan metode Hill Cipher adalah dengan membagi teks asli menjadi perblok. Ukuran blok disesuaikan dengan ukuran matriks yang menjadi kunci, matriks berukuran $nxn$ (Ariyus, 2008:59).

Kemudian teks asli dikonversikan menjadi bilangan, dengan $A = 0$, $B = 1$, $C = 2$ sampai $Z = 25$ yang akan ditunjukkan dalam tabel di bawah ini:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Tabel 4.1 Konversi Huruf ke Angka

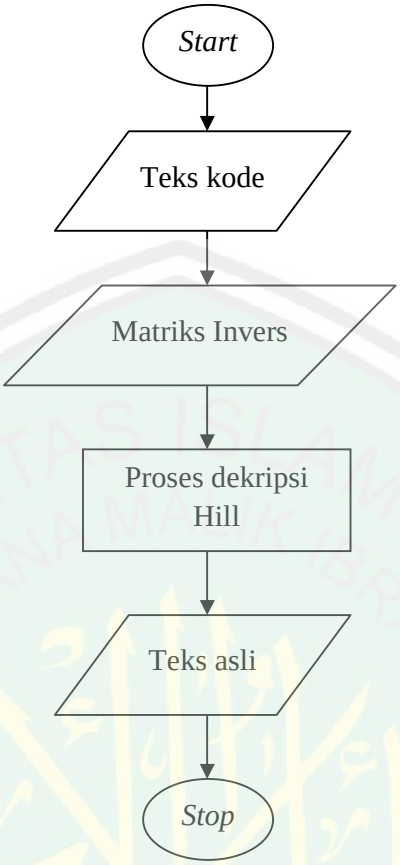
Kunci pada metode Hill Cipher ini menggunakan matriks yang memiliki invers agar teks asli dapat didekripsi kembali menjadi teks semula. Suatu matriks K memiliki invers jika dan hanya jika determinannya tidak nol. Namun karena $Z_{26}$ maka K memiliki invers modulo 26.

Hasugian (2013) menyebutkan bahwa secara matematis proses enkripsi pada metode Hill Cipher adalah

C = $K \cdot P$
C = teks kode
K = kunci
P = teks asli

### 4.1.2 Proses Dekripsi Hill Cipher

Proses dekripsi dengan metode Hill Cipher ini dapat digambarkan dalam *flowchart* di bawah ini:




Gambar 4.2 Proses Dekripsi Hill Cipher

Pada dasarnya proses dekripsi sama dengan proses enkripsi, akan tetapi pada proses dekripsi ini kata kuncinya menggunakan invers matriksnya. Hasugian (2013) menyebutkan bahwa secara matematis proses dekripsi pada metode Hill Cipher dapat dituliskan sebagai berikut:

$$C = K \cdot P$$
$$K^{-1} \cdot C = K^{-1} \cdot K \cdot P$$
$$K^{-1} \cdot C = I \cdot P$$
$$C = K^{-1} \cdot C$$

### 4.1.3 Proses Enkripsi Dekripsi Menggunakan Kunci Matriks $2x2$

**a. Proses Enkripsi**

Teks asli: PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

Kunci: $\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$

Teks asli akan dikonversi terlebih dahulu ke dalam bentuk bilangan, sehingga menjadi:

| P | E | N | D | I | D | I | K | A | N | M | E | R | U | P | A | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 4 | 13 | 3 | 8 | 3 | 8 | 10 | 0 | 13 | 12 | 4 | 17 | 20 | 15 | 0 | 10 |

| A | N | K | E | B | U | T | U | H | A | N | M | U | T | L | A | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 13 | 10 | 4 | 1 | 20 | 19 | 20 | 7 | 0 | 13 | 12 | 20 | 19 | 11 | 0 | 10 |

Karena kunci yang dipakai adalah matriks yang berukuran $2x2$, maka teks asli dibagi menjadi blok-blok yang berisi 2 huruf.

| 15 4 | 13 3 | 8 3 | 8 10 | 0 13 | 12 4 | 17 20 |
|---|---|---|---|---|---|---|
| Blok I | Blok II | Blok III | Blok IV | Blok V | Blok VI | Blok VII |

| 15 0 | 10 0 | 13 10 | 4 1 | 20 19 | 20 7 | 0 13 |
|---|---|---|---|---|---|---|
| Blok VIII | Blok IX | Blok X | Blok XI | Blok XII | Blok XIII | Blok XIV |

| 12 20 | 19 11 | 0 11 |
|---|---|---|
| Blok XV | Blok XVI | Blok XVII |

Proses enkripsi dilakukan satu persatu dari blok tersebut:

Blok I : $\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} 30+12 \\ 15+4 \end{bmatrix} = \begin{bmatrix} 42 \\ 19 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 16 \\ 19 \end{bmatrix} = \begin{bmatrix} Q \\ T \end{bmatrix}$

Blok II : $\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 13 \\ 3 \end{bmatrix} = \begin{bmatrix} 26+9 \\ 13+3 \end{bmatrix} = \begin{bmatrix} 35 \\ 16 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 9 \\ 16 \end{bmatrix} = \begin{bmatrix} J \\ Q \end{bmatrix}$

Blok III : $\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 3 \end{bmatrix} = \begin{bmatrix} 16+9 \\ 8+3 \end{bmatrix} = \begin{bmatrix} 25 \\ 11 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 25 \\ 11 \end{bmatrix} = \begin{bmatrix} Z \\ L \end{bmatrix}$

Blok IV : $\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} 16+30 \\ 8+10 \end{bmatrix} = \begin{bmatrix} 46 \\ 18 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 20 \\ 18 \end{bmatrix} = \begin{bmatrix} U \\ S \end{bmatrix}$

Blok V : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}0\\13\end{bmatrix} = \begin{bmatrix}0+39\\0+13\end{bmatrix} = \begin{bmatrix}39\\13\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\13\end{bmatrix} = \begin{bmatrix}N\\N\end{bmatrix}$

Blok VI : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}12\\4\end{bmatrix} = \begin{bmatrix}24+12\\12+4\end{bmatrix} = \begin{bmatrix}36\\16\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}10\\16\end{bmatrix} = \begin{bmatrix}K\\Q\end{bmatrix}$

Blok VII : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}17\\20\end{bmatrix} = \begin{bmatrix}34+60\\17+20\end{bmatrix} = \begin{bmatrix}94\\37\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}16\\11\end{bmatrix} = \begin{bmatrix}Q\\L\end{bmatrix}$

Blok VIII : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}15\\0\end{bmatrix} = \begin{bmatrix}30+0\\15+0\end{bmatrix} = \begin{bmatrix}30\\15\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}4\\15\end{bmatrix} = \begin{bmatrix}E\\P\end{bmatrix}$

Blok IX : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}10\\0\end{bmatrix} = \begin{bmatrix}20+0\\10+0\end{bmatrix} = \begin{bmatrix}20\\10\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\10\end{bmatrix} = \begin{bmatrix}U\\K\end{bmatrix}$

Blok X : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}13\\10\end{bmatrix} = \begin{bmatrix}26+30\\13+10\end{bmatrix} = \begin{bmatrix}56\\23\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}4\\23\end{bmatrix} = \begin{bmatrix}E\\X\end{bmatrix}$

Blok XI : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}4\\1\end{bmatrix} = \begin{bmatrix}8+3\\4+1\end{bmatrix} = \begin{bmatrix}11\\5\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}11\\5\end{bmatrix} = \begin{bmatrix}L\\F\end{bmatrix}$

Blok XII : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}20\\19\end{bmatrix} = \begin{bmatrix}40+57\\20+19\end{bmatrix} = \begin{bmatrix}97\\39\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\13\end{bmatrix} = \begin{bmatrix}T\\N\end{bmatrix}$

Blok XIII : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}20\\7\end{bmatrix} = \begin{bmatrix}40+21\\20+7\end{bmatrix} = \begin{bmatrix}61\\27\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}9\\1\end{bmatrix} = \begin{bmatrix}J\\B\end{bmatrix}$

Blok XIV : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}0\\13\end{bmatrix} = \begin{bmatrix}0+39\\0+13\end{bmatrix} = \begin{bmatrix}39\\13\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\13\end{bmatrix} = \begin{bmatrix}N\\N\end{bmatrix}$

Blok XV : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}12\\20\end{bmatrix} = \begin{bmatrix}24+60\\12+20\end{bmatrix} = \begin{bmatrix}84\\32\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}6\\6\end{bmatrix} = \begin{bmatrix}G\\G\end{bmatrix}$

Blok XVI : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}19\\11\end{bmatrix} = \begin{bmatrix}38+33\\19+11\end{bmatrix} = \begin{bmatrix}71\\30\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\4\end{bmatrix} = \begin{bmatrix}T\\E\end{bmatrix}$

Blok XVII : $\begin{bmatrix}2 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}0\\10\end{bmatrix} = \begin{bmatrix}0+30\\0+10\end{bmatrix} = \begin{bmatrix}30\\10\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}4\\10\end{bmatrix} = \begin{bmatrix}E\\K\end{bmatrix}$

Dari proses enkripsi di atas diperoleh teks kode sebagai berikut:

QTJQZLUSNNKQQLEPUKEXLFTNJBNNGGTEEK

**b. Proses Dekripsi**

Pada proses dekripsi ini teks kode akan diubah menjadi teks asli atau seperti bentuk semula.

Teks kode: QTJQZLUSNNKQQLEPUKEXLFTNJBNNGGTEEK

$K = \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$

$K^{-1} = \frac{1}{\det(k)} \begin{bmatrix} 1 & -3 \\ -1 & 2 \end{bmatrix}$

$K^{-1} = \frac{1}{-1} \begin{bmatrix} 1 & -3 \\ -1 & 2 \end{bmatrix}$

$K^{-1} = -1 \begin{bmatrix} 1 & -3 \\ -1 & 2 \end{bmatrix}$

$= \begin{bmatrix} -1 & 3 \\ 1 & -2 \end{bmatrix}$

Hasugian (2013) mengatakan bahwa jika pada invers matriks terdapat bilangan negatif maka ditambah 26 agar nilai tetap positif, ini digunakan karena bil 0-26.

Jadi untuk $K^{-1} = \begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix}$

Proses dekripsi:

Blok I : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 6 \\ 19 \end{bmatrix} = \begin{bmatrix} 400 + 57 \\ 16 + 456 \end{bmatrix} = \begin{bmatrix} 457 \\ 472 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} P \\ E \end{bmatrix}$

Blok II : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 9 \\ 16 \end{bmatrix} = \begin{bmatrix} 225 + 48 \\ 9 + 384 \end{bmatrix} = \begin{bmatrix} 273 \\ 393 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 13 \\ 3 \end{bmatrix} = \begin{bmatrix} N \\ D \end{bmatrix}$

Blok III : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 25 \\ 11 \end{bmatrix} = \begin{bmatrix} 625 + 33 \\ 25 + 264 \end{bmatrix} = \begin{bmatrix} 658 \\ 289 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 8 \\ 3 \end{bmatrix} = \begin{bmatrix} I \\ D \end{bmatrix}$

Blok IV : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 20 \\ 18 \end{bmatrix} = \begin{bmatrix} 500 + 54 \\ 20 + 432 \end{bmatrix} = \begin{bmatrix} 554 \\ 452 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} I \\ K \end{bmatrix}$

Blok V : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 13 \\ 13 \end{bmatrix} = \begin{bmatrix} 325 + 39 \\ 13 + 312 \end{bmatrix} = \begin{bmatrix} 364 \\ 312 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} A \\ N \end{bmatrix}$

Blok VI : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 10 \\ 16 \end{bmatrix} = \begin{bmatrix} 250 + 48 \\ 10 + 384 \end{bmatrix} = \begin{bmatrix} 298 \\ 394 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} M \\ E \end{bmatrix}$

Blok VII : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 16 \\ 11 \end{bmatrix} = \begin{bmatrix} 400 + 33 \\ 16 + 264 \end{bmatrix} = \begin{bmatrix} 433 \\ 280 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 17 \\ 20 \end{bmatrix} = \begin{bmatrix} R \\ U \end{bmatrix}$

Blok VIII : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 4 \\ 15 \end{bmatrix} = \begin{bmatrix} 100 + 45 \\ 4 + 360 \end{bmatrix} = \begin{bmatrix} 145 \\ 364 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 15 \\ 0 \end{bmatrix} = \begin{bmatrix} P \\ A \end{bmatrix}$

Blok IX : $\begin{bmatrix} 25 & 3 \\ 1 & 24 \end{bmatrix} \begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{bmatrix} 500 + 30 \\ 20 + 260 \end{bmatrix} = \begin{bmatrix} 530 \\ 260 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 10 \\ 0 \end{bmatrix} = \begin{bmatrix} K \\ A \end{bmatrix}$

Blok X : $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}4\\23\end{bmatrix}=\begin{bmatrix}100+69\\4+552\end{bmatrix}=\begin{bmatrix}169\\556\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\10\end{bmatrix}=\begin{bmatrix}N\\K\end{bmatrix}$

Blok XI : $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}11\\5\end{bmatrix}=\begin{bmatrix}275+15\\11+120\end{bmatrix}=\begin{bmatrix}290\\131\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}4\\1\end{bmatrix}=\begin{bmatrix}E\\B\end{bmatrix}$

Blok XII : $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}19\\13\end{bmatrix}=\begin{bmatrix}475+39\\19+312\end{bmatrix}=\begin{bmatrix}514\\331\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\19\end{bmatrix}=\begin{bmatrix}U\\T\end{bmatrix}$

Blok XIII : $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}9\\1\end{bmatrix}=\begin{bmatrix}225+3\\9+24\end{bmatrix}=\begin{bmatrix}228\\33\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\7\end{bmatrix}=\begin{bmatrix}U\\H\end{bmatrix}$

Blok XIV: $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}13\\13\end{bmatrix}=\begin{bmatrix}325+39\\13+312\end{bmatrix}=\begin{bmatrix}364\\325\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}0\\13\end{bmatrix}=\begin{bmatrix}A\\N\end{bmatrix}$

Blok XV : $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}6\\6\end{bmatrix}=\begin{bmatrix}150+18\\6+144\end{bmatrix}=\begin{bmatrix}168\\150\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}12\\20\end{bmatrix}=\begin{bmatrix}M\\U\end{bmatrix}$

Blok XVI : $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}19\\4\end{bmatrix}=\begin{bmatrix}475+12\\19+96\end{bmatrix}=\begin{bmatrix}487\\115\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\11\end{bmatrix}=\begin{bmatrix}T\\L\end{bmatrix}$

Blok XVII: $\begin{bmatrix}25 & 3\\ 1 & 24\end{bmatrix}\begin{bmatrix}4\\10\end{bmatrix}=\begin{bmatrix}100+30\\4+240\end{bmatrix}=\begin{bmatrix}130\\244\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}0\\10\end{bmatrix}=\begin{bmatrix}A\\K\end{bmatrix}$

Dari proses dekripsi di atas dapat diperoleh hasil seperti semula yaitu:

PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

### 4.1.4 Proses Enkripsi Dekripsi Menggunakan Kunci Matriks $3x3$

**a. Proses Enkripsi**

Teks asli: PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

Kunci: $\begin{bmatrix}1 & 2 & 3\\ 2 & 5 & 3\\ 1 & 0 & 8\end{bmatrix}$

Setelah teks asli dikonversikan ke dalam bentuk angka, kemudian dibagi menjadi blok-blok yang berisi 3 huruf tiap bloknya karena kunci yang dipakai adalah matriks yang berukuran $3x3$. Jika dalam blok ada huruf yang kurang maka peneliti menambah dengan huruf O.

| 15 4 13 | 3 8 3 | 8 10 0 | 13 12 4 | 17 20 15 | 0 10 0 | 13 10 4 |
|---|---|---|---|---|---|---|
| Blok I | Blok II | Blok III | Blok IV | Blok V | Blok VI | Blok VII |

| 1 20 19 | 20 7 0 | 13 12 20 | 19 11 0 | 10 14 14 |
|---|---|---|---|---|
| Blok VIII | Blok IX | Blok X | Blok XI | Blok XII |

Proses enkripsi:

Blok I : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}15\\4\\13\end{bmatrix}=\begin{bmatrix}15+8+39\\30+20+39\\15+0+104\end{bmatrix}=\begin{bmatrix}62\\89\\119\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}10\\11\\15\end{bmatrix}=\begin{bmatrix}K\\L\\P\end{bmatrix}$

Blok II : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}3\\8\\3\end{bmatrix}=\begin{bmatrix}3+16+9\\6+40+9\\3+0+24\end{bmatrix}=\begin{bmatrix}28\\55\\27\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}2\\3\\1\end{bmatrix}=\begin{bmatrix}C\\D\\B\end{bmatrix}$

Blok III : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}8\\10\\0\end{bmatrix}=\begin{bmatrix}8+20+0\\16+50+0\\8+0+0\end{bmatrix}=\begin{bmatrix}28\\66\\8\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}2\\14\\8\end{bmatrix}=\begin{bmatrix}C\\O\\I\end{bmatrix}$

Blok IV : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}13\\12\\4\end{bmatrix}=\begin{bmatrix}13+24+12\\26+60+12\\13+0+32\end{bmatrix}=\begin{bmatrix}49\\98\\45\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}23\\20\\19\end{bmatrix}=\begin{bmatrix}X\\U\\T\end{bmatrix}$

Blok V : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}17\\20\\15\end{bmatrix}=\begin{bmatrix}17+40+45\\34+100+45\\17+0+120\end{bmatrix}=\begin{bmatrix}102\\179\\137\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}24\\23\\7\end{bmatrix}=\begin{bmatrix}Y\\X\\H\end{bmatrix}$

Blok VI : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}0\\10\\0\end{bmatrix}=\begin{bmatrix}0+20+0\\0+50+0\\0+0+0\end{bmatrix}=\begin{bmatrix}20\\50\\0\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\24\\0\end{bmatrix}=\begin{bmatrix}U\\Y\\A\end{bmatrix}$

Blok VII : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}13\\10\\4\end{bmatrix}=\begin{bmatrix}13+20+12\\26+50+12\\13+0+32\end{bmatrix}=\begin{bmatrix}45\\88\\45\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\10\\19\end{bmatrix}=\begin{bmatrix}T\\K\\T\end{bmatrix}$

Blok VIII : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}1\\20\\19\end{bmatrix}=\begin{bmatrix}1+40+57\\2+100+57\\1+0+152\end{bmatrix}=\begin{bmatrix}98\\159\\153\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\3\\23\end{bmatrix}=\begin{bmatrix}U\\D\\X\end{bmatrix}$

Blok IX : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}20\\7\\0\end{bmatrix}=\begin{bmatrix}20+14+0\\40+35+0\\20+0+0\end{bmatrix}=\begin{bmatrix}34\\75\\20\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}8\\23\\20\end{bmatrix}=\begin{bmatrix}I\\X\\U\end{bmatrix}$

Blok X : $\begin{bmatrix}1&2&3\\2&5&3\\1&0&8\end{bmatrix}\begin{bmatrix}13\\12\\20\end{bmatrix}=\begin{bmatrix}13+24+60\\26+60+60\\13+0+160\end{bmatrix}=\begin{bmatrix}97\\146\\173\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\16\\17\end{bmatrix}=\begin{bmatrix}T\\Q\\R\end{bmatrix}$

Blok XI : $\begin{bmatrix}1 & 2 & 3\\2 & 5 & 3\\1 & 0 & 8\end{bmatrix}\begin{bmatrix}19\\11\\0\end{bmatrix}=\begin{bmatrix}19+22+0\\38+55+0\\19+0+0\end{bmatrix}=\begin{bmatrix}41\\93\\19\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}15\\15\\19\end{bmatrix}=\begin{bmatrix}P\\P\\T\end{bmatrix}$

Blok XII : $\begin{bmatrix}1 & 2 & 3\\2 & 5 & 3\\1 & 0 & 8\end{bmatrix}\begin{bmatrix}10\\14\\14\end{bmatrix}=\begin{bmatrix}10+28+42\\20+70+42\\10+0+112\end{bmatrix}=\begin{bmatrix}80\\132\\122\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}2\\2\\18\end{bmatrix}=\begin{bmatrix}C\\C\\S\end{bmatrix}$

Dari proses dekripsi di atas diperoleh teks kode sebagai berikut:

KLPCDBCOIXUTYXHUYATKTUDXIXUTQRPPTCCS

**b. Proses Dekripsi**

Pada proses dekripsi teks kode akan diubah menjadi teks asli atau seperti bentuk semula.

Teks kode: KLPCDBCOIXUTYXHUYATKTUDXIXUTQRPPTCCS

Kunci: $\begin{bmatrix}1 & 2 & 3\\2 & 5 & 3\\1 & 0 & 8\end{bmatrix}$

$K^{-1}$: $\begin{bmatrix}-40 & 16 & 9\\13 & -5 & -3\\5 & -2 & -1\end{bmatrix}$ dengan modulo 26 $K^{-1}$: $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}$

Proses dekripsi:

Blok I : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}10\\11\\15\end{bmatrix}=\begin{bmatrix}120+176+135\\130+231+345\\50+264+375\end{bmatrix}=\begin{bmatrix}431\\706\\689\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}15\\4\\13\end{bmatrix}=\begin{bmatrix}P\\E\\N\end{bmatrix}$

Blok II : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}2\\3\\1\end{bmatrix}=\begin{bmatrix}24+48+9\\26+63+23\\10+72+25\end{bmatrix}=\begin{bmatrix}81\\112\\107\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}3\\8\\3\end{bmatrix}=\begin{bmatrix}D\\I\\D\end{bmatrix}$

Blok III : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}2\\14\\8\end{bmatrix}=\begin{bmatrix}24+224+72\\26+294+184\\10+336+200\end{bmatrix}=\begin{bmatrix}320\\504\\546\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}8\\10\\0\end{bmatrix}=\begin{bmatrix}I\\K\\A\end{bmatrix}$

Blok IV: $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}23\\20\\19\end{bmatrix}=\begin{bmatrix}276+320+171\\299+420+437\\115+480+475\end{bmatrix}=\begin{bmatrix}767\\1156\\1070\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\12\\4\end{bmatrix}=\begin{bmatrix}N\\M\\E\end{bmatrix}$

Blok V: $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}24\\23\\7\end{bmatrix}=\begin{bmatrix}288+368+63\\312+483+161\\120+552+175\end{bmatrix}=\begin{bmatrix}719\\956\\847\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}17\\20\\15\end{bmatrix}=\begin{bmatrix}R\\U\\P\end{bmatrix}$

Blok VI : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}20\\24\\0\end{bmatrix}=\begin{bmatrix}240+384+0\\260+504+0\\100+576+0\end{bmatrix}=\begin{bmatrix}624\\764\\676\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}0\\10\\0\end{bmatrix}=\begin{bmatrix}A\\K\\A\end{bmatrix}$

Blok VII : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}19\\10\\19\end{bmatrix}=\begin{bmatrix}228+160+171\\247+210+437\\95+240+475\end{bmatrix}=\begin{bmatrix}559\\894\\810\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\10\\4\end{bmatrix}=\begin{bmatrix}N\\K\\E\end{bmatrix}$

Blok VIII : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}20\\3\\23\end{bmatrix}=\begin{bmatrix}240+48+207\\260+63+529\\100+72+575\end{bmatrix}=\begin{bmatrix}495\\852\\747\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}1\\20\\19\end{bmatrix}=\begin{bmatrix}B\\U\\T\end{bmatrix}$

Blok IX : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}8\\23\\20\end{bmatrix}=\begin{bmatrix}96+368+180\\104+483+460\\40+552+500\end{bmatrix}=\begin{bmatrix}644\\1047\\1092\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\7\\0\end{bmatrix}=\begin{bmatrix}U\\H\\A\end{bmatrix}$

Blok X: $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}19\\16\\17\end{bmatrix}=\begin{bmatrix}228+256+153\\247+336+391\\95+384+425\end{bmatrix}=\begin{bmatrix}637\\974\\904\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\12\\20\end{bmatrix}=\begin{bmatrix}N\\M\\U\end{bmatrix}$

Blok XI : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}15\\15\\19\end{bmatrix}=\begin{bmatrix}180+240+171\\195+315+437\\75+360+475\end{bmatrix}=\begin{bmatrix}591\\947\\910\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\11\\0\end{bmatrix}=\begin{bmatrix}T\\L\\A\end{bmatrix}$

Blok XII : $\begin{bmatrix}12 & 16 & 9\\13 & 21 & 23\\5 & 24 & 25\end{bmatrix}\begin{bmatrix}2\\2\\18\end{bmatrix}=\begin{bmatrix}24+32+162\\26+42+414\\10+48+450\end{bmatrix}=\begin{bmatrix}218\\482\\506\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}10\\14\\14\end{bmatrix}=\begin{bmatrix}K\\O\\O\end{bmatrix}$

Dari proses dekripsi di atas dapat diperoleh hasil seperti semula yaitu:

PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

### 4.1.5 Proses Enkripsi Dekripsi Menggunakan Kunci Matriks $4x4$

**a. Proses Enkripsi**

Teks asli: PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

Kunci: $\begin{bmatrix}0 & 1 & 2 & 2\\1 & 1 & 2 & 3\\2 & 2 & 2 & 3\\2 & 3 & 3 & 3\end{bmatrix}$

Setelah teks asli dikonversikan ke dalam bentuk angka, kemudian dibagi menjadi blok-blok yang berisi 4 huruf tiap bloknya karena kunci yang dipakai adalah matriks yang berukuran $4x4$. Jika dalam blok ada huruf yang kurang maka peneliti menambah dengan huruf O.

| 15 4 13 3 | 8 3 8 10 | 0 13 12 4 | 17 20 15 0 | 10 0 13 0 |
|---|---|---|---|---|
| Blok I | Blok II | Blok III | Blok IV | Blok V |

| 4 1 20 19 | 20 7 0 13 | 12 20 19 11 | 0 10 14 14 |
|---|---|---|---|
| Blok VI | Blok VII | Blok VIII | Blok IX |

Proses enkripsi:

Blok I: $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}15\\4\\13\\3\end{bmatrix}=\begin{bmatrix}0+4+26+6\\15+4+26+9\\30+8+26+9\\30+12+39+9\end{bmatrix}=\begin{bmatrix}36\\54\\73\\90\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}10\\2\\21\\12\end{bmatrix}=\begin{bmatrix}K\\C\\V\\M\end{bmatrix}$

Blok II: $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}8\\3\\8\\10\end{bmatrix}=\begin{bmatrix}0+3+16+20\\8+3+16+30\\16+6+16+30\\16+9+24+30\end{bmatrix}=\begin{bmatrix}39\\57\\68\\79\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}13\\5\\16\\1\end{bmatrix}=\begin{bmatrix}N\\F\\Q\\B\end{bmatrix}$

Blok III: $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}0\\13\\12\\4\end{bmatrix}=\begin{bmatrix}0+13+24+8\\0+13+24+12\\0+26+24+12\\0+39+36+12\end{bmatrix}=\begin{bmatrix}45\\49\\62\\87\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}19\\23\\10\\9\end{bmatrix}=\begin{bmatrix}T\\Q\\K\\J\end{bmatrix}$

Blok IV: $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}17\\20\\15\\0\end{bmatrix}=\begin{bmatrix}0+20+30+0\\17+20+30+0\\34+40+30+0\\34+60+45+0\end{bmatrix}=\begin{bmatrix}50\\67\\104\\139\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}24\\15\\0\\9\end{bmatrix}=\begin{bmatrix}Y\\P\\A\\J\end{bmatrix}$

Blok V: $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}10\\0\\13\\10\end{bmatrix}=\begin{bmatrix}0+0+26+20\\10+0+26+30\\20+0+26+30\\20+0+39+30\end{bmatrix}=\begin{bmatrix}46\\66\\76\\89\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}20\\14\\24\\11\end{bmatrix}=\begin{bmatrix}U\\O\\Y\\L\end{bmatrix}$

Blok VI : $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}4\\1\\20\\19\end{bmatrix}=\begin{bmatrix}0+1+40+38\\4+1+40+57\\8+2+40+57\\8+3+60+57\end{bmatrix}=\begin{bmatrix}79\\102\\107\\128\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}1\\24\\3\\24\end{bmatrix}=\begin{bmatrix}B\\Y\\D\\Y\end{bmatrix}$

Blok VII: $\begin{bmatrix}0&1&2&2\\1&1&2&3\\2&2&2&3\\2&3&3&3\end{bmatrix}\begin{bmatrix}20\\7\\0\\13\end{bmatrix}=\begin{bmatrix}0+7+0+26\\20+7+0+39\\40+14+0+39\\40+21+0+39\end{bmatrix}=\begin{bmatrix}33\\66\\93\\100\end{bmatrix}$ dengan modulo 26 $\begin{bmatrix}7\\14\\15\\22\end{bmatrix}=\begin{bmatrix}H\\O\\P\\W\end{bmatrix}$

Blok VIII: $\begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 3 \\ 2 & 2 & 2 & 3 \\ 2 & 3 & 3 & 3 \end{bmatrix} \begin{bmatrix} 12 \\ 20 \\ 19 \\ 11 \end{bmatrix} = \begin{bmatrix} 0+20+38+22 \\ 12+20+38+33 \\ 24+40+38+33 \\ 24+60+57+33 \end{bmatrix} = \begin{bmatrix} 80 \\ 103 \\ 135 \\ 174 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 2 \\ 25 \\ 5 \\ 18 \end{bmatrix} = \begin{bmatrix} C \\ Z \\ F \\ S \end{bmatrix}$

Blok IX: $\begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 3 \\ 2 & 2 & 2 & 3 \\ 2 & 3 & 3 & 3 \end{bmatrix} \begin{bmatrix} 0 \\ 10 \\ 14 \\ 14 \end{bmatrix} = \begin{bmatrix} 0+10+28+28 \\ 0+10+28+42 \\ 0+20+28+42 \\ 0+30+42+42 \end{bmatrix} = \begin{bmatrix} 66 \\ 80 \\ 90 \\ 114 \end{bmatrix}$ dengan modulo 26 $\begin{bmatrix} 14 \\ 2 \\ 12 \\ 10 \end{bmatrix} = \begin{bmatrix} O \\ C \\ M \\ K \end{bmatrix}$

Sehingga diperoleh teks kode sebagai berikut:

KCVMNFQBTQKJYPAJUOYLBYDYHOPWCZFSOCMK

**b. Proses Dekripsi**

Pada proses dekripsi ini teks kode akan diubah menjadi teks asli atau seperti bentuk semula.

Teks kode: KCVMNFQBTQKJYPAJUOYLBYDYHOPWCZFSOCMK

Kunci: : $\begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 3 \\ 2 & 2 & 2 & 3 \\ 2 & 3 & 3 & 3 \end{bmatrix}$

$K^{-1}$: : $\begin{bmatrix} -3 & 3 & -3 & 2 \\ 3 & -4 & 4 & -2 \\ -3 & 4 & -5 & 3 \\ 2 & -2 & 3 & -2 \end{bmatrix}$ dengan modulo 26 $K^{-1}$: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix}$

Blok I: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 10 \\ 2 \\ 21 \\ 12 \end{bmatrix} = \begin{bmatrix} 230+6+483+24 \\ 30+44+84+288 \\ 230+8+441+36 \\ 20+48+63+288 \end{bmatrix} = \begin{bmatrix} 743 \\ 446 \\ 715 \\ 419 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 15 \\ 4 \\ 13 \\ 3 \end{bmatrix} = \begin{bmatrix} P \\ E \\ N \\ D \end{bmatrix}$$

Blok II: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 13 \\ 5 \\ 16 \\ 1 \end{bmatrix} = \begin{bmatrix} 299+15+368+2 \\ 39+110+64+24 \\ 299+20+336+3 \\ 26+120+48+24 \end{bmatrix} = \begin{bmatrix} 684 \\ 237 \\ 658 \\ 218 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 8 \\ 3 \\ 8 \\ 10 \end{bmatrix} = \begin{bmatrix} I \\ D \\ I \\ K \end{bmatrix}$$

Blok III: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 19 \\ 23 \\ 10 \\ 9 \end{bmatrix} = \begin{bmatrix} 437+69+230+18 \\ 57+506+40+216 \\ 437+92+210+27 \\ 38+552+30+216 \end{bmatrix} = \begin{bmatrix} 754 \\ 816 \\ 766 \\ 836 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 0 \\ 13 \\ 12 \\ 4 \end{bmatrix} = \begin{bmatrix} A \\ N \\ M \\ E \end{bmatrix}$$

Blok VI: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 24 \\ 15 \\ 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 552+45+0+18 \\ 72+330+0+216 \\ 552+60+0+27 \\ 48+360+0+216 \end{bmatrix} = \begin{bmatrix} 615 \\ 618 \\ 639 \\ 624 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 17 \\ 20 \\ 15 \\ 0 \end{bmatrix} = \begin{bmatrix} R \\ U \\ P \\ A \end{bmatrix}$$

Blok V: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 20 \\ 14 \\ 24 \\ 11 \end{bmatrix} = \begin{bmatrix} 460+42+552+22 \\ 60+308+96+264 \\ 460+56+504+33 \\ 40+336+72+264 \end{bmatrix} = \begin{bmatrix} 1076 \\ 728 \\ 1053 \\ 712 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 10 \\ 0 \\ 13 \\ 10 \end{bmatrix} = \begin{bmatrix} K \\ A \\ N \\ K \end{bmatrix}$$

Blok VI: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 1 \\ 24 \\ 3 \\ 24 \end{bmatrix} = \begin{bmatrix} 23+72+69+48 \\ 3+528+12+576 \\ 23+96+63+72 \\ 2+576+9+576 \end{bmatrix} = \begin{bmatrix} 212 \\ 1119 \\ 254 \\ 1163 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 4 \\ 1 \\ 20 \\ 19 \end{bmatrix} = \begin{bmatrix} E \\ B \\ U \\ T \end{bmatrix}$$

Blok VII: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 7 \\ 14 \\ 15 \\ 22 \end{bmatrix} = \begin{bmatrix} 161+42+345+44 \\ 21+308+60+528 \\ 161+56+315+66 \\ 14+336+45+528 \end{bmatrix} = \begin{bmatrix} 592 \\ 917 \\ 598 \\ 923 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 20 \\ 7 \\ 0 \\ 13 \end{bmatrix} = \begin{bmatrix} U \\ H \\ A \\ N \end{bmatrix}$$

Blok VIII: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 2 \\ 25 \\ 5 \\ 18 \end{bmatrix} = \begin{bmatrix} 46+75+115+36 \\ 6+550+20+432 \\ 46+100+105+54 \\ 4+600+15+432 \end{bmatrix} = \begin{bmatrix} 272 \\ 1008 \\ 305 \\ 1051 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 12 \\ 20 \\ 19 \\ 11 \end{bmatrix} = \begin{bmatrix} M \\ U \\ T \\ L \end{bmatrix}$$

Blok IX: $\begin{bmatrix} 23 & 3 & 23 & 2 \\ 3 & 22 & 4 & 24 \\ 23 & 4 & 21 & 3 \\ 2 & 24 & 3 & 24 \end{bmatrix} \begin{bmatrix} 14 \\ 2 \\ 12 \\ 10 \end{bmatrix} = \begin{bmatrix} 322+6+276+20 \\ 42+44+48+240 \\ 322+8+252+30 \\ 28+48+36+240 \end{bmatrix} = \begin{bmatrix} 624 \\ 374 \\ 612 \\ 352 \end{bmatrix}$ dengan modulo 26

$$\begin{bmatrix} 0 \\ 10 \\ 14 \\ 14 \end{bmatrix} = \begin{bmatrix} A \\ K \\ O \\ O \end{bmatrix}$$

Dari proses penjabaran di atas yaitu dengan menggunakan kunci matriks yang elemennya $2x2$ pada proses enkripsi dan proses dekripsi dengan pembagian blok masing-masing 2 huruf, menggunakan kunci matriks yang elemennya $3x3$ pada proses enkripsi dan proses dekripsi dengan pembagian blok masing-masing 3 huruf, menggunakan kunci matriks yang elemennya $4x4$ pada proses enkripsi dan proses dekripsi dengan pembagian blok masing-masing 4 huruf, dari segi proses dapat dilihat bahwa proses enkripsi dan proses dekripsi yang menggunakan kunci matriks yang elemennya lebih banyak maka peluang keamanannya lebih besar atau semakin banyak jumlah elemen matriks maka semakin kuat keamanannya, dengan kata lain untuk memperkuat keamanan bisa dengan memperbanyak elemen matriks kunci. Dalam segi hasil sama saja baik dengan menggunakan matriks yang elemennya sedikit maupun banyak.

## 4.2 Proses Penyandian Caesar Cipher

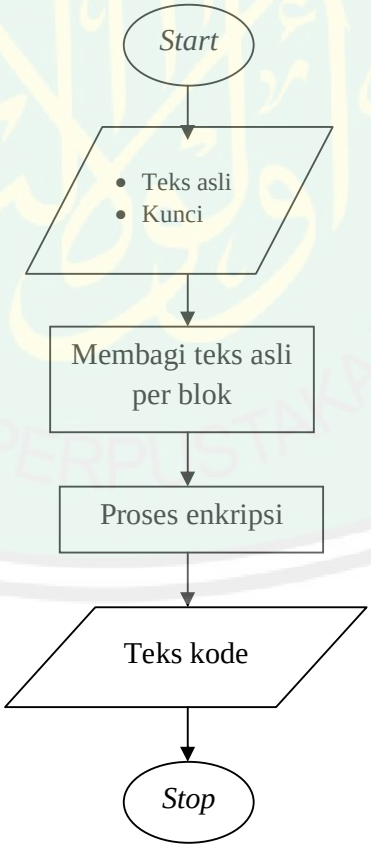
Teknik Caesar Cipher mempunyai banyak cara kemudian pada perkembangannya algoritma kode caesar memberikan suatu gagasan baru untuk menggunakan kunci lain yang disebut *polyalphabetic*. Kunci bisa jadi nama, alamat atau apa saja yang diinginkan oleh pengirim pesan dengan kunci tidak ada

pengulangan huruf. Di dalam cara ini ada yang menggunakan satu kunci, dua kunci, atau lebih dari satu kunci/beberapa kunci. Metode ini terdiri dari tiga bagian, yaitu blok, karakter, dan zig-zag (Ariyus, 2008:54). Namun di dalam penelitian ini peneliti hanya membahas satu bagian saja, yaitu bagian blok.

### 4.2.1 Proses Enkripsi Dekripsi Metode Blok

**a. Proses Enkripsi**

Metode untuk mengenkripsi dengan menggunakan blok adalah dengan membagi jumlah teks asli menjadi blok-blok yang ditentukan, sesuai dengan keinginan pengirim pesan. Metode ini proses enkripsi dan dekripsi sama (Ariyus, 2008:56). Pada proses ini akan ditampilkan dalam *flowchart* di bawah ini:




Gambar 4.3 Proses Enkripsi Caesar Blok

Contoh: PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

Kunci : 1. SURABAYA

2. BANDUNG

3. JAKARTA

Teks asli dibagi menjadi blok-blok dan setiap blok berisi beberapa karakter sesuai dengan keinginan pengirim pesan. Pada penelitian ini peneliti membagi teks asli menjadi beberapa macam blok dan beberapa macam jumlah karakter yang berbeda, diantaranya adalah menjadi 9 blok yang bersisi 4 karakter tiap bloknya, 7 blok 5 karakter, 6 blok 6 karakter, 5 blok 7 karakter, dan 5 blok 8 karakter. Kemudian untuk aturan kunci peneliti menggunakan urutan yang berbeda-beda juga yaitu:

9 blok 4 karakter dengan aturan kunci K1, K2, K3, K3, K2, K1 dst.

7 blok 5 karakter dengan aturan kunci K3, K3, K2, K2, K1, K1 dst.

6 blok 6 karakter dengan aturan kunci K2, K1, K3, K1, K2, K1, K3, K1 dst.

5 blok 7 karakter dengan aturan kunci K1, K2, K3, K1, K2, K3 dst.

5 blok 8 karakter dengan aturan kunci K3, K2, K1, K3, K2, K1, K3, K2, K1 dst.

Contoh: PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

1. Misalnya kalimat tersebut dibagi menjadi 9 blok, tiap blok berisi 4 karakter. Jika blok terakhir tidak mencukupi maka ditambah dengan karakter lain yang diinginkan. Penulis akan menambah karakter yang kurang dengan huruf O.

| PEND | IDIK | ANME | RUPA | KANK |
|---|---|---|---|---|
| K1 | K2 | K3 | K3 | K2 |

| EBUT | UHAN | MUTL | AKOO |
|---|---|---|---|
| K1 | K1 | K2 | K3 |

K1 (kunci di depan )

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | U | R | A | B | Y | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | T | V | W | X | Z |

K2 (kunci di tengah)

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | E | F | H | I | J | K | L | M | O | B | A | N | D | U | G | P | Q | R | S | T | V | W | X | Y | Z |

K3 (kunci di belakang)

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | C | D | E | F | G | H | I | L | M | N | O | P | Q | S | U | V | W | X | Y | Z | J | A | K | R | T |

Dari contoh di atas diperoleh teks kode sebagai berikut:

LBJA MHMB BQPF WZUB BCDB BUQP QDSJ NTSA BNSS

Sehingga menjadi:

LBJAMHMBBQPFWZUBBCDBBUQPQDSJNTSABNSS

2. Misalnya kalimat tersebut dibagi menjadi 7 blok, tiap blok berisi 5 karakter.

Jika blok terakhir tidak mencukupi maka ditambah dengan huruf O.

| PENDI | DIKAN | MERUP | AKANK | EBUTU |
|---|---|---|---|---|
| K3 | K3 | K2 | K2 | K1 |

| HANMU | TLAKO |
|---|---|
| K1 | K3 |

Dari contoh di atas diperoleh teks kode sebagai berikut:

UFQEL ELNBQ NIQTG CBCDB BUQPQ DSJIQ YOBNS

Sehingga menjadi:

UFQELELNBQNIQTGCBCDBBUQPQDSJIQYOBNS

3. Misalnya kalimat tersebut dibagi menjadi 6 blok, tiap blok berisi 6 karakter.

Jika blok terakhir tidak mencukupi maka ditambah dengan huruf O.

| PENDID | IKANME | RUPAKA | NKEBUT | UHANMU |
|---|---|---|---|---|
| K2 | K1 | K3 | K1 | K2 |

| TLAKOO |
|---|
| K1 |

Dari contoh di atas diperoleh teks kode sebagai berikut:

GIDHNH EGSJIB WZUBNB JGBUQP TLCDNT PHSGKK

Sehingga menjadi:

GIDHNHEGSJIBWZUBNBJGBUQPTLCDNTPHSGKK

4. Misalnya kalimat tersebut dibagi menjadi 5 blok, tiap blok berisi 7 karakter. Jika blok terakhir tidak mencukupi maka ditambah dengan huruf O.

| PENDIDI | KANMERU | PAKANKE | BUTUHAN | MUTLAKO |
|---|---|---|---|---|
| K1 | K2 | K3 | K1 | K2 |

Dari contoh di atas diperoleh teks kode sebagai berikut:

LBJAEAE BCDNIQT UBNBQNF UQPQDSJ NTSACBU

Sehingga menjadi:

LBJAEAEBCDNIOTUBNBPNFUQPQDSJNTSACBU

5. Misalnya kalimat tersebut dibagi menjadi 5 blok, tiap blok berisi 8 karakter. Jika blok terakhir tidak mencukupi maka ditambah dengan huruf O.

| PENDIDIK | ANMERUPA | KANKEBUT | UHANMUTL | AKOOOOOO |
|---|---|---|---|---|
| K3 | K2 | K1 | K3 | K2 |

Dari contoh di atas diperoleh teks kode sebagai berikut:

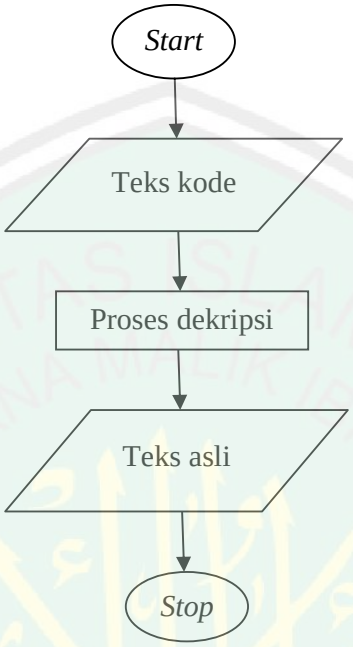
UFQELELN CDNIQTGC GSJGBUQP ZIBQPZYO CBUUUUUU

Sehingga menjadi:

UFQELELNCDNIOTGCGSJGBUQPZIBQPZYOCBUUUUUU

**b. Proses Dekripsi**

Pada proses dekripsi ini yaitu mengubah teks kode menjadi teks asli seperti semula. Pada proses dekripsi peneliti akan menampilkan dalam bentuk *flowchart* di bawah ini:




Gambar 4.4 Proses Dekripsi Caesar Blok

Dalam hal ini peneliti menguraikannya menjadi 5 cara:

1. Kalimat yang dibagi menjadi 9 blok yang berisi 4 karakter tiap bloknya.

| LBJA | MHMB | BQPF | WZUB | BCDB |
|---|---|---|---|---|
| K1 | K2 | K3 | K3 | K2 |

| BUQP | QDSJ | NTSA | BNSS |
|---|---|---|---|
| K1 | K1 | K2 | K3 |

PEND IDIK ANME RUPA KANK EBUT UHAN MUTL AKOO

Sehingga menjadi:

PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

2. Kalimat yang dibagi menjadi 7 blok yang berisi 5 karakter tiap bloknya.

| UFQEL | ELNBQ | NIQTG | CBCDB | BUQPQ |
|---|---|---|---|---|
| K3 | K3 | K2 | K2 | K1 |

| DSJIQ | YOBNS |
|---|---|
| K1 | K3 |

PENDI DIKAN MERUP AKANK EBUTU HANMU TLAKO

Sehingga menjadi:

PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

3. Kalimat yang dibagi menjadi 6 blok yang berisi 6 karakter tiap bloknya.

| GIDHNH | EGSJIB | WZUBNB | JGBUQP | TLCDNT |
|---|---|---|---|---|
| K2 | K1 | K3 | K1 | K2 |

| PHSGKK |
|---|
| K1 |

PENDID IKANME RUPAKA NKEBUT UHANMU TLAKOO

Sehingga menjadi:

PENDIDIKAN MERUPAKAN MUTLAK

4. Kalimat yang dibagi menjadi 5 blok yang berisi 7 karakter tiap bloknya.

| LBJAEAE | BCDNIQT | UBNBQNF | UQPQDSJ | NTSACBU |
|---|---|---|---|---|
| K1 | K2 | K3 | K1 | K2 |

PENDIDI KANMERU PAKANKE BUTUHAN MUTLAKO

Sehingga menjadi:

PENDIDIKAN MERUPAKAN MUTLAK

5. Kalimat yang dibagi menjadi 5 blok yang berisi 8 karakter tiap bloknya.

| UFQELELN | CDNIOTGC | GSJGBUQP | ZIBQPZYO | CBUUUUUU |
|---|---|---|---|---|
| K3 | K2 | K1 | K3 | K2 |

PENDIDIK ANMERUPA KANKEBUT UHANMUTL AKOOOOOO

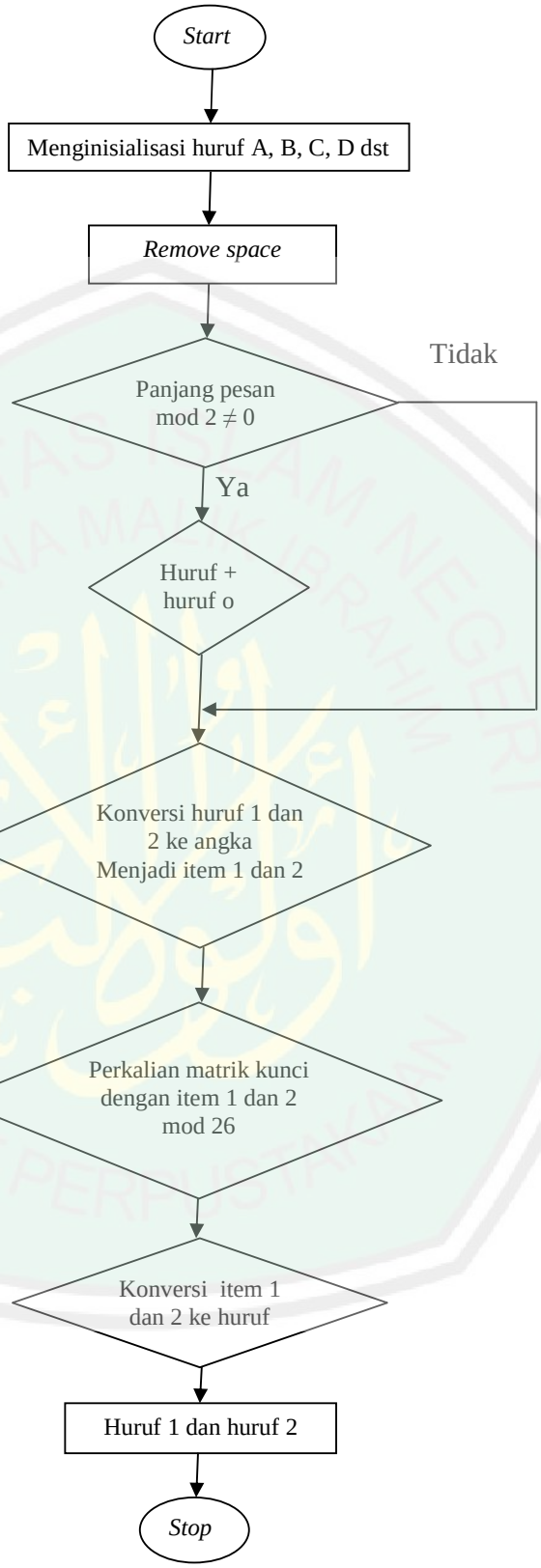
Sehingga menjadi:

PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK

Dari penjabaran di atas dapat diketahui bahwa di dalam metode Caesar Cipher misal teks asli dibagi menjadi berapapun blok dan tiap bloknya terdiri dari berapapun jumlah karakter hurufnya dalam segi proses enkripsi dan proses dekripsi tidak ada perbedaan, untuk perbedaan peracakan kunci dalam proses enkripsi dan dekripsi semakin tidak beraturan aturan kunci yang dipakai maka semakin kecil peluang orang lain untuk dapat membukanya. Dalam segi hasil tidak ada perbedaan.

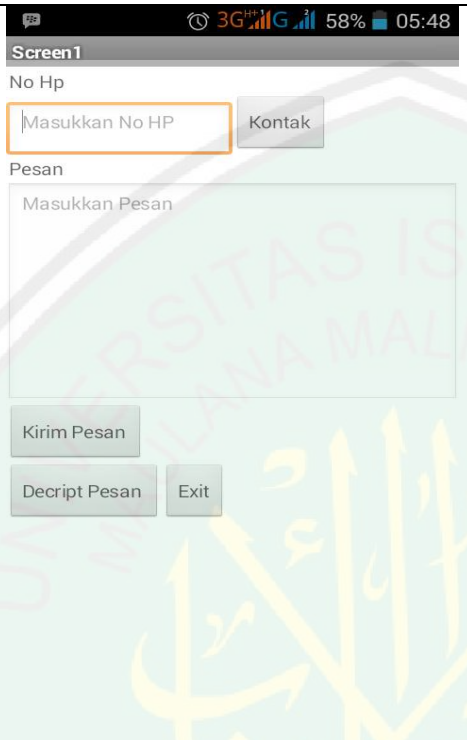
### 4.3 Simulasi Hill Cipher dan Caesar Cipher dengan Appinventor

Pada bab ini simulasi dilakukan dengan menggunakan aplikasi Appinventor. Sebelum membuat program terlebih dahulu dibuat *flowchart*. Di bawah ini adalah *flowchart* Hill Cipher:

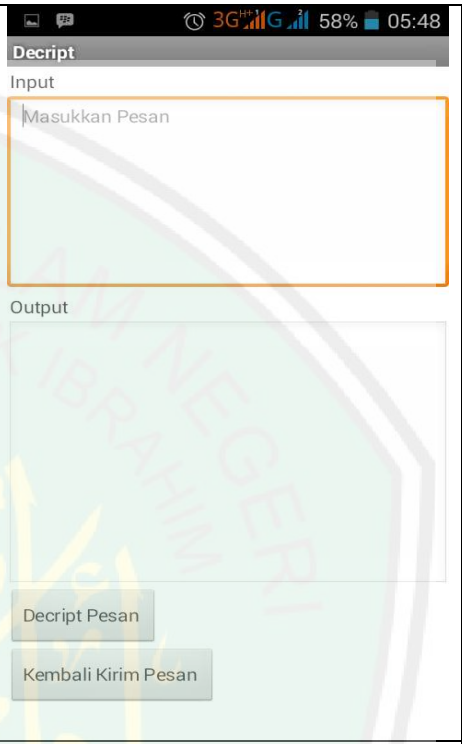



Gambar 4.5 *Flowchart* Program Hill Cipher

Gambar *form* awal yang akan digunakan simulasi untuk mengirim pesan akan ditunjukkan pada Gambar 4.6 dan untuk mendekripsikan pesan ditunjukkan pada Gambar 4.7.




Gambar 4.6 *Form* Mengirim Pesan Hill Cipher




Gambar 4.7 *Form* Mendekripsikan Teks Hill Cipher

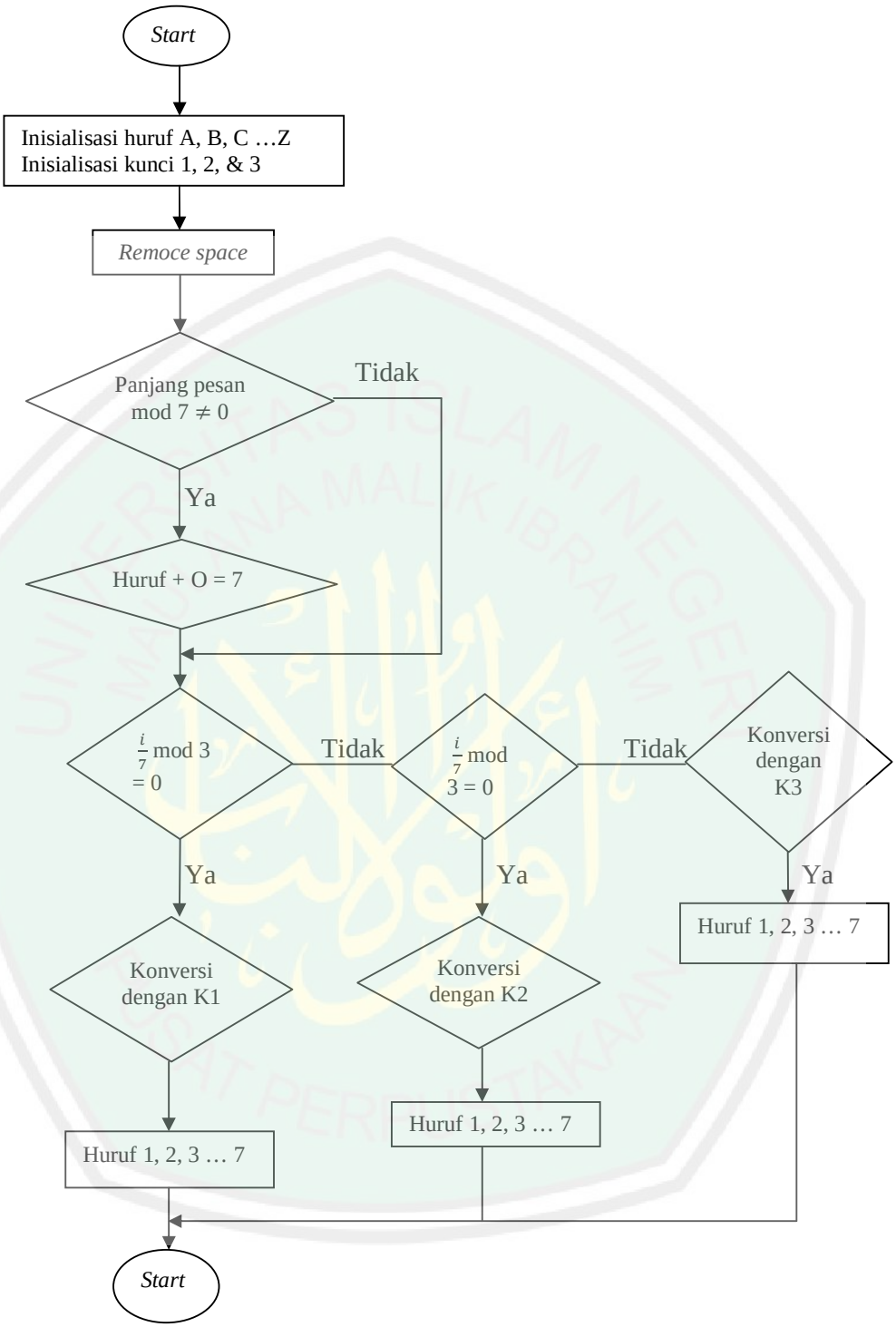
Dari *form* di atas dapat dilakukan simulasi Hill Cipher dengan mengirim pesan yaitu langkah pertama masukkan nomor HP yang dituju di kotak pertama atau dengan menekan tombol kontak untuk mencari nomor yang tersimpan di kontak, kemudian menulis pesan di kotak pesan, selanjutnya untuk mengirim pesan dengan menekan tombol kirim pesan. Contohnya akan ditunjukkan pada Gambar 4.8 misal akan mengirim pesan yang bertuliskan PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK.


Gambar 4.8 Contoh Mengirim Pesan Hill Cipher

Kemudian orang yang menerima pesan akan menerima pesan dalam bentuk teks acak yaitu QTJQZLUSNNKQQLEPUKEXLFTNJBNNGGTEEK, untuk bisa mendekripsikan berarti harus mempunyai aplikasi yang sama dengan orang yang mengirim pesan. Setelah itu masukkan teks acak tersebut pada kotak *input* dan menekan tombol *decript* pesan maka akan keluar di *output* kalimat yang semula yaitu PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK. Proses ini akan ditunjukkan pada Gambar 4.9.

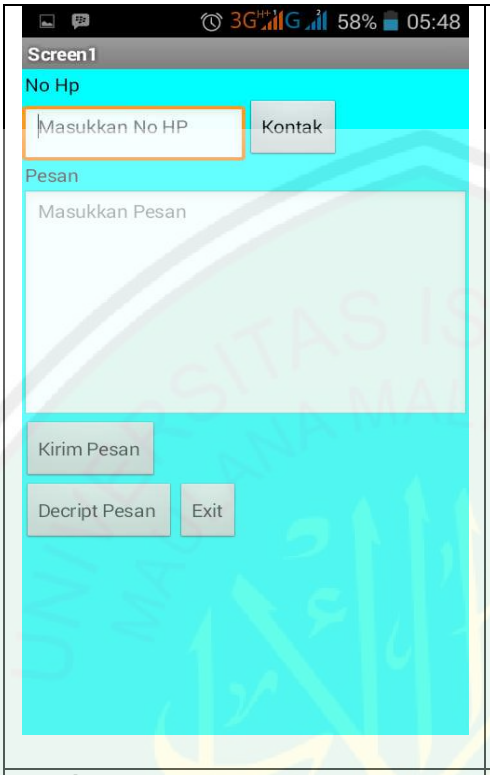

Gambar 4.9 Contoh Mengirim Pesan Hill Cipher

Untuk simulasi metode Caesar Cipher sama dengan metode Hill Cipher, yaitu langkah pertama harus dibuat *flowchart* terlebih dahulu, *flowchart* metode Caesar Cipher sebagai berikut:




Gambar 4.10 *Flowchart* program Caesar Cipher

*Form* simulasi Caesar Cipher akan ditunjukkan pada Gambar 4.11 untuk mengirim pesan dan pada Gambar 4.12 untuk mendekripsikan pesan.




Gambar 4.11 *Form* Mengirim Pesan Caesar Cipher


Gambar 4.12 *Form* Mendekripsikan Teks Caesar Cipher

Dari *form* di atas dapat dilakukan simulasi Caesar Cipher yang mana caranya sama dengan simulasi Hill Cipher, yaitu langkah pertama dengan masukkan nomor HP yang dituju di kotak pertama atau dengan menekan tombol kontak untuk mencari nomor yang tersimpan di kontak, kemudian menulis pesan di kotak pesan, selanjutnya untuk mengirim pesan dengan menekan tombol kirim pesan. Contohnya akan ditunjukkan pada Gambar 4.13 misal akan mengirim pesan yang bertuliskan PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK.


Gambar 4.13 Contoh Mengirim Pesan Caesar Cipher

Kemudian orang yang menerima pesan akan menerima pesan dalam bentuk teks acak yaitu LBJAEAEBCDNIOTUBNBPNFUQPQDSJNTSACBU, untuk bisa mendekripsikan berarti harus mempunyai aplikasi yang sama dengan orang yang mengirim pesan. Setelah itu masukkan teks acak tersebut pada kotak *input* dan menekan tombol *decript* pesan maka keluar di *output* kalimat yang semula yaitu PENDIDIKAN MERUPAKAN KEBUTUHAN MUTLAK. Proses ini akan ditunjukkan pada Gambar 4.14.


Gambar 4.14 Contoh Mengirim Pesan Caesar Cipher

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

### 4.4 Integrasi Agama dengan Penyandian

Penelitian ini membahas tentang penyandian kata, penyandian biasanya digunakan untuk menyandikan data-data guna untuk menyimpan data yang bersifat rahasia, yang tidak semua orang berhak mengetahui, ilmu matematika yang membahas tentang penyandian sering disebut dengan kriptografi. Kriptografi ini yang menyandikan teks asli menjadi teks kode berupa teks yang tidak bisa dibaca atau acak.

Begitu juga semua manusia punya sesuatu yang disembunyikannya, apakah yang disembunyikan itu berupa hal positif seperti perbuatan baik, tekad

untuk melakukan sesuatu, cita-cita, harapan ataupun yang negatif seperti perbuatan dosa dan maksiat, hal tersebut disebut dengan rahasia. Rahasia yang disimpan manusia bisa saja hanya berkaitan dengan kepentingan pribadi dan keluarga, teman, dan mungkin rahasia negara. Bahkan Allah Swt. sebagai *Khaliq* juga menentukan nasib hamba-Nya tanpa diketahui oleh yang lain, semua menjadi rahasia Allah Swt. (Denros, 2013:1).

Dari pernyataan di atas bahwa semua hal yang bersifat rahasia itu harus disimpan baik-baik agar tidak semua orang yang tidak berhak mengetahui menjadi mengetahui. Islam juga menganjurkan untuk menyimpan rahasia, yang dijelaskan dalam al-Quran surat an-Nisa' ayat 58 yang berbunyi:

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-Nisa'/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:

اَدِّالْاَمَانَةَ إِلَى مَنِ ائْتَمَنَكَ, وَلَاتَخُنْ مَنْ خَانَكَ

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

Selain surat an-Nisa' ayat 58 di dalam al-Quran juga dijelaskan anjuran untuk menjaga pesan bersifat rahasia yang terdapat dalam surat al-Anfal ayat 27 yang berbunyi:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

*"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui" (QS. al-Anfal/8:27).*

Penyandian pesan juga sudah diterapkan pada saat turunnya wahyu kepada Nabi Muhammad, yaitu di dalam buku Ringkasan Shahih Bukhori hadits yang artinya:

> *Dari Aisyah Ummul Mukminin RA, bahwa Al Harits bin Hisyam RA bertanya kepada Rasulullah Saw., "Wahai Rasulullah, bagaimana caranya wahyu datang kepadamu?" Rasulullah Saw. menjawab, "kadang-kadang wahyu itu datang kepadaku seperti bunyi lonceng, itulah yang paling berat bagiku. Setelah bunyi itu berhenti, aku pun memahami apa yang dikatakan. Adakalanya malaikat menampakkan diri kepadaku dalam bentuk seorang laki-laki lalu berbicara kepadaku, maka aku memahami apa yang diucapkan. "Aisyah RA berkata, "aku pernah melihat beliau ketika wahyu turun kepadanya di suatu hari yang sangat dingin, yang mana setelah wahyu itu selesai turun, kelihatan dahi beliau bersimpah peluh."*

Dari hal tersebut dapat disimpulkan bahwa kita berkewajiban untuk menyimpan rahasia yang tidak semua orang boleh mengetahuinya. Hal itu juga sudah dianjurkan oleh Islam dan disebutkan di dalam al-Quran.

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil pembahasan, dapat diperoleh kesimpulan sebagai berikut:

1. Di dalam metode Hill Cipher perbandingan antara pemakaian kunci matriks $2x2$, $3x3$, dan $4x4$, adalah dalam segi prosesnya yang menggunakan matriks yang elemennya lebih banyak maka semakin kuat keamanannya, namun di dalam sisi hasil akan sama saja.
2. Di dalam metode Caesar Cipher perbandingan antara jumlah blok atau jumlah karakter tiap bloknya dalam proses enkripsi dan dekripsi adalah sama. Untuk perbedaan peracakan kunci dalam proses enkripsi dan dekripsi semakin tidak beraturan aturan kunci yang dipakai maka semakin kecil peluang orang lain untuk dapat membukanya. Untuk segi hasilnya tidak ada perbedaan.
3. Penyandian metode Hill Cipher dan Caesar Cipher dapat dibuat simulasi dengan menggunakan aplikasi Appinventor dan simulasi ini dapat digunakan oleh orang lain dengan mudah.
4. Penelitian ini tentang penyandian yang artinya menjaga keamanan data atau menyembunyikan data yang bersifat rahasia agar tidak diketahui orang yang tidak berhak, maka aturan tersebut juga terbukti telah diperintahkan di dalam al-Quran yaitu salah satunya yang terdapat di dalam surat an-Nisa' ayat 58 yang berbunyi:

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-Nisa'/4:58).*

Maka dari itu di dalam kehidupan sehari-hari pun kita harus menjaga rahasia diri sendiri atau orang lain, karena semua manusia punya sesuatu yang disembunyikannya, apakah yang disembunyikan itu berupa hal positif seperti perbuatan baik, tekad untuk melakukan sesuatu, cita-cita, harapan ataupun yang negatif seperti perbuatan dosa dan maksiat, hal tersebut disebut dengan rahasia. Rahasia yang disimpan manusia bisa saja hanya berkaitan dengan kepentingan pribadi, keluarga, teman, dan mungkin rahasia negara.

## 5.2 Saran

Pada penelitian ini peneliti menyadari bahwa masih banyak terdapat kekurangan, sehingga banyak yang perlu diperbaiki. Untuk penelitian selanjutnya, disarankan untuk menggunakan aplikasi program komputer yang lainnya, atau menggunakan metode kriptografi modern yang lebih kompleks.

## DAFTAR PUSTAKA


Anton, H. 1987. *Aljabar Linier Elementer (Edisi Kelima)*. Jakarta: Erlangga.

Arhami, M dan Desiani, A. 2005. *Pemrograman Matlab*. Yogyakarta: Andi Offset.

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.

Bakar, B.A. 2000. *Tafsir Ibnu Katsir juz 1.* Bandung: Sinar Baru Algensindo.

Bakar, B.A. 2001. *Tafsir Ibnu Kasir juz 5.* Bandung: Sinar Baru Algensindo.

Denros, M. 2013. *Bisa Menjaga Rahasia.* (Online): (http://gemirasolok.blogspot.com/2013/10/35-bisa-menjaga-rahasia.html), diakses 14 September 2013.

Gazali, W. 2005. *Matriks & Transformasi Linear*. Yogyakarta: Graha Ilmu.

Hadley, G. 1992. *Aljabar Linear*. Jakarta: Erlangga.

Hasugian, A.H. 2013. Implementasi Algoritma Hill Cipher dalam Penyandian Data. *Pelita Informatika Budi Darma*. 4: 2301-9425.

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

Munir, R. 2002. *Matematika Diskrit (Revisi Kelima).* Bandung: Informatika.

Saefullah, A dan Sa'adiyatulharamain, K. 2007. *Ringkasan Shahih Bukhori*. Jakarta: Pustaka azzam.

Simarmata, J. 2005. *Pengamanan Sistem Komputer*. Yogyakarta: Andi.

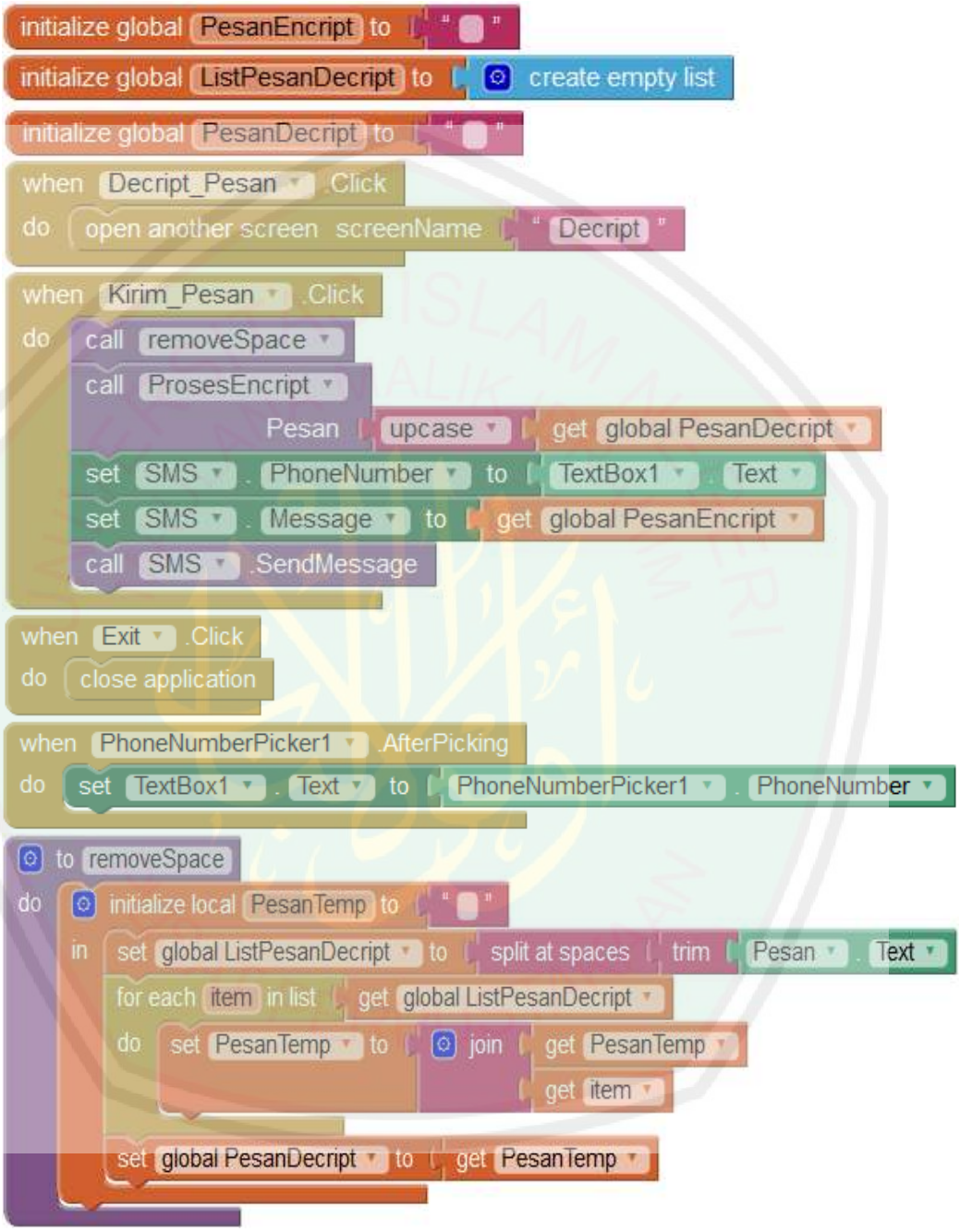
Sugiono. 2010. *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.

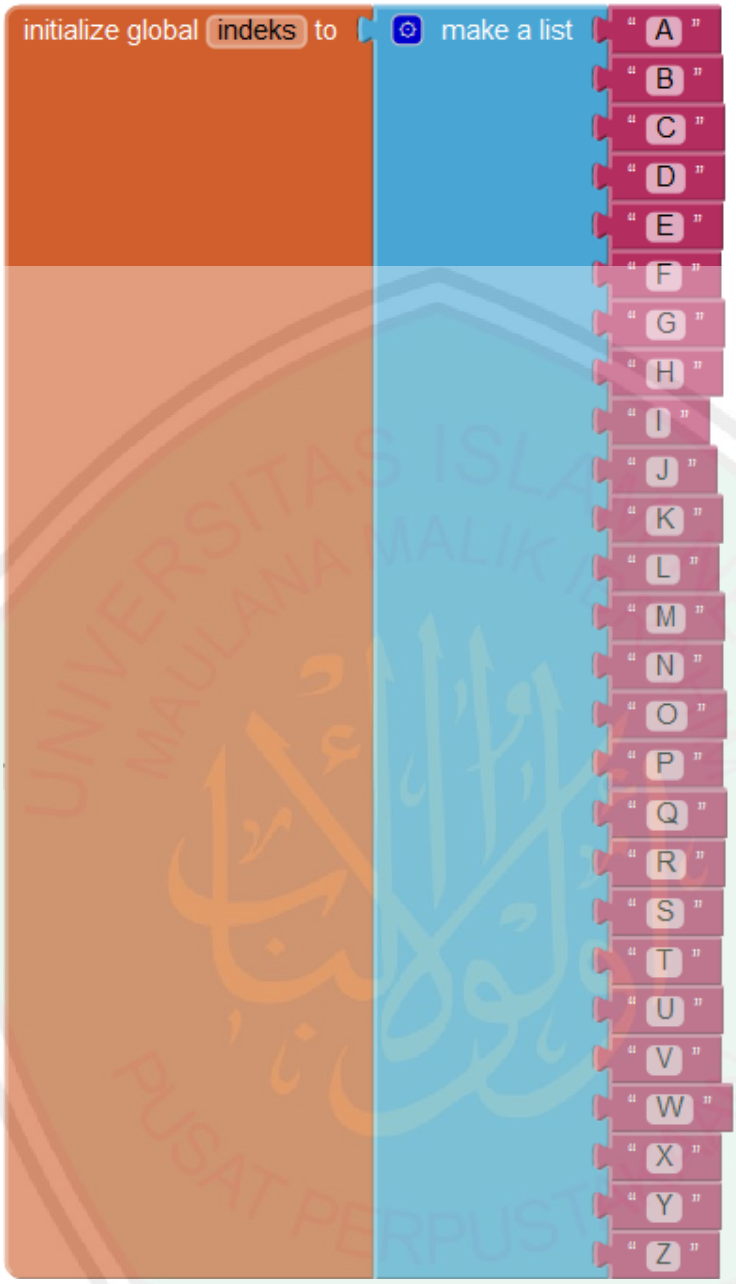
Supranto, J. 2003. *Pengantar Matrix (Edisi Revisi).* Jakarta: Rineka Cipta.

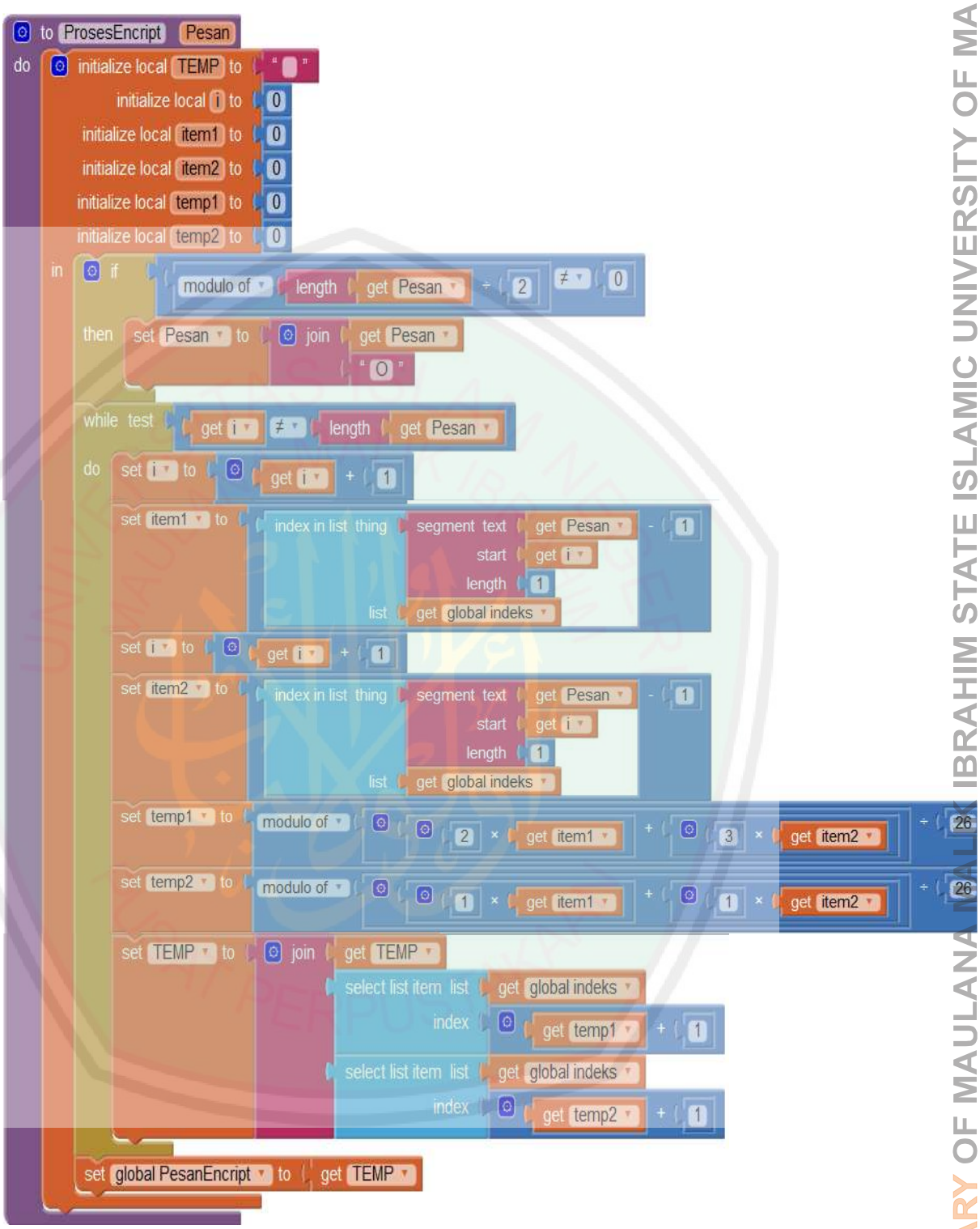
Widyanarko, A. 2009. *Studi dan Analisis Mengenai Hill Cipher, Teknik Kriptanalis dan Upaya Penanggulannya.* (Online): (http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2007-2008/Makalah1/MakalahIF5054-2007-A-026.pdf), diakses 18 Februari 2015.

LAMPIRAN

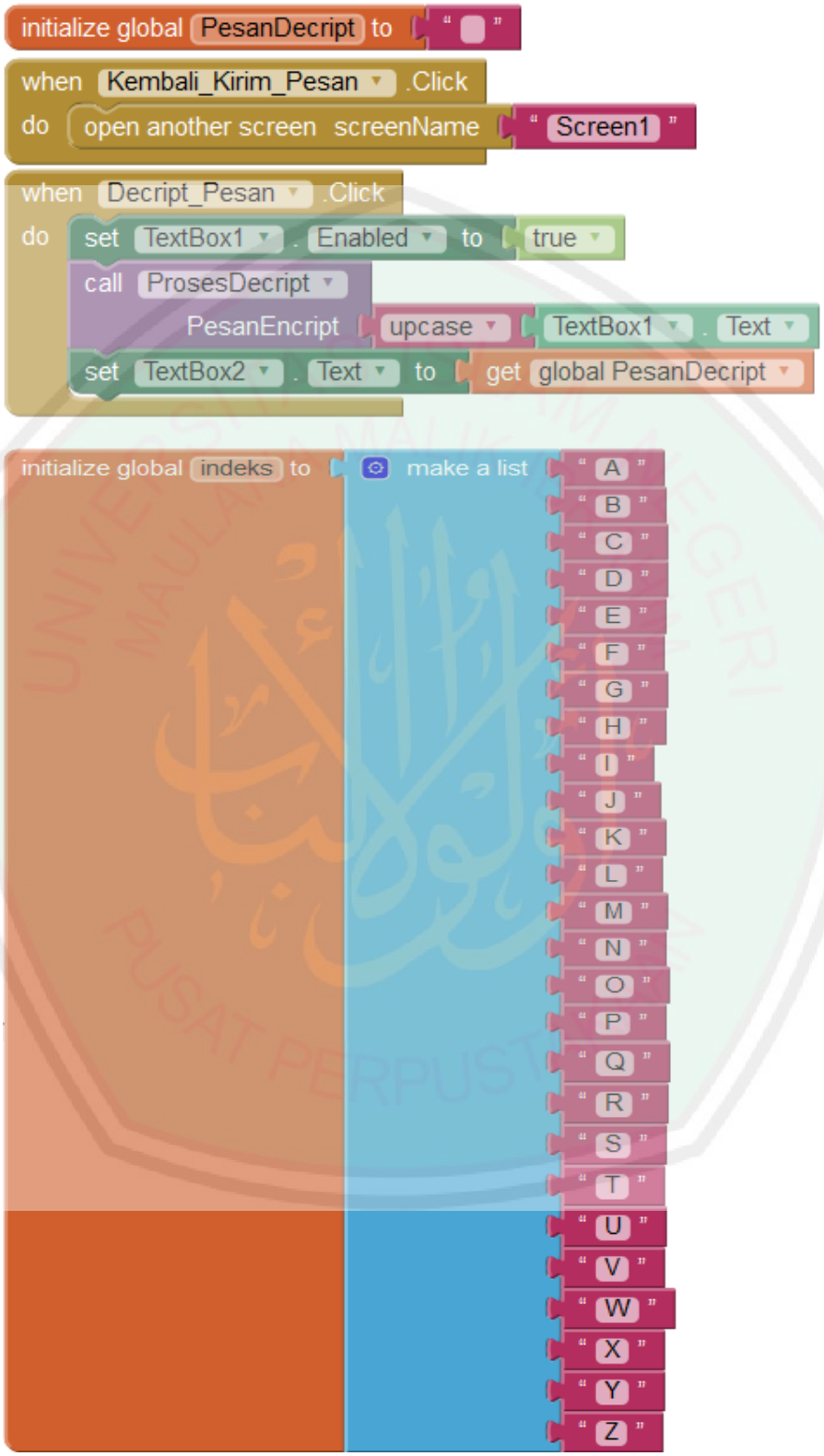
Lampiran 1. Enkripsi Hill Cipher

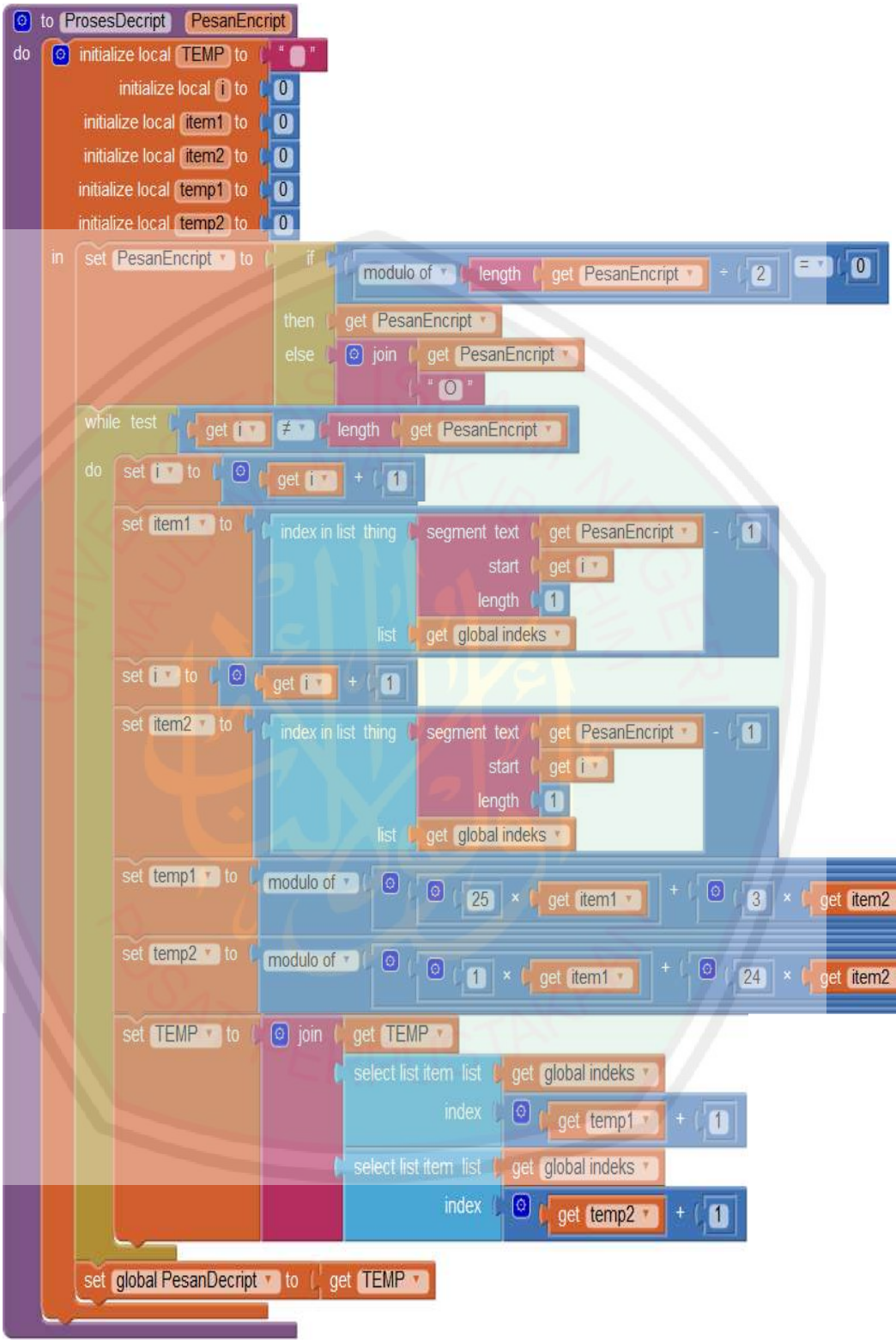




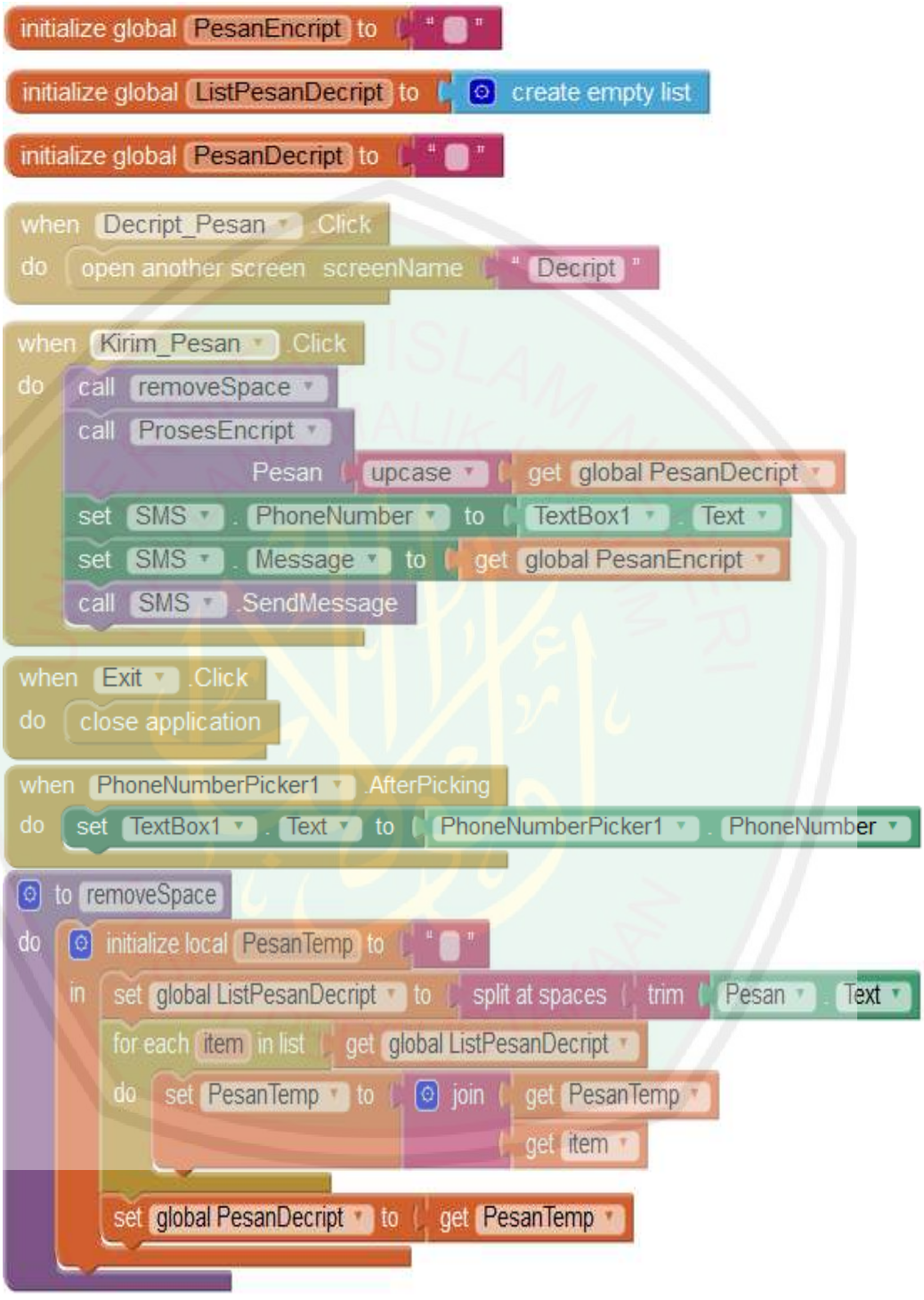


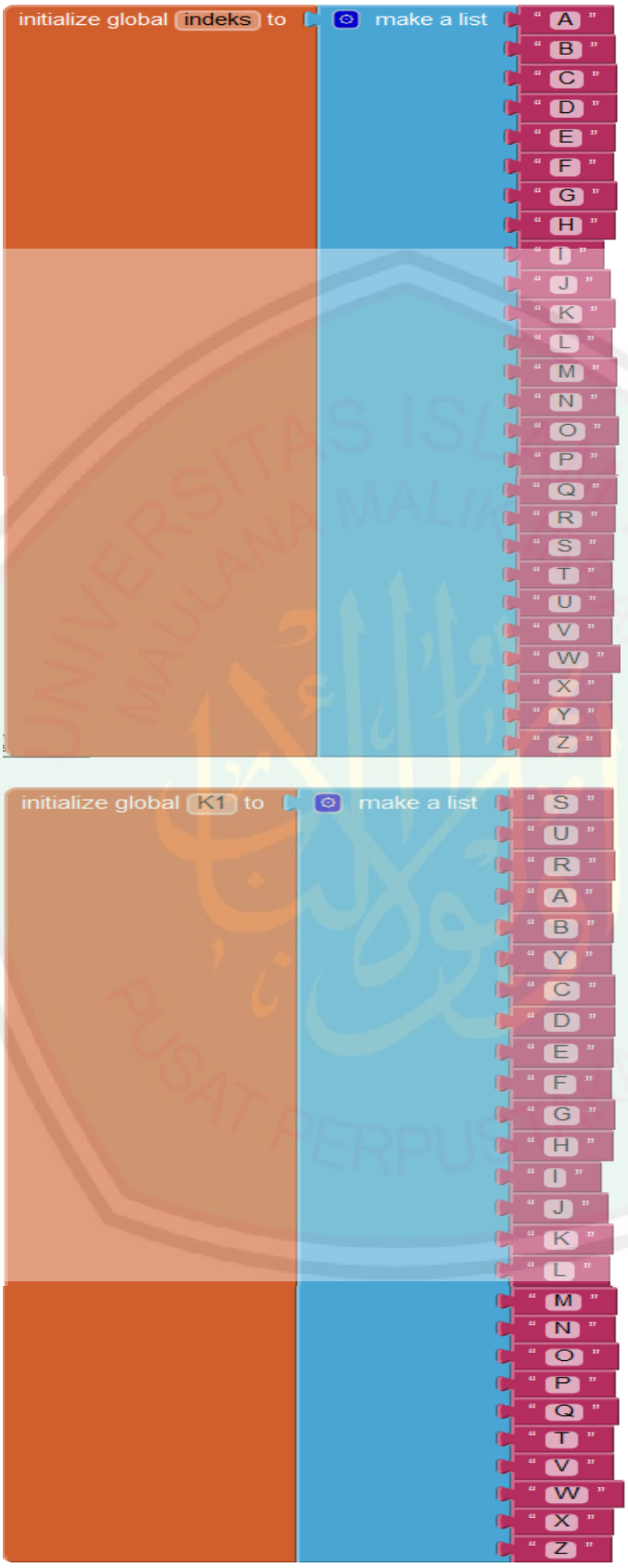
Lampiran 2. Dekripsi Hill Cipher

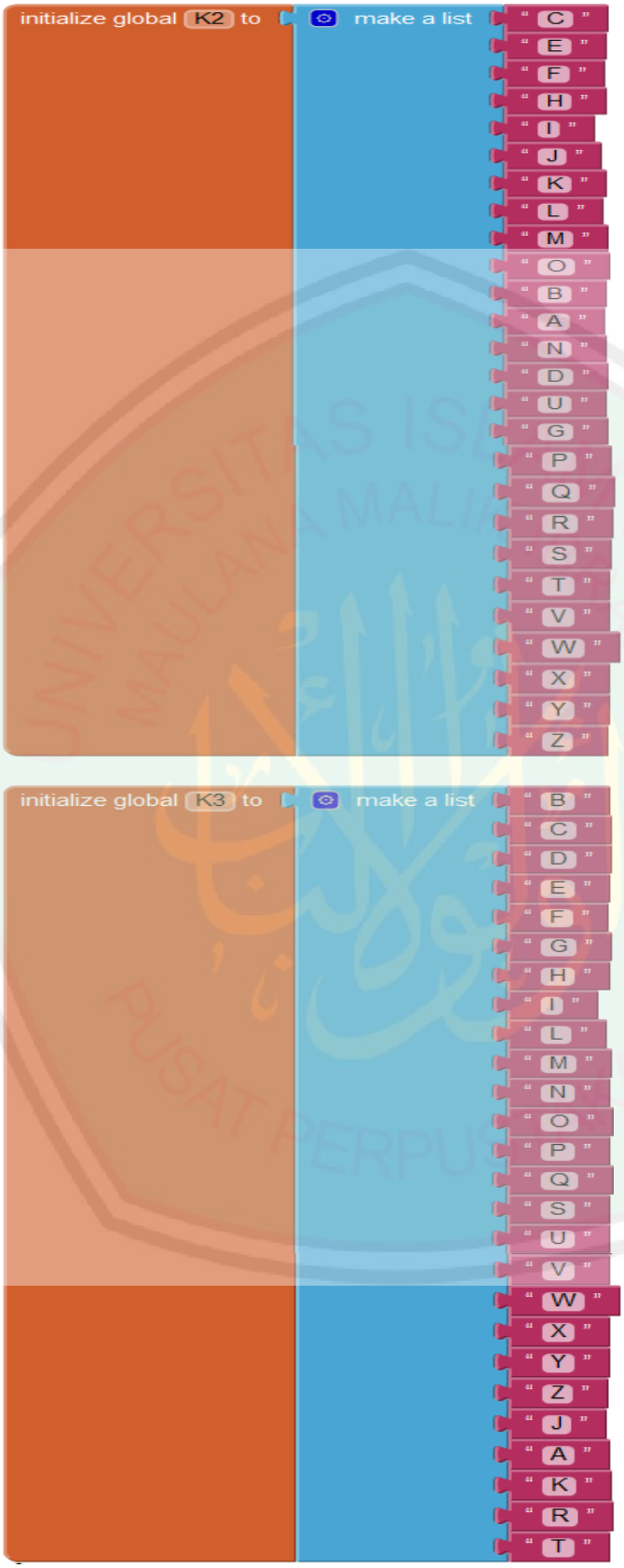


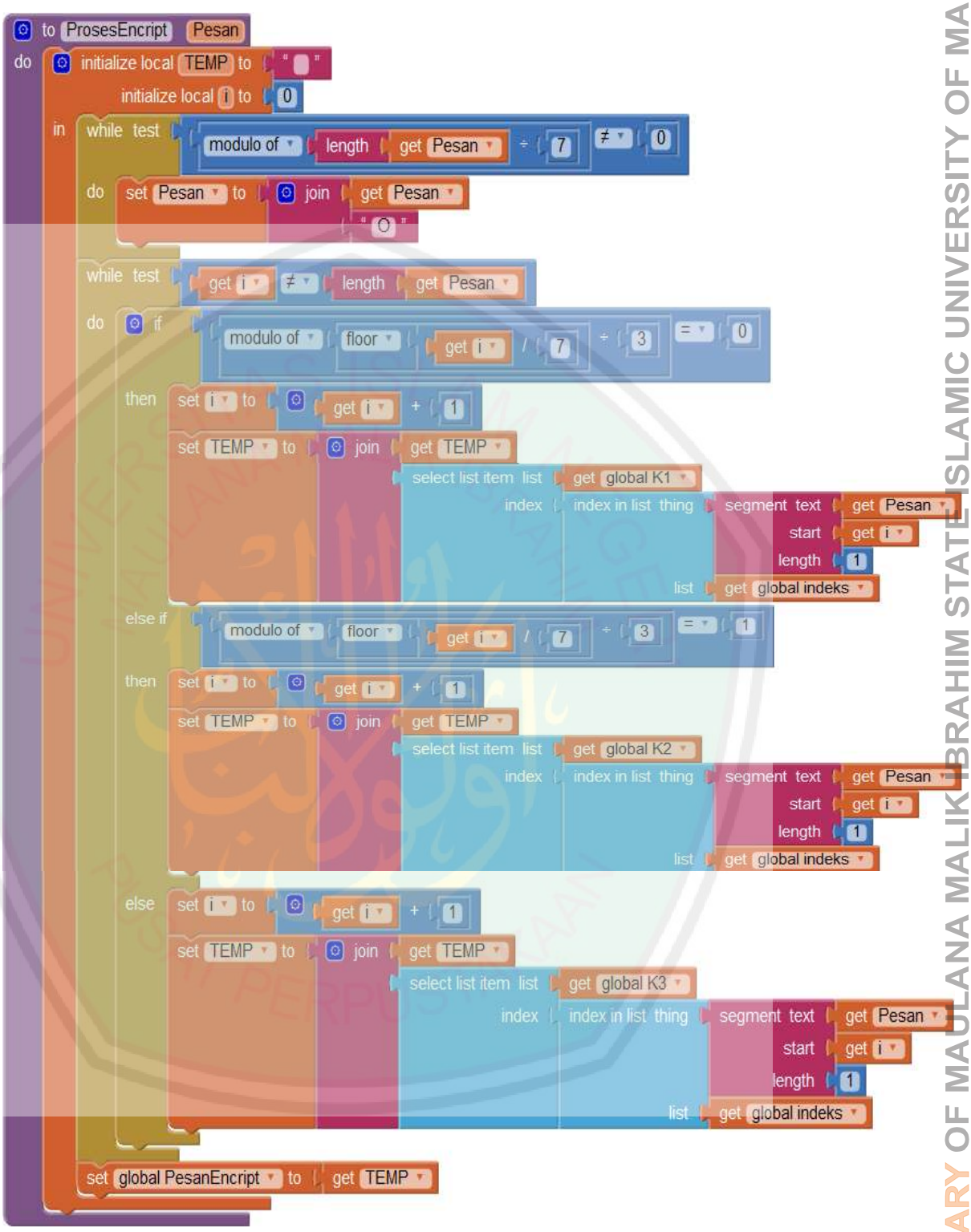


Lampiran 3. Enkripsi Caesar Cipher









4. Lampiran Dekripsi Caesar Cipher