ALGORITMA *HYBRID* RSA *(RIVEST, SHAMIR, ADLEMAN)* DAN *VIGENERE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

OLEH
AKHMAD KHUMAIDI
NIM. 15610029

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2020

ALGORITMA *HYBRID* RSA *(RIVEST, SHAMIR, ADLEMAN)* DAN *VIGENERE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

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

Oleh
Akhmad Khumaidi
NIM. 15610029

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2020

ALGORITMA *HYBRID* RSA *(RIVEST, SHAMIR, ADLEMAN)* DAN *VIGENERE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

Oleh
Akhmad Khumaidi
NIM. 15610029

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 30 Maret 2020

Pembimbing I,	Pembimbing II,
Muhammad Khudzaifah, M.Si	Mohammad Nafie Jauhari, M.Si
NIP. 19900511 20160801 1 057	NIP. 19870218 20160801 1 056

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

ALGORITMA *HYBRID* RSA *(RIVEST, SHAMIR, ADLEMAN)* DAN *VIGENERE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

Oleh
Akhmad Khumaidi
NIM. 15610029

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 13 April 2020

Penguji Utama	: Mohammad Jamhuri, M.Si	.....
Ketua Penguji	: Dr. Imam Sujarwo, M.Pd	.....
Sekretaris Penguji	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	: Mohammad Nafie Jauhari, M.Si	.....

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Akhmad Khumaidi

NIM : 15610029

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Algoritma *Hybrid* RSA *(Rivest, Shamir, Adleman)* dan *Vigenere Cipher* untuk Mengamankan Pesan.

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

Malang, 30 Maret 2020
Yang membuat pernyataan,

METERAI TEMPEL
TGL. 20
14690AHF470852042
6000
ENAM RIBU RUPIAH

Akhmad Khumaidi
NIM. 15610029

MOTO

Cukup Bagiku Allah SWT.

حَسْبُنَا اللَّهُ وَنِعْمَ الْوَكِيلُ

"Cukuplah Allah menjadi Penolong kami dan Allah adalah sebaik-baik Pelindung"(QS. Ali Imran: 173).

PERSEMBAHAN

Dengan rasa syukur penulis persembahkan karya ini kepada:

Bapak Ismail, Ibu Heni Masitoh, serta Adik Rokhim dan Azam tercinta yang telah memberikan do'a, dukungan, dan semangat kepada penulis. Para guru yang telah memberikan bekal ilmu pengetahuan yang bermafaat serta sahabat-sahabat yang selalu memberikan semangat yang berarti bagi penulis.

KATA PENGANTAR

Assalamu,alaikum Wr. Wb.

Puji syukur penulis panjatkan ke hadirat Allah Swt. yang telah melimpahkan rahmat dan Hidayah-Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul "Algoritma *Hybrid* RSA *(Rivest, Shamir, Adleman)* dan *Vigenere Cipher* untuk Mengamankan Pesan" ini dengan baik. Shalawat serta salam senantiasa tercurahkan kepada Nabi Muhammad Saw. yang telah membimbing umatnya dari berbagai permasalahan menuju kehidupan yang bahagia di dunia dan akhirat.

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

1. Prof. Dr. Abd. Haris, M.Ag, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Usman Pagalay, M.Si, selaku ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Juhari, M.Si, selaku dosen wali.
5. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah memberikan arahan dan bimbingan kepada penulis dengan baik.

6. Mohammad Nafie Jauhari, M.Si, selaku pembimbing II yang telah memberikan arahan dan bimbingan kepada penulis dengan baik.
7. Seluruh dosen dan staf administrasi Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan ilmu pengetahuan pada penulis.
8. Bapak, ibu, dan Adik-adik tercinta yang telah memberikan do'a, dukungan, dan semangat kepada penulis.
9. Semua teman-teman matematika angkatan 2015 dan teman-teman sekontrakan yang selalu memberikan dukungan dan berjuang bersama-sama dalam menuntut ilmu.
10. Semua pihak yang ikut serta dalam membantu dan menyelesaikan skripsi ini.

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

Wassalamu'alaikum Wr. Wb.

Malang, 30 Maret 2020

Penulis

DAFTAR ISI

DAFTAR GAMBAR

ABSTRAK

Khumaidi, Akhmad. 2020. **Algoritma *Hybrid* RSA *(Rivest, Shamir, Adleman)* dan *Vigenere Cipher* untuk Mengamankan Pesan**. Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Mohammad Nafie Jauhari, M.Si.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, Algoritma *Hybrid*, RSA, *Vigenere Cipher*

Kriptografi adalah ilmu yang mempelajari tentang bagaimana cara menjaga keamanan pesan saat dikirimkan dari suatu tempat ke tempat lain. Enkripsi merupakan proses mengubah pesan biasa (*plaintext*) menjadi pesan kode (*ciphertext*) dan dekripsi merupakan proses pengubahan kembali dari *ciphertext* menjadi *plaintext*. Algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya disebut algoritma simetris sedangkan algoritma yang menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya disebut algoritma asimetris.

Algoritma *hybrid* adalah algoritma yang menggunakan dua sesi kunci untuk enkripsi dan dekripsinya yaitu kunci pada algoritma simetris untuk melindungi pesan dan kunci pada algoritma asimetris untuk melindungi kunci pada algoritma simetris. Penelitian ini membahas tentang algoritma *hybrid* RSA dan *vigenere cipher* untuk mengamankan pesan, *vigenere cipher* adalah algoritma simetris dan RSA adalah algoritma asimetris. Penelitian ini bertujuan untuk meningkatkan keamanan pesan dengan menggunakan algoritma *hybrid*.

Hasil penelitian menunjukkan bahwa algoritma *hybrid* RSA dan *vigenere cipher* dapat diterapkan untuk meningkatkan keamanan pesan, tingkat keamanan pesan pertama terletak pada keragaman huruf kunci pada enkripsi *vigenere cipher* dan tingkat keamanan pesan kedua terletak pada enkripsi dan dekripsi RSA terhadap kunci *vigenere cipher*. Hasil penilitian ini dapat diimplementasikan dengan program aplikasi menggunakan App Inventor.

ABSTRACT

Khumaidi, Akhmad. 2020. **Hybrid RSA (Rivest, Shamir, Adleman) and Vigenere Cipher Algorithm to Secure Messages.** Thesis. Department of Mathematics, Faculty of Science and Technology, State Islamic University of Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Mohammad Nafie Jauhari, M.Si.

Keywords: Cryptography, Encryption, Decryption, Hybrid Algorithms, RSA, Vigenere Cipher

Cryptography is the study of how to maintain the security of messages when sent from one place to another. An encryption is the process of changing ordinary messages (plaintext) to coded messages (ciphertext) and decryption is the process of changing back from ciphertext to plaintext. Algorithms that use the same key for encryption and decryption are called a symmetric algorithm while algorithms that use different keys for encryption and decryption are called an asymmetric algorithm.

Hybrid algorithm is an algorithm that uses two key sessions for encryption and decryption, namely using a key on the symmetric algorithm to protect the message and a key on the asymmetric algorithm to protect the key on the symmetric algorithm. This research discusses hybrid RSA and vigenere cipher algorithm to secure messages, vigenere cipher is a symmetric algorithm and RSA is an asymmetric algorithm. This study aims to increase the level of message security by using a hybrid algorithm.

The results showed that the hybrid RSA and vigenere cipher algorithm can be applied to improve the message security, the first security level lies in the diversity of alphabet key in the vigenere cipher encryption and the second security level lies in the RSA encryption and decryption of the vigenere cipher key. The results of this study can be implemented in the front of an application using App Inventor.

ملخص

حميدي، أحمد. ٢٠٢٠. خوارزمية هجينة *(Rivest, Shamir, Adleman)* RSA و *Vigenere Cipher* لتأمين الرسائل. أطروحة. شعبة الرياضيات، كلية العلوم والتكنولوجيا، الجامعة الإسلامية الحكومية مولانا مالك إبراهيم مالانج. المشرف: (١) محمد حذيفه الماجستير (٢) محمد نافي جوهري الماجستير.

الكلمات الرئيسية: التشفير، التشفير، فك التشفير، خوارزمية هجينة، RSA، *Vigenere Cipher*

التشفير هو دراسة كيفية الحفاظ على أمان الرسائل عند إرسالها من مكان إلى آخر. التشفير هو عملية التغيير من الرسائل العادية (نص عادي) إلى رسائل مشفرة (نص مشفر) وفك التشفير هو عملية التغيير من نص مشفر إلى نص عادي. الخوارزميات التي تستخدم نفس المفتاح للتشفير وفك التشفير تسمى الخوارزميات المتماثلة بينما الخوارزميات التي تستخدم مفاتيح مختلفة للتشفير وفك التشفير تسمى الخوارزميات غير المتماثلة.

الخوارزمية الهجينة هي خوارزمية تستخدم مفتاحي جلسة للتشفير وفك التشفير، وهما مفتاح في خوارزمية متماثلة لحماية الرسائل ومفتاح في خوارزمية غير متماثلة لحماية المفاتيح في خوارزمية متماثلة. في هذا البحث، نناقش خوارزمية الهجينة RSA و *Vigenere Cipher* لتأمين الرسائل، حيث يكون *Vigenere Cipher* خوارزمية متماثلة و RSA خوارزمية غير متماثلة. تهدف هذه الدراسة إلى زيادة مستوى أمن الرسائل باستخدام خوارزمية هجينة.

أظهرت النتائج أنه يمكن تطبيق خوارزمية هجينة RSA و *Vigenere Cipher* لتحسين أمان الرسالة، ومستوى أمان الرسالة الأولى يمكن في تنوع الأحرف الرئيسية في *Vigenere Cipher* ومستوى أمان الرسالة الثاني يمكن في تشفير RSA وفك تشفير مفتاح *Vigenere Cipher*. يمكن تنفيذ نتائج هذه الدراسة باستخدام برنامج تطبيقي باستخدام App Inventor.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Sebuah sistem keamanan teknologi informasi di zaman sekarang ini sangat dibutuhkan terutama pada lembaga tertentu yang mempunyai pesan yang bersifat rahasia. Pesan terbagi menjadi dua jenis, yaitu pesan yang bersifat rahasia dan pesan yang bersifat tidak rahasia. Pesan yang bersifat rahasia adalah pesan yang penting yaitu pesan yang selalu diperhatikan dan dijaga, sedangkan pesan yang bersifat tidak rahasia adalah pesan yang tidak penting ataupun penting namun tidak terlalu diperhatikan dan dijaga bahkan orang dapat mudah menggandakan suatu pesan tersebut. Dari kenyataan tersebut agar pesan yang kita kirim atau simpan tidak diketahui oleh orang lain maka diperlukanlah sebuah kunci atau sandi untuk membukanya. Jadi dalam hal ini hanya orang yang mempunyai kunci atau sandi itulah yang berhak membuka pesan tersebut baik secara dikirim maupun disimpan sendiri.

Kriptografi adalah ilmu yang mempelajari tentang bagaimana cara menjaga keamanan pesan saat dikirimkan dari suatu tempat ke tempat lain. Konsep dasar dari kriptografi adalah mengubah dari teks biasa *(plaintext)* menjadi teks kode *(ciphertext)* kemudian diubah lagi menjadi teks biasa *(plaintext)* agar dapat dibaca oleh penerima pesan. Proses pengubahan dari *plaintext* menjadi *ciphertext* disebut proses enkripsi *(encryption)*, sedangkan proses mengubah kembali dari *ciphertext* menjadi *plaintext* disebut proses dekripsi *(decryption)* (Ariyus, 2006a:77-78).

Menurut (Ariyus, 2008:108) algoritma kriptografi terdiri dari tiga macam menurut kuncinya yaitu: simetris, asimetris, dan *hybrid*. Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya, untuk enkripsi disebut kunci umum *(public key)* dan untuk dekripsi disebut kunci rahasia *(private key)*. Algoritma *hybrid* adalah algoritma yang menggunakan kunci ganda untuk enkripsi dan dekripsinya yaitu memakai kunci pada algoritma simetris dan asimetris, kunci pada algoritma asimetris berfungsi untuk melindungi kunci pada algoritma simetris, sehingga lebih aman dalam mengamankan pesan.

Maka dari itu dalam penelitian ini penulis ingin menganalisa sistem enkripsi dan dekripsi yang berjudul Algoritma *Hybrid* RSA *(Rivest, Shamir, Adleman)* dan *Vigenere Cipher* untuk Mengamankan Pesan, dimana RSA adalah algoritma asimetris dan *Vigenere Cipher* adalah algoritma simetris. Secara umum konsep kriptografi algoritma *hybrid* adalah pesan yang akan dikirim oleh pengirim diubah tampilan pesan menjadi bentuk yang tidak dimengerti dengan menggunakan kunci simetris biasa, kemudian kunci simetris biasa diubah menjadi kunci simetris kode dengan menggunakan kunci umum, sehingga orang yang tidak mempunyai kunci simetris kode dan kunci rahasia tidak mengetahui kunci simetris biasa dan maksud dari pesan yang dikirim. Sedangkan penerima pesan yang dituju dapat melakukan pengubahan kunci simetris kode menjadi kunci simetris biasa dengan menggunakan kunci rahasia, sehingga tampilan pesan yang tidak dimengerti bisa diubah kembali menjadi bentuk yang dapat dimengerti dan mempunyai arti.

Tentang sebuah konsep kriptografi juga terdapat dalam Al-Quran yaitu yang berupa amanat, hal tersebut terdapat di dalam surat An-Nisa' ayat 58 yang artinya yaitu:

"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': 58).

Di dalam tafsir Ibnu katsir disebutkan bahwa Allah SWT. memberitahukan bahwa Dia memerintahkan agar amanat-amanat itu disampaikan kepada yang berhak menerimanya (Ad-Dimasyqi, 2000:251).

Dari penjelasan tafsir surat An-Nisa' ayat 58 di atas dapat diketahui bahwa Allah SWT memerintahkan agar amanat-amanat itu disampaikan kepada yang berhak menerimanya, hal tersebut sebagaimana sebuah pesan dalam konsep kriptografi, bahwa pesan yang dikirimkan dari suatu tempat ke tempat lain haruslah terkirim dan terjaga keamanannya sehingga pesan tersebut dapat terbaca oleh penerima pesan dengan aman.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka penelitian ini mempunyai rumusan masalah sebagai berikut:

1. Bagaimana proses Algoritma *Hybrid* dengan menggunakan RSA dan *Vigenere Cipher*?
2. Bagaimana proses enkripsi dan dekripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada sebuah pesan?

3. Bagaimana proses enkripsi dan dekripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada sebuah pesan dengan menggunakan aplikasi?

1.3 Tujuan Penelitian

Berdasarkan latar belakang di atas maka penelitian ini mempunyai tujuan sebagai berikut:

1. Untuk mengetahui proses Algoritma *Hybrid* dengan menggunakan RSA dan *Vigenere Cipher*.
2. Untuk meningkatkan keamanan pesan dengan menggunakan Algoritma *Hybrid* RSA dan *Vigenere Cipher*.
3. Mengimplementasikan Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada sebuah aplikasi.

1.4 Manfaat Penelitian

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

1. Dapat menambah wawasan tentang kriptografi khususnya pada Algoritma Hybrid dengan menggunakan RSA dan *Vigenere Cipher*.
2. Dapat menambah bahan kepustakaan dan informasi pembelajaran mata kuliah yang berhubungan dengan kriptografi.
3. Dapat memperkaya sumber pengetahuan tentang kriptografi dan solusi bagi pihak-pihak yang menggunakan teknologi informasi dan komunikasi untuk dapat melakukan pengiriman pesan dengan aman.

1.5 Batasan Masalah

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

1. Implementasi enkripsi dan dekripsi berdasarkan angka dan huruf/ abjad.
2. Pengurutan tabel angka terhadap huruf atau abjad dimulai dari 0.
3. Hasil enkripsi kunci berupa angka dan dekripsi berupa abjad atau huruf.
4. Hasil enkripsi dan dekripsi pesan berupa huruf atau abjad.
5. Aplikasi dibuat menggunakan App Inventor.

1.6 Metode Penelitian

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

1. Menjelaskan tentang Algoritma *Hybrid* RSA dan *Vigenere Cipher*.
2. Memberikan contoh serta langkah-langkah enkripsi dan dekripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher*
3. Mengimplementasikan Algoritma *Hybrid* RSA dan *Vigenere Cipher* kedalam sebuah aplikasi dengan menggunakan App Inventor.

1.7 Sistematika Penulisan

Dalam penelitian ini sistematika penulisan 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, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II Kajian Pustaka

Bagian kajian pustaka ini terdapat teori-teori dan konsep-konsep yang dapat mendukung dalam penelitian ini. Teori atau konsep tersebut meliputi teori bilangan, konsep kriptografi, dan lain-lain.

BAB III Pembahasan

Bagian pembahasan ini berisi tentang penjelasan dan penguraian secara keseluruhan langkah-langkah yang telah disebutkan dalam metode penelitian dan menjawab rumusan masalah.

BAB IV Penutup

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

BAB II

KAJIAN PUSTAKA

2.1 Teori Bilangan

Kajian tentang sifat-sifat bilangan asli dapat diartikan sebagai teori bilangan. Dalam penjelasan yang lebih mendalam, teori bilangan mempelajari tentang bilangan dan sifat-sifatnya. Sebagai salah satu cabang matematika, teori bilangan disebut sebagai "aritmetika lanjut (*advanced aritmetics)*" karena berkaitan dengan sifat-sifat bilangan asli (Muhsetyo, 1997:1).

Salah satu teori yang mendasari perhitungan dari kriptografi adalah teori bilangan, bilangan yang digunakan adalah bilangan bulat *(integer)* yang nantinya bisa digunakan pada sistem kriptografi simetris, asimetris, dan *hybrid*.

2.1.1 Bilangan Bulat

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal. Himpunan semua bilangan bulat dinyatakan dengan $\mathbb{Z}$ *(Zahlen)* yang diambil dari bahasa jerman atau dinotasikan dengan *I (Integer)* yang diambil dari bahasa inggris, himpunan bilangan bulat yaitu $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Himpunan bilangan bulat dibagi menjadi tiga, yaitu bilangan bulat positif yaitu bilangan bulat yang lebih besar dari nol yang dinotasikan dengan $\mathbb{Z}^+$, nol, dan bilangan bulat negatif yaitu bilangan bulat yang kurang dari nol yang dinotasikan dengan $\mathbb{Z}^-$ (Abdussakir, 2009:102).

2.1.2 Keterbagian

Kajian sifat-sifat yang berkaitan dengan keterbagian *(divisibility)* merupakan dasar pengembangan dari teori bilangan. Jika suatu bilangan bulat dibagi oleh suatu bilangan bulat yang lain, maka hasilnya adalah bilangan bulat atau bukan bilangan bulat (Muhsetyo, 1997:43).

Definisi 2.1

Misalkan $a, b \in \mathbb{Z}$ dengan $a \neq 0$. a dikatakan membagi b, ditulis $a|b$, jika dan hanya jika $b = ax$, untuk suatu $x \in \mathbb{Z}$ (Abdussakir, 2009:114).

Contoh:

1. $5|15$, sebab ada $3 \in \mathbb{Z}$, sehingga $15 = 5 \cdot 3$
2. $8|40$, sebab ada $5 \in \mathbb{Z}$, sehingga $40 = 8 \cdot 5$

Teorema 2.1

Diberikan $a, b, c \in \mathbb{Z}$.

1. Jika $a|b$ maka $a|bx$ untuk setiap bilangan bulat x
2. Jika $a|b$ dan $b|c$, maka $a|c$
3. Jika $a|b$ dan $a|c$, maka $a|(bx + cy)$ untuk setiap $x, y \in \mathbb{Z}$
4. Jika $a|b$ dan $b|a$, maka $a = \pm b$
5. Jika $a|b$, $a > 0$, dan $b > 0$, maka $a \leq b$
6. Untuk setiap bilangan bulat $m \neq 0, a|b$ jika dan hanya jika $ma|mb$

(Abdussakir, 2009:115).

Bukti:

1. Jika $a|b$, maka ada $y \in \mathbb{Z}$, sehingga $b = ay$. Akibatnya, untuk setiap $x \in \mathbb{Z}$ diperoleh $bx = (ay)x = a(yx)$. Karena pada bilangan bulat berlaku sifat

tertutup pada perkalian maka terdapat $p = yx$. Sehingga berlaku $bx = ap$. Jadi, $a|bx$.

2. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Dan $b|c$, maka $c = by$ untuk $y \in \mathbb{Z}$. Diperoleh $c = by = (ax)y = a(xy)$, untuk suatu $xy \in \mathbb{Z}$. Jadi, $a|c$.
3. Jika $a|b$, maka $b = ap$ untuk $p \in \mathbb{Z}$. Dan $a|c$, maka $c = aq$ untuk $q \in \mathbb{Z}$. Akibatnya $bx = (ap)x$ untuk setiap $x \in \mathbb{Z}$ dan $cy = (aq)y$ untuk setiap $q \in \mathbb{Z}$. Diperoleh $bx + cy = (ap)x + (aq)y = a(px + qy)$ untuk suatu $px + qy \in \mathbb{Z}$. Jadi, $a|(bx + cy)$.
4. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Dan $b|a$, maka $a = by$ untuk $y \in \mathbb{Z}$. Diperoleh $b = ax = (by)x = b(yx)$ maka $b - b(yx) = b(1 - yx) = 0$ karena $b \neq 0$, maka $1 - yx = 0$ atau $xy = 1$. Diperoleh $x = y = 1$ atau $x = y = -1$ sehingga didapatkan $a = \pm b$.
5. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Jika $a > 0, b > 0$ dan $b = ax$ maka $x > 0$ untuk $x = 1$ maka dipenuhi $a = b$. Sedangkan untuk $x > 1$ maka $b > a$. Jadi $a \leq b$.
6. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Akibatnya untuk $m \in \mathbb{Z}$ dan $m \neq 0$ maka berlaku $mb = m(ax) = (ma)x$. Jadi $ma|mb$.

   Jika $ma|mb$ dan $m \neq 0$, maka $mb = (ma)x$ untuk suatu $x \in \mathbb{Z}$. $mb = (ma)x = m(ax)$ atau $mb - m(ax) = m(b - ax) = 0$. Karena $m \neq 0$, maka $b - ax = 0$ atau $b = ax$ untuk suatu $x \in \mathbb{Z}$. Jadi $a|b$.

Definisi 2.2

Ditentukan $x, y \in \mathbb{Z}$, x dan y keduanya tidak bersama-sama bernilai 0. $a \in \mathbb{Z}$ disebut pembagi (faktor) persekutuan *(common divisor, common factor)*

dari x dan y jika $a|x$ (a membagi x) dan $a|y$ (a membagi y). $a \in \mathbb{Z}$ disebut pembagi (faktor) persekutuan terbesar *(gcd = greatest common divisor, gcf = greatest common factor)* dari x dan y jika a adalah bilangan bulat positif terbesar yang membagi x (yaitu $a|x$) dan membagi y (yaitu $a|y$).

Notasi:

$d = (x, y)$ dibaca d adalah faktor (pembagi) persekutuan terbesar dari x dan $yd = (x_1, x_2, \ldots, x_n)$ dibaca d adalah (pembagi) persekutuan terbesar dari $x_1, x_2, \ldots, x_n$.

Perlu diperhatikan bahwa $d = (a, b)$ didefinisikan untuk setiap pasang bilangan bulat $a, b \in \mathbb{Z}$, kecuali $a = 0$ dan $b = 0$. Demikian pula, perlu dipahami bahwa (a, b) selalu bernilai bilangan bulat positif, yaitu $d \in \mathbb{Z}$ dan $d > 0$ (atau $d \geq 1$) (Muhsetyo, 1997:60-61).

Contoh:

1. Himpunan semua faktor 16 adalah:

   $A = \{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$

   Himpunan semua faktor 12 adalah:

   $B = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$

   Himpunan semua faktor persekutuan 16 dan 12 adalah:

   $C = \{-4, -2, -1, 1, 2, 4\}$

   Karena unsur C yang terbesar adalah 4, maka $(16, 12) = 4$.

Definisi 2.3

Bilangan a dan b dikatakan prima relatif jika $(a, b) = 1$ (Abdussakir, 2009:124).

Contoh:

1. $(12, 5) = 1$. Jadi, 12 dan 5 merupakan prima relatif.
2. $(16, 12) = 4$. Jadi, 16 dan 12 bukan merupakan prima relatif.

Teorema 2.2

Jika $c|ab$ dan $(a, c) = 1$, maka $c|b$ (Abdussakir, 2009:124)

Bukti:

Karena $(a, c) = 1$, maka terdapat $m, n \in Z$ sehingga $ma + nc = 1$.

Dan berlaku pula bahwa $mab + ncb = b$.

Diketahui $c|ab$, maka $c|mab$. Karena $c|c$ maka $c|cnb$.

Dengan demikian $c|(mab + ncb) = c|b(ma + nc)$. Jadi, $c|b$.

2.1.3 Bilangan Prima dan Komposit

Sifat pembagian pada bilangan bulat melahirkan konsep-konsep bilangan prima, salah satu konsep bilangan bulat yang digunakan dalam penghitungan komputer adalah bilangan prima. Dengan ditemukannya bilangan prima, teori bilangan berkembang semakin pesat dan lebih mendalam. Banyak teorema dan sifat-sifat yang dikembangkan berdasarkan bilangan prima. Bilangan prima juga memainkan peranan yang sangat penting pada algoritma RSA yaitu pada kunci umum dan kunci rahasia.

Bilangan bulat positif yang mempunyai aplikasi penting dalam ilmu komputer dan matematika diskrit adalah bilangan prima. Sedangkan bilangan prima itu sendiri adalah bilangan bulat positif yang lebih dari 1 yang hanya habis dibagi oleh 1 dan dirinya sendiri (Munir, 2012:200).

Definisi 2.4

Jika p suatu bilangan bulat positif lebih dari 1 yang hanya mempunyai pembagi positif 1 dan p, maka p disebut bilangan prima. Jika suatu bilangan bulat $q > 1$ bukan suatu bilangan prima, maka q disebut bilangan komposit (Muhsetyo, 1997:92).

Definisi bilangan prima adalah bilangan asli yang tepat mempunyai dua pembagi. Sedangkan bilangan yang mempunyai lebih dari dua pembagi disebut bilangan komposit (Irawan,dkk, 2014:51). .

Contoh:

1. $2, 3, 5$ adalah bilangan prima, karena pembaginya adalah 1 dan bilangan itu sendiri. Sedangkan $4, 6, 8$ adalah bilangan komposit, seperti 4 memiliki pembagi $1, 2$ dan 4 ; 6 memiliki pembagi $1, 2, 3$ dan 6; dan seterusnya.
2. $-2, -3$ bukan bilangan prima, demikian pula $-4, -6$ bukan bilangan komposit, karena bilangan prima dan komposit itu lebih besar dari 1 atau bilangan bulat positif lebih dari 1.

Teorema 2.3

Jika p adalah suatu bilangan prima dan $p|ab$, maka $p|a$ atau $p|b$ (Muhsetyo, 1997:100).

Bukti:

Anggaplah $p \nmid a$, karena p adalah suatu bilangan prima dan $p \nmid a$, maka p hanya mempunyai pembagi 1 dan p, sehingga $(a, p) = 1$.

Menurut teorema 2.2, jika $p|ab$ dan $(a, p) = 1$, maka $p|b$.

Dengan cara serupa, dan dianggap $p|b$, maka dapat dibuktikan bahwa $p|a$.

2.1.4 Kongruensi

Berbicara tentang kongruensi berarti tidak lepas dengan masalah keterbagian. Karena membahas konsep masalah keterbagian dan sifat-sifatnya merupakan pengkajian secara lebih mendalam menggunakan konsep kongruensi. Sehingga kongruensi merupakan cara lain untuk mengkaji keterbagian dalam himpunan bilangan bulat (Irawan, dkk, 2014:63).

Definisi 2.5

Diketahui $a, b, m \in \mathbb{Z}$. a disebut kongruen dengan b modulo m, ditulis $a \equiv b \ (mod\ m)$, jika $(a - b)$ habis dibagi m, yaitu $m|(a - b)$. Sedangkan jika $(a - b)$ tidak habis dibagi m, yaitu $m \nmid (a - b)$, maka ditulis $a \not\equiv b \ (mod\ m)$, dibaca a tidak kongruen dengan b modulo m. Karena $(a - b)$ habis dibagi oleh m jika dan hanya jika $(a - b)$ habis dibagi oleh $-m$, maka: $a \equiv b \ (mod\ m)$ jika dan hanya jika $b \equiv a \ (mod\ m)$ (Muhsetyo, 1997:138).

Misalkan a dan b adalah bilangan bulat dan m adalah bilangan bulat > 0, maka $a \equiv b \ (mod\ m)$ jika m habis membagi $a - b$ (Munir, 2012:192).

Contoh:

$17 \equiv 2 \ (mod\ 3)$ (3 habis membagi $17 - 2 = 15 \rightarrow 15 \div 3 = 5$)

$-7 \equiv 15 \ (mod\ 11)$ (11 habis membagi $-7 - 15 = -22 \rightarrow -22 \div 11 = 2$)

$17 \not\equiv 2 \ (mod\ 11)$ (7 tidak habis membagi $17 - 2 = 15$)

$-7 \not\equiv 15 \ (mod\ 3)$ (3 tidak habis membagi $-7 - 15 = -22$)

Kekongruenan $a \equiv b \ (mod\ m)$ dapat pula dituliskan dalam hubungan $a = b + km$, yang dalam hal ini adalah sembarang k adalah bilangan bulat. Pembuktiannya adalah sebagai berikut:

Menurut definisi 2.5, $a \equiv b(mod\ m)$ jika $m|(a-b)$, maka menurut definisi 2.1 pada keterbagian terdapat bilangan bulat k sedemikian sehingga $a-b=km$ atau $a=b+km$.

Teorema 2.4

Andaikan a, b dan c adalah bilangan bulat dan m bilangan asli, maka berlaku:

1. Refleksif $a \equiv a\ (mod\ m)$
2. Simetris, jika $a \equiv b\ (mod\ m)$, maka:

   $b \equiv a\ (mod\ m)$ dan $a-b \equiv 0\ (mod\ m)$ adalah pernyataan yang ekuivalen
3. Transitif, jika $a \equiv b\ (mod\ m)$ dan $b \equiv c\ (mod\ m)$ maka $a \equiv c\ (mod\ m)$

(Irawan, dkk, 2014:64-65).

Bukti:

1. $a \equiv a\ (mod\ m)$ berarti $m|a-a$ (menurut definisi 2.5)

   Jika $m \neq 0$ maka $m|0$ sebab $a-a=0$.
2. $a \equiv b\ (mod\ m)$ berarti $m|a-b$ (menurut definisi 2.5)

   menurut definisi 2.1 pada keterbagian ada bilangan bulat t sehingga:

   $m|a-b$ dapat dinyatakan $a-b=tm$

   $\Leftrightarrow -(a-b)=-tm$

   $\Leftrightarrow b-a=(-t)m$

   Menurut definisi 2.5, ini berarti $b \equiv a\ (mod\ m)$.

   $a \equiv b\ (mod\ m)$ berarti $m|a-b$ (menurut definisi 2.5)

menurut definisi 2.1 pada keterbagian ada bilangan bulat t sehingga $m|a-b$ dapat dinyatakan $a-b=tm$, untuk setiap $(a-b)-0=tm$, maka $a-b\equiv 0\ (mod\ m)$.

3. $a\equiv b\ (mod\ m)$ berarti $m|a-b$ (menurut definisi 2.5)

   $b\equiv c\ (mod\ m)$ berarti $m|b-c$ (menurut definisi 2.5)

   menurut definisi 2.1 pada keterbagian ada bilangan bulat t_1 dan t_2 sehingga:

   $m|a-b$ dapat dinyatakan $a-b=t_1m$

   $m|b-c$ dapat dinyatakan $b-c=t_2m$

   Kedua persamaan dijumlahkan sehingga diperoleh:

$$a-c=(t_1+t_2)m$$

   Ini berarti, menurut definisi 2.5 menjadi $a\equiv c\ (mod\ m)$.

Teorema 2.5

Jika $a\equiv b\ (mod\ m)$, maka $(a+c)\equiv(b+c)\ (mod\ m)$ (Irawan, dkk, 2014:65).

Bukti:

$a\equiv b\ (mod\ m)$ berarti $m|a-b$ (menurut definisi 2.5)

menurut definisi 2.1 pada keterbagian ada bilangan bulat t sehingga:

$m|a-b$ dapat dinyatakan $a-b=tm$

$$\Leftrightarrow (a-b)+0=tm$$

$$\Leftrightarrow (a-b)+(c-c)=tm$$

$$\Leftrightarrow (a+c)-(b+c)=tm$$

Sesuai definisi 2.5 maka diperoleh $(a+c)\equiv(b+c)\ (mod\ m)$.

Teorema 2.6

Jika $a \equiv b \ (mod\ m)$, maka $(ac) \equiv (bc) \ (mod\ m)$ (Irawan, dkk, 2014:65).

Bukti:

$a \equiv b \ (mod\ m)$ berarti $m|a - b$ (menurut definisi 2.5)

menurut definisi 2.1 pada keterbagian ada bilangan bulat t sehingga:

$m|a - b$ dapat dinyatakan $a - b = tm$

$\Leftrightarrow (a - b)c = (tm)c$

$\Leftrightarrow ac - bc = (tc)m$

Sesuai definisi 2.5 maka diperoleh $(ac) \equiv (bc) \ (mod\ m)$.

Teorema 2.7

Andaikan $a, b, c, d,$ dan m bilangan asli. Jika $a \equiv b \ (mod\ m)$ dan $c \equiv d \ (mod\ m)$, maka $ac \equiv bd \ (mod\ m)$ (Irawan, dkk, 2014:67).

Bukti:

$a \equiv b \ (mod\ m)$ berarti $m|a - b$ (menurut definisi 2.5)

$c \equiv d \ (mod\ m)$ berarti $m|c - d$ (menurut definisi 2.5)

menurut definisi 2.1 pada keterbagian ada bilangan bulat t_1 dan t_2 sehingga:

$m|a - b$ dapat dinyatakan $a - b = t_1 m$

$(a - b)c = (t_1 m)c$

$ac - bc = (t_1 m)c \ldots\ldots\ldots\ldots (1)$

$m|c - d$ dapat dinyatakan $c - d = t_2 m$

$(c - d)b = (t_2 m)b$

$cb - db = (t_2 m)b \ldots\ldots\ldots\ldots (2)$

Dari (1) dan (2) dijumlahkan sehingga diperoleh:

$ac - bc = (t_1 m)c$

$cb - db = (t_2 m)b \quad +$

$ac - bd = (t_1 c + t_2 b)m$

Ini berarti sesuai definisi 2.5 $(ac) \equiv (bd)\ (mod\ m)$.

Teorema 2.8

Jika $a \equiv b\ (mod\ m)$, maka $a^n \equiv b^n\ (mod\ m)$ untuk n bilangan bulat positif (Irawan, dkk, 2014:68).

Bukti:

$a \equiv b\ (mod\ m)$ berarti $m|a - b$ (menurut definisi 2.5)

menurut definisi 2.1 pada keterbagian ada bilangan bulat t sehingga:

$m|a - b$ dapat dinyatakan $a - b = tm$

Kita kenal bahwa bentuk:

$$a^n - b^n = (a - n)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

Persamaan diatas menunjukkan bahwa

$$a - b|(a - n)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

Ini berarti $a - b|(a^n - b^n)$ jadi $a^n \equiv b^n\ (mod\ m)$.

2.1.5 Sistem Residu

Definisi 2.6

Suatu himpunan bilangan bulat $\{r_1, r_2, \dots, r_3\}$ disebut dengan sistem residu tereduksi modulo m jika:

a) $(r_i, m) = 1\ \ (i = 1, 2, \dots, k)$.

b) $r_i \not\equiv r_j \ (mod\ m)$ untuk semua $i \neq j$.

c) Jika $(x,m) = 1$, maka $x \equiv r\ mod\ (m)$

(Muhsetyo, 1997:279).

Contoh:

Himpunan $\{1, 5\}$ adalah sistem residu tereduksi modulo 6 karena:

a. $r_1 = 1, (r_1, 6) = (1, 6) = 1$ dan $r_2 = 5, (r_2, 6) = (5, 6) = 1$

b. $1 \not\equiv 5\ (mod\ 6)$

c. $(7, 6) = 1 \rightarrow 7 \equiv 1\ (mod\ 6)$

$(11, 6) = 1 \rightarrow 11 \equiv 5\ (mod\ 6)$.

Definisi 2.7

Jika m adalah suatu bilangan bulat positif, maka banyaknya residu di dalam sistem residu tereduksi modulo m adalah $\phi(m)$. $\phi(m)$ disebut fungsi ϕ-Euler dari m. Dari definisi 2.6 dapat diketahui bahwa $\phi(m)$ adalah sama dengan banyaknya bilangan bulat positif kurang dari m yang relatif prima dengan m (Muhsetyo, 1997:279).

Contoh:

1. Himpunan $\{1, 2\}$ adalah sistem residu tereduksi modulo 3 sehingga $\phi(3) = 2$
2. Himpunan $\{1, 2, 3, 4\}$ adalah sistem residu tereduksi modulo 5 sehingga $\phi(5) = 4$
3. Himpunan $\{1, 2, 4, 7, 8, 11, 13, 14\}$ adalah sistem residu tereduksi modulo 15 sehingga $\phi(15) = 8$

Teorema 2.9

Diberikan $(a, m) = 1$, jika $r_1, r_2, \dots, r_n$ sebagai sistem residu lengkap modulo m, maka $ar_1, ar_2, \dots, ar_n$ juga merupakan sistem residu lengkap modulo m (Irawan,dkk, 2014:72).

Bukti:

Jika $(a, m) = 1$ maka berdasarkan teorema 2.2 pada keterbagian didapat $(ar_i, m) = 1$. Banyak bilangan $ar_1, ar_2, \dots, ar_n$ sama dengan $r_1, r_2, \dots, r_n$. Oleh karena itu hanya yang perlu ditunjukkan bahwa $ar_i \not\equiv ar_j \ (mod\ m)$ bila $i \neq j$. Menurut definisi 2.6 bagian (b) menyatakan secara langsung bahwa $r_i \not\equiv r_j \ (mod\ m)$ sehingga $ar_i \not\equiv ar_j \ (mod\ m)$ untuk setiap $i \neq j$.

Teorema 2.10 (Teorema Euler)

Jika $(a, p) = 1$ maka $a^{\phi(p)} \equiv 1 \ (mod\ p)$ (Irawan,dkk, 2014:73).

Bukti:

Andaikan $r_1, r_2, \dots, r_{\phi(p)}$ adalah suatu sistem residu reduksi modulo p. Menurut teorema 2.9 $ar_1, ar_2, \dots, ar_{\phi(p)}$ juga merupakan sistem residu reduksi modulo p. Oleh sebab itu, untuk setiap r_i ada ar_j sedemikian hingga $r_i \equiv ar_j \ (mod\ p)$. Akibatnya bilangan-bilangan $ar_1, ar_2, \dots, ar_{\phi(p)}$ tidak lain dari pada residu-residu modulo p dari $r_1, r_2, \dots, r_{\phi(p)}$ walaupun urutannya mungkin saja tidak sama. Sehingga didapat $ar_1, ar_2, \dots, ar_{\phi(p)} = r_1, r_2, \dots, r_{\phi(p)} \ (mod\ p)$.

Dan akibatnya: $a^{\phi(p)}(r_1, r_2, \dots, r_{\phi(p)}) \equiv r_1, r_2, \dots, r_{\phi(p)} \ (mod\ p)$.

Karena $(r_i, p) = 1$ maka $a^{\phi(p)}(r_1, r_2, \dots, r_{\phi(p)}) \equiv 1 \ (mod\ p)$.

Contoh:

1. $a = 3;\ p = 10;\ \phi(10) = 4; 3^4 = 81 \equiv 1\ (mod\ 10)$
2. $a = 2;\ p = 11;\ \phi(11) = 10; 2^{10} = 1024 \equiv 1\ (mod\ 11)$

Teorema 2.11 (Teorema Kecil Fermat)

Jika p adalah suatu bilangan prima dan $p \nmid a$ maka $a^{p-1} \equiv 1(mod\ p)$ (Muhsetyo, 1997:152).

Bukti:

Karena p adalah suatu bilangan prima dengan $p \nmid a$, maka $(p, a) = 1$, (jika $(p, a) \neq 1$) yaitu p dan a tidak relatif prima, maka p dan a mempunyai faktor selain 1 dan p (bertentangan dengan sifat p sebagai bilangan prima), selanjutnya karena $(p, a) = 1$ maka untuk $a^{\phi(p)} \equiv 1\ (mod\ p)$.

p adalah bilangan prima, berarti dari bilangan-bilangan bulat:

$\{0, 1, 2, 3, \dots, p - 1\}$

yang tidak relatif prima dengan p hanyalah 0, sehingga:

$\{1, 2, 3, \dots, p - 1\}$

merupakan sistem residu tereduksi modulo p, dengan demikian $\phi(p) = p - 1$, karena $\phi(p) = p - 1$ dan $a^{\phi(p)} \equiv 1\ (mod\ p)$, maka $a^{p-1} \equiv 1(mod\ p)$.

Contoh:

1. $a = 11;\ p = 2;\ \phi(2) = 1; 11^1 = 11 \equiv 1\ (mod\ 2)$
2. $a = 10;\ p = 3;\ \phi(3) = 2; 10^3 = 1000 \equiv 1\ (mod\ 3)$

2.2 Kriptografi

2.2.1 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, Kriptografi adalah ilmu yang mempelajari tentang bagaimana cara menjaga keamanan pesan saat dikirimkan dari suatu tempat ke tempat lain (Ariyus, 2006a:77).

Kriptografi juga dapat disebut dengan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Sebuah pesan rahasia harus terjaga keamanannya, salah satu cara yaitu penyandian pesan dengan kunci, yang bertujuan untuk menyembunyikan pesan dari orang-orang yang tidak ditujukan pesan tersebut kepadanya (Munir, 2006:3).

2.2.2 Sejarah Kriptografi

Kriptografi memiliki sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu dan diperkenalkan oleh orang-orang Mesir untuk mengirim pesan ke pasukan militer yang berada di lapangan. Dengan demikian pesan tersebut tidak bisa terbaca oleh pihak musuh walaupun kurir pembawa pesan tersebut tertangkap oleh musuh (Ariyus, 2006a:77).

Saat ini dengan lahirnya teknologi komputer yang terus berkembang maka metode kriptografi pun juga terus berkembang dan semakin beragam. Keberagaman ini terlihat dari algoritma-lagoritma yang digunakan dalam menuangkan konsep kriptografi. Konsep dasar dari kriptografi adalah mengubah

dari teks biasa *(plaintext)* menjadi teks kode *(ciphertext)* kemudian diubah lagi menjadi teks biasa *(plaintext)* agar dapat dibaca oleh penerima pesan. Proses pengubahan dari *plaintext* menjadi *ciphertext* disebut proses enkripsi *(encryption)*, sedangkan proses menngubah kembali dari *ciphertext* menjadi *plaintext* disebut proses dekripsi *(decryption)* (Ariyus, 2006a:78).

Bahkan di dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital *(fingerprint)* (Ariyus, 2006a:77).

2.2.3 Komponen-komponen Kriptografi

Menurut (Ariyus, 2008:10) terdapat beberapa komponen dalam kriptografi yaitu:

1. Enkripsi

   Enkripsi adalah pesan asli *(plaintext)* yang diubah dengan algoritma tertentu sehingga menjadi kode-kode yang tidak dimengerti *(ciphertext)*. Enkripsi merupakan hal yang sangat penting dalam kriptografi.

2. Dekripsi

   Dekripsi merupakan kebalikan dari enkripsi yaitu pesan yang telah dienkripsi dikembalikan ke bentuk asalnya. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.

3. Kunci

   Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).

4. *Ciphertext*

   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 arti (makna).

5. *Plaintext*

   Plaintext sering disebut dengan teks biasa atau pesan asli ini merupakan sebuah pesan yang diketik dengan memiliki makna.

6. Pesan.

   Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dan sebagainya) atau yang disimpan di dalam media perekam (kertas, storage, dan sebagainya).

7. *Cryptanalysis*

   Cryptanalysis bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan pesan asli tanpa harus mengetahui kunci yang sah secara wajar.

2.2.4 Kriptogrfi Klasik dan Modern

1. Kriptografi Klasik

   Kriptografi Klasik merupakan algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini merupakan teknik klasik dan sudah digunakan beberapa abad yang lalu, dua teknik dasar yang biasa digunakan yaitu:

   a. Teknik Substitusi: Penggantian setiap karakter teks biasa *(plaintext)* dengan karakter lain.

   b. Teknik Transposisi: Teknik yang menggunakan permutasi karakter (Ariyus, 2006b:16).

2. Kriptografi Modern

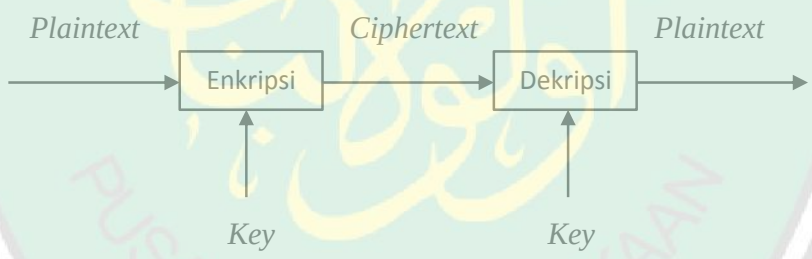
Kriptografi modern merupakan suatu algoritma yang digunakan pada zaman sekarang ini, yang mana kriptografi modern mempunyai kerumitan yang sangat komplek, karena dalam menjalankannya memerlukan bantuan komputer (Ariyus, 2006b:16).

2.2.5 Macam-macam Algoritma Kriptografi

Menurut (Ariyus, 2008:108) terdapat tiga macam algoritma pada kriptografi modern yaitu:

1. Algoritma Simetris

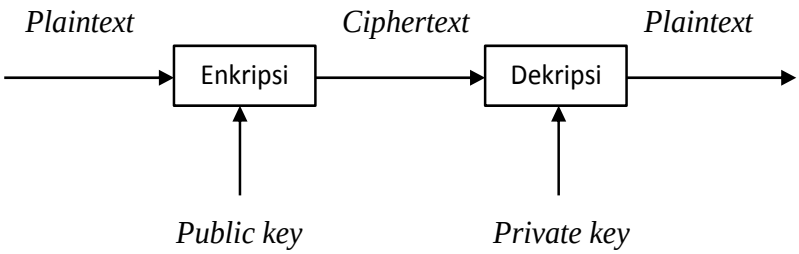
Algoritma Simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Lebih jelasnya perhatikan pada gambar 2.1 berikut:



Gambar 2.1 Algoritma Simetris

2. Algoritma Asimetris

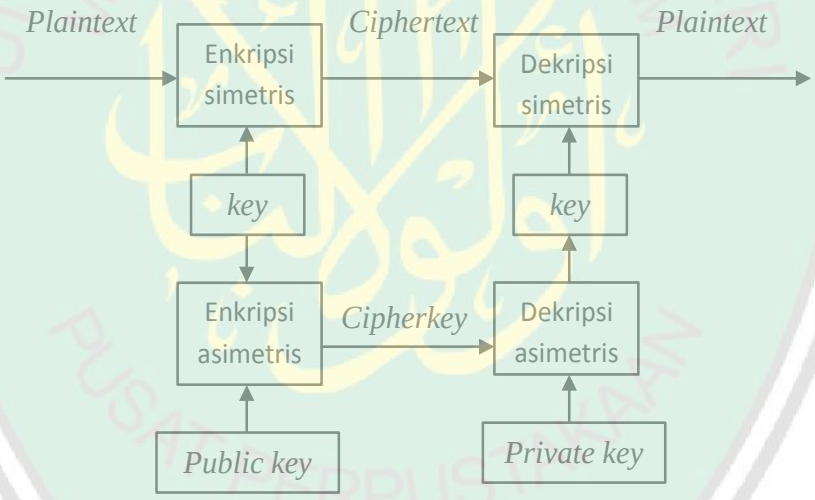
Algoritma Asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya, untuk enkripsi disebut kunci umum *(public key)* dan untuk dekripsi disebut kunci rahasia *(private key)*. Contoh algoritma asimetris yang terkenal yaitu algoritma RSA (merupakan singkatan dari nama penemunya, yakni Revest, Shamir dan Adleman).



Gambar 2.2 Algoritma Asimetris

3. Algoritma *Hybrid*

Algoritma *hybrid* adalah algoritma yang menggunakan kunci ganda untuk enkripsi dan dekripsinya yaitu memakai kunci rahasia (simetris) disebut juga kunci sesi dan kunci asimetris untuk pemberian tanda tangan digital serta melindungi kunci simetris. Seperti gambar berikut ini:



Gambar 2.3 Algoritma *Hybrid*

2.2.6 *Vigenere Cipher*

Vigenere cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifradel. Sig. Giovan Battista Bellaso pada tahun 1553.

Nama vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode *autokey cipher* meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso (Wicaksono, 2017:3).

Algoritma *vigenere cipher* dirancang untuk menghilangkan pola frekuensi huruf pada cipherteks. Dengan begitu, cipherteks yang dihasilkan dengan algoritma *vigenere cipher* ini tidak akan bisa dikenakan metode analisis frekuensi. Algoritma ini bekerja dengan cara yang hampir mirip dengan algoritma *caesar cipher*. Namun pada algoritma *vigenere cipher* ini, pergeseran yang dilakukan tidak selalu sama seperti pada *caesar cipher* (Wicaksono, 2017:3).

Vigenere cipher menggunakan tabel *vigenere standart* dalam mengenkripsi pesan. Tabel yang digunakan merupakan tabel 26 huruf *alfabetik standart*, yang dimulai dari A sampai Z. Kunci pada *vigenere cipher* dipakai berulang kali sebanyak pesan yang akan dienkripsi. Semakin beragam huruf *alfabetik* yang dipakai sebagai kunci, maka semakin kuat keamanan algoritma *vigenere cipher*. Berikut ini rumus enkripsi dan dekripsi *vigenere cipher* :

Enkripsi: $C_i = (P_i + K_i)\ (mod\ 26)$

Dekripsi: $P_i = (C_i - K_i)\ (mod\ 26)$ (Harahap, 2016:61).

2.2.7 Kriptografi RSA

Kriptografi RSA ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci asimetris, RSA mempunyai dua

kunci, yaitu kunci umum dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci yang digunakan untuk enkripsi disebut kunci umum *(public key)*, sedangkan kunci yang digunakan untuk dekripsi disebut kunci rahasia *(private key)*. Untuk menemukan kunci rahasia, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang biasa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Sehingga semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA (Ginting, 2015:254).

Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar. Oleh karena itu, RSA dianggap aman. Untuk membangkitkan kedua kunci, dipilih dua bilangan prima acak yang besar.

Rumus enkripsi

$$C = M^e \ mod\ n$$

Rumus dekripsi

$$M = C^d \ mod\ n = (M^e)^d \ mod\ n = M^{ed} \ mod\ n$$

Pembangkitan kunci pada algoritma RSA:

Memilih p, q dimana p dan q adalah bilangan prima

Dihitung $n = p \times q$

Dihitung $\Phi(n) = (p-1)(q-1)$

Memilih bilangan integer e dimana $\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$

Dihitung d dimana $d \equiv e^{-1} \; mod \; \Phi(n)$, dan $d < \Phi(n)$

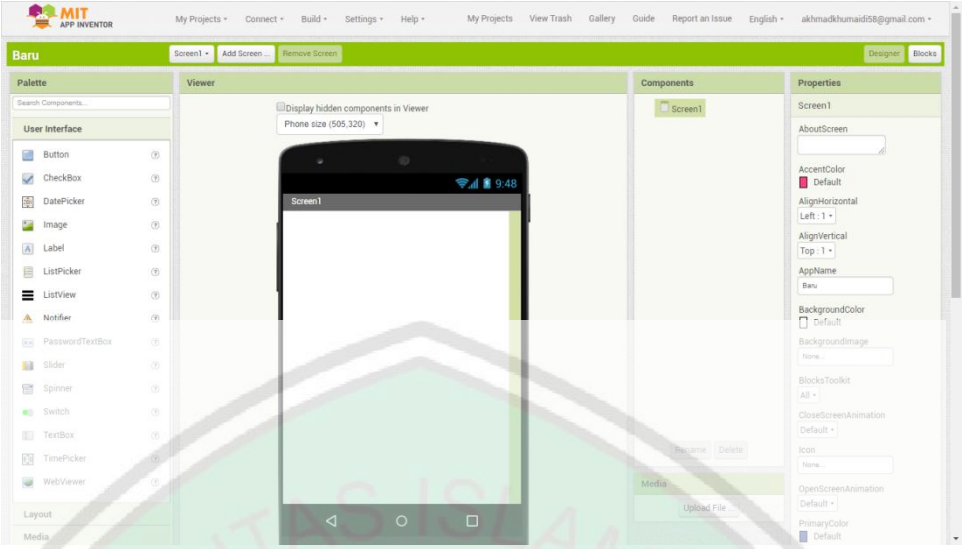
Kunci public dimana $KU = (e, n)$

Kunci private dimana $KR = (d, n)$ (Ariyus, 2006a:137).

2.3 App Inventor

App Inventor 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 sederhana. Jika kita sudah berpengalaman menggunakan App Inventor kita juga bisa membuat program yang sangat rumit dan berguna hanya dengan menggunakan App Inventor (Prasetiyo, 2014:1)

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



Gambar 2.4 App Inventor

Design View terdiri dari lima komponen dasar:

1. *Palette*

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

2. *Viewer*

   Viewer terdiri dari tampilan *handphone* dan komponen-komponen yang bisa di klik. Disitu pengguna bisa melihat komponen yang tidak bisa dilihat dengan *handphone*.

3. *Component*

   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.

4. Media

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

5. *Properties*

Setiap komponen yang anda tambahkan ke dalam projek, pengguna dapat mengatur komponen itu bagaimana dia berinteraksi dengan pengguna maupun dengan komponen lain, atau bagaimana tampilannya. Serta setiap komponen memiliki kolom *properties* yang berbeda-beda (Prasetiyo, 2014:7-12).

2.4 Integrasi Agama dengan Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari tentang bagaimana cara menjaga keamanan pesan saat dikirimkan dari suatu tempat ke tempat lain (Ariyus, 2006a:77).

Tentang sebuah keamanan atau kerahasiaan juga terdapat dalam Al-Quran yaitu yang berupa amanat, hal tersebut terdapat di dalam surat Al-Anfal ayat 27 yang artinya yaitu:

"Hai orang-orang yang beriman, janganlah kalian mengkhianati Allah dan Rasul-(Nya) dan (juga) janganlah kalian mengkhianati amanat-amanat yang dipercayakan kepada kalian, sedangkan kalian mengetahui" (QS. Al-Anfal: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. (Ad-Dimasyqi, 2001:407).

Di dalam hadis Al-Hasan, dari Samurah, juga disebutkan bahwa Rasulullah Saw. telah bersabda yang artinya:

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

Hadis riwayat Imam Ahmad dan semua pemilik kitab sunan. Makna hadis ini umum mencakup semua jenis amanat yang diharuskan bagi manusia menyampaikannya (Ad-Dimasyqi, 2000:251-252).

Dari penjelasan tafsir surat Al-Anfal ayat 27 di atas dapat diketahui bahwa Allah SWT melarang kita untuk berbuat khianat, hal tersebut sebagaimana tentang sebuah keamanan dan kerahasiaan bahwa pesan yang akan dikirim dari suatu tempat ke tempat lain haruslah terkirim dan terjaga keamanan dan kerahasiaanya sehingga pesan tersebut dapat terbaca oleh penerima pesan, apabila tidak terjaga

keamanan dan kerahasiaanya maka orang yang telah membocorkan pesan tersebut yang mengkhianati sebuah pesan yang telah dikirim.

Tentang sebuah pesan yang dikirim adalah sebuah pesan bebas yang memiliki makna (arti) baik itu berupa data, informasi dan lain sebagainya. Hal tersebut sesuai dengan hadis diatas yang menyatakan bahwa amanat yang dimaksud adalah mencakup semua jenis amanat yang diharuskan bagi manusia menyampaikannya.

BAB III

PEMBAHASAN

3.1 Algoritma *Hybrid* RSA dan *Vigenere Cipher*

Algoritma *hybrid* adalah algoritma yang menggabungkan dua buah algoritma yaitu algoritma simetris dan algoritma asimetris, dimana algoritma simestris berfungsi untuk melindungi suatu pesan sedangkan algoritma asimetris berfungsi untuk melindungi kunci pada algoritma simetris.

Pada bab ini penulis membahas tentang bagaimana proses algoritma *hybrid* RSA dan *vigenere cipher*, dimana algoritma *vigenere cipher* berfungsi untuk melindungi suatu pesan sedangkan algoritma RSA berfungsi untuk melindungi kunci dari algoritma *vigenere cipher*. Berikut adalah penjelasan tentang algoritma *vigenere cipher* dan algoritma RSA dalam algoritma *hybrid*:

3.1.1 Algoritma *Vigenere Cipher*

Algoritma *vigenere cipher* merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk enkripsi dan dekripsinya, pada algoritma *hybrid* ini algoritma *vigenere cipher* menggunakan tabel konversi abjad A sampai Z. Kunci pada algoritma *vigenere cipher* dipakai berulang kali sebanyak pesan yang akan dienkripsi. Semakin beragam huruf *alfabet* yang dipakai sebagai kunci, maka semakin kuat pula keamanan algoritma *vigenere cipher*. Berikut adalah rumus algoritma *vigenere cipher* dalam algoritma *hybrid*:

Enkripsi: $C_i = (P_i + K_i)\ (mod\ 26)$

Dekripsi: $P_i = (C_i - K_i)\ (mod\ 26)$

Keterangan:

P_i = Huruf ke-i dalam *plaintext*

C_i = Huruf ke-i dalam *ciphertext*

K_i = Huruf ke-i dalam *Key*.

3.1.2 Algoritma RSA

Algoritma RSA merupakan algoritma asimetris yaitu menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya, pada algoritma *hybrid* ini algoritma RSA berfungsi untuk mengamankan kunci pada algoritma *vigenere cipher*. Kunci pada algoritma RSA dibangkitkan dengan menggunakan dua buah bilangan prima dengan langkah-langkah sebagai berikut:

1) Memilih p, q dimana p dan q adalah bilangan prima
2) Dihitung $n = p \times q$
3) Dihitung $\Phi(n) = (p-1) \times (q-1)$
4) Memilih bilangan integer e dimana $\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$
5) Dihitung d dimana $d \equiv e^{-1} \bmod \Phi(n)$, dan $d < \Phi(n)$, sehingga

$ed \equiv e.e^{-1} \ (mod\ \Phi(n))$	(Teorema 2.6)
$ed \equiv 1 \ (mod\ \phi(n))$	(Definisi Identitas)
$\phi(n) \mid ed - 1$	(Definisi 2.5)
$ed - 1 = \phi(n).t$	(Definisi 2.1)
$ed = \phi(n).t + 1$	(kedua ruas ditambah 1)
$d = \frac{\phi(n).t+1}{e}$	(kedua ruas dibagi e)

Berikut adalah rumus algoritma RSA dalam algoritma *hybrid*, karena suatu pesan dari algoritma RSA adalah kunci dari algoritma *vigenere cipher* maka $m = k$, sehingga:

Rumus enkripsi RSA

$$c = k^e \ (mod\ n)$$

Rumus dekripsi RSA

$$k = c^d \ (mod\ n) = (k^e)^d \ (mod\ n) = k^{ed} \ (mod\ n).$$

Keterangan:

e = Kunci umum.

d = Kunci rahasia.

c = *Cipherkey*.

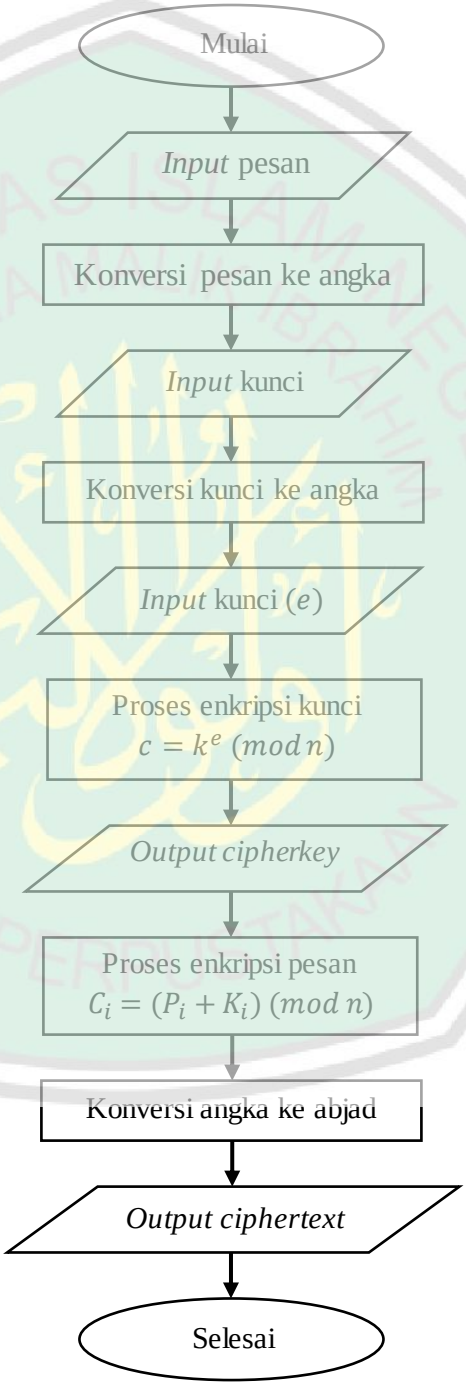
m = *Message*

k = *Plainkey*.

3.2 Proses Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan

3.2.1 Enkripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan

Berikut adalah *flowchart* enkripsi algoritma *hybrid* RSA dan *vigenere cipher* pada suatu pesan:



Gambar 3.1 *Flowchart* Enkripsi Algoritma *Hybrid*

Setalah membuat *flowchart* enkripsi algoritma *hybrid* RSA dan *vigenere cipher* pada suatu pesan, kemudian melakukan proses enkripsi pada pesan dengan menggunakan algoritma *vigenere cipher* dengan langkah-langkah sebagai berikut:

1. Tabel konversi abjad:

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

2. Pesan biasa atau *plaintext* (P_i):

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}
A	K	H	M	A	D	K	H	U	M	A	I	D	I	X
0	10	7	12	0	3	10	7	20	12	0	8	3	8	23

Catatan: agar panjang pesan sama dengan perulangan panjang kunci, maka otomatis pesan akan ditambahkan dengan sebarang huruf, misalkan huruf "X".

3. Kunci atau *key* (K_i):

K_1	K_2	K_3	K_4	K_5
M	A	M	A	T
12	0	12	0	19

4. Proses enkripsi pesan:

$$C_i = (P_i + K_i)\ (mod\ 26)$$

$$C_1 = (P_1 + K_1)\ (mod\ 26) = (0 + 12)\ (mod\ 26) = 12$$

$C_2 = (P_2 + K_2)\ (mod\ 26) = (10 + 0)\ (mod\ 26) = 10$

$C_3 = (P_3 + K_3)\ (mod\ 26) = (7 + 12)\ (mod\ 26) = 19$

$C_4 = (P_4 + K_4)\ (mod\ 26) = (12 + 0)\ (mod\ 26) = 12$

$C_5 = (P_5 + K_5)\ (mod\ 26) = (0 + 19)\ (mod\ 26) = 19$

$C_6 = (P_6 + K_1)\ (mod\ 26) = (3 + 12)\ (mod\ 26) = 15$

$C_7 = (P_7 + K_2)\ (mod\ 26) = (10 + 0)\ (mod\ 26) = 10$

$C_8 = (P_8 + K_3)\ (mod\ 26) = (7 + 12)\ (mod\ 26) = 19$

$C_9 = (P_9 + K_4)(mod\ 26) = (20 + 0)(mod\ 26) = 20$

$C_{10} = (P_{10} + K_5)\ (mod\ 26) = (12 + 19)\ (mod\ 26) = 5$

$C_{11} = (P_{11} + K_1)\ (mod\ 26) = (0 + 12)\ (mod\ 26) = 12$

$C_{12} = (P_{12} + K_2)\ (mod\ 26) = (8 + 0)\ (mod\ 26) = 8$

$C_{13} = (P_{13} + K_3)\ (mod\ 26) = (3 + 12)\ (mod\ 26) = 15$

$C_{14} = (P_{14} + K_4)\ (mod\ 26) = (8 + 0)\ (mod\ 26) = 8$

$C_{15} = (P_{15} + K_5)\ (mod\ 26) = (23 + 19)\ (mod\ 26) = 16$

5. Hasil enkripsi/ *ciphertext*/ pesan kode:

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
12	10	19	12	19	15	10	19	20	5	12	8	15	8	16
M	K	T	M	T	P	K	T	U	F	M	I	P	I	Q

Setelah pesan terenkripsi, kemudian kunci dari algoritma *vigenere cipher* di enkripsi dengan menggunakan algoritma RSA, berikut langkah-langkah proses enkripsi algoritma RSA pada kunci algoritma *vigenere cipher*:

1. Ambil sebarang bilangan prima $p = 7$ dan $q = 11$
2. Hitung $n = 7 \times 11 = 77$

3. Hitung $\Phi(n) = (7-1)(11-1) = 60$

4. Pilih bilangan bulat $e = 17$ dimana $\gcd(60, 17) = 1;\ 1 < 17 < 60$

5. Tabel konversi abjad:

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

6. *Plainkey* atau kunci dari algoritma *vigenere cipher* (k):

M	A	M	A	T
12	0	12	0	19

7. Proses enkripsi kunci:

$k^e \ (mod\ n) = c$

$12^{17}\ (mod\ 77) = 45$

$0^{17}\ (mod\ 77) = 0$

$12^{17}\ (mod\ 77) = 45$

$0^{17}\ (mod\ 77) = 0$

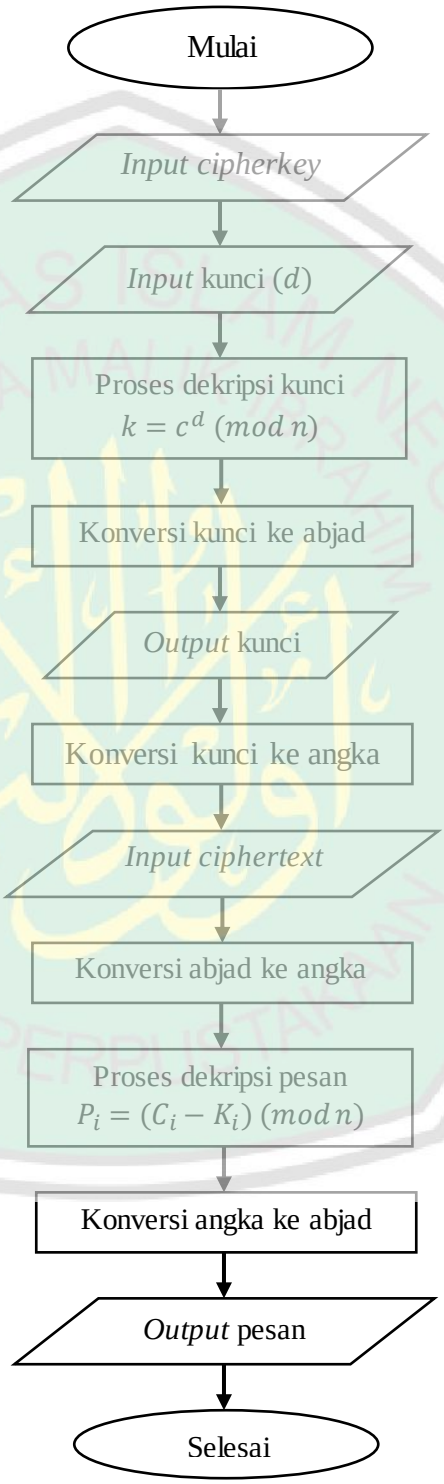
$19^{17}\ (mod\ 77) = 24$

8. *Cipherkey* atau kunci *vigenere cipher* kode:

45	0	45	0	24

3.2.2 Dekripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan

Berikut adalah *flowchart* dekripsi algoritma *hybrid* RSA dan *vigenere cipher* pada suatu pesan:



Gambar 3.2 *Flowchart* Dekripsi Algoritma *Hybrid*

Setalah membuat *flowchart* dekripsi algoritma *hybrid* RSA dan *vigenere cipher* pada suatu pesan, kemudian melakukan proses dekripsi pada kunci dengan menggunakan algoritma RSA dengan langkah-langkah sebagai berikut:

1. Ambil sebarang bilangan prima $p = 7$ dan $q = 11$
2. Hitung $n = 7 \times 11 = 77$
3. Hitung $\Phi(n) = (7-1)(11-1) = 60$
4. Pilih bilangan bulat $e = 17$ dimana $\gcd(60, 17) = 1;\ 1 < 17 < 60$
5. Hitung d yaitu:

   $d \equiv 17^{-1}\ (mod\ \Phi(n))$, dimana $d < \Phi(n)$

   $17d \equiv 1\ (mod\ 60)$

   $60|17d - 1$

   $17d - 1 = 60t$

   $17d = 60t + 1$

   $d = \dfrac{60t + 1}{17}$

   Maka, jika

   $t = 1 \rightarrow d = \dfrac{60.1 + 1}{17} = 3{,}59$

   $t = 2 \rightarrow d = \dfrac{60.2 + 1}{17} = 7{,}12$

   $\vdots \qquad \vdots$

   $\vdots \qquad \vdots$

   $t = 15 \rightarrow d = \dfrac{60.15 + 1}{17} = 53$

   Ditemukan hasil bilangan primanya yaitu

   $d = 53$, dimana $53 < 60$

6. *Cipherkey* atau kunci *vigenere cipher* kode (c):

45	0	45	0	24

7. Proses dekripsi kunci:

$c^d \ (mod\ n) = k$

$45^{53}\,(mod\ 77) = 12$

$0^{53}\,(mod\ 77) = 0$

$45^{53}\,(mod\ 77) = 12$

$0^{53}\,(mod\ 77) = 0$

$24^{53}\,(mod\ 77) = 19$

8. *Plainkey* atau kunci *vigenere cipher*:

12	0	12	0	19
M	A	M	A	T

Setelah kunci terdekripsi, kemudian pesan dapat di dekripsi dengan menggunakan algoritma *vigenere cipher*, berikut langkah-langkah proses dekripsi algoritma *vigenere cipher* pada suatu pesan:

1. Tabel konversi abjad:

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

2. *Ciphertext* atau pesan kode (*C*):

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
M	K	T	M	T	P	K	T	U	F	M	I	P	I	Q
12	10	19	12	19	15	10	19	20	5	12	8	15	8	16

3. Kunci atau *key* (*K*):

K_1	K_2	K_3	K_4	K_5
M	A	M	A	T
12	0	12	0	19

4. Proses dekripsi pesan:

$P_i = (C_i - K_i)\ (mod\ 26)$

$P_1 = (C_1 - K_1)\ (mod\ 26) = (12 - 12)\ (mod\ 26) = 0$

$P_2 = (C_2 - K_2)\ (mod\ 26) = (10 - 0)\ (mod\ 26) = 10$

$P_3 = (C_3 - K_3)\ (mod\ 26) = (19 - 12)\ (mod\ 26) = 7$

$P_4 = (C_4 - K_4)\ (mod\ 26) = (12 - 0)\ (mod\ 26) = 12$

$P_5 = (C_5 - K_5)(mod\ 26) = (19 - 19)\ (mod\ 26) = 0$

$P_6 = (C_6 - K_1)\ (mod\ 26) = (15 - 12)\ (mod\ 26) = 3$

$P_7 = (C_7 - K_2)(mod\ 26) = (10 - 0)\ (mod\ 26) = 10$

$P_8 = (C_8 - K_3)\ (mod\ 26) = (19 - 12)\ (mod\ 26) = 7$

$P_9 = (C_9 - K_4)\ (mod\ 26) = (20 - 0)\ (mod\ 26) = 20$

$P_{10} = (C_{10} - K_5)\ (mod\ 26) = (5 - 19)\ (mod\ 26) = 12$

$P_{11} = (C_{11} - K_1)(mod\ 26) = (12 - 12)\ (mod\ 26) = 0$

$P_{12} = (C_{12} - K_2)(mod\ 26) = (8 - 0)\ (mod\ 26) = 8$

$P_{13} = (C_{13} - K_3)\ (mod\ 26) = (15 - 12)\ (mod\ 26) = 3$

$$P_{14} = (C_{14} - K_4)\ (mod\ 26) = (8 - 0)\ (mod\ 26) = 8$$

$$P_{15} = (C_{15} - K_5)\ (mod\ 26) = (16 - 19)\ (mod\ 26) = 23$$

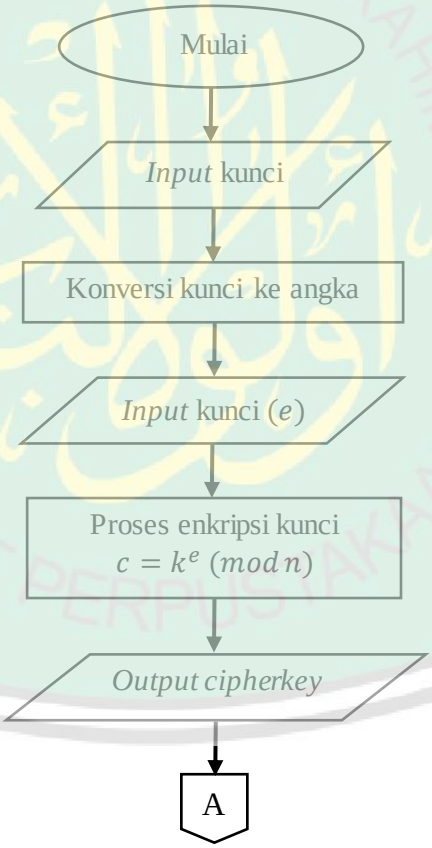
5. Hasil dekripsi/ *plaintext*/ pesan biasa:

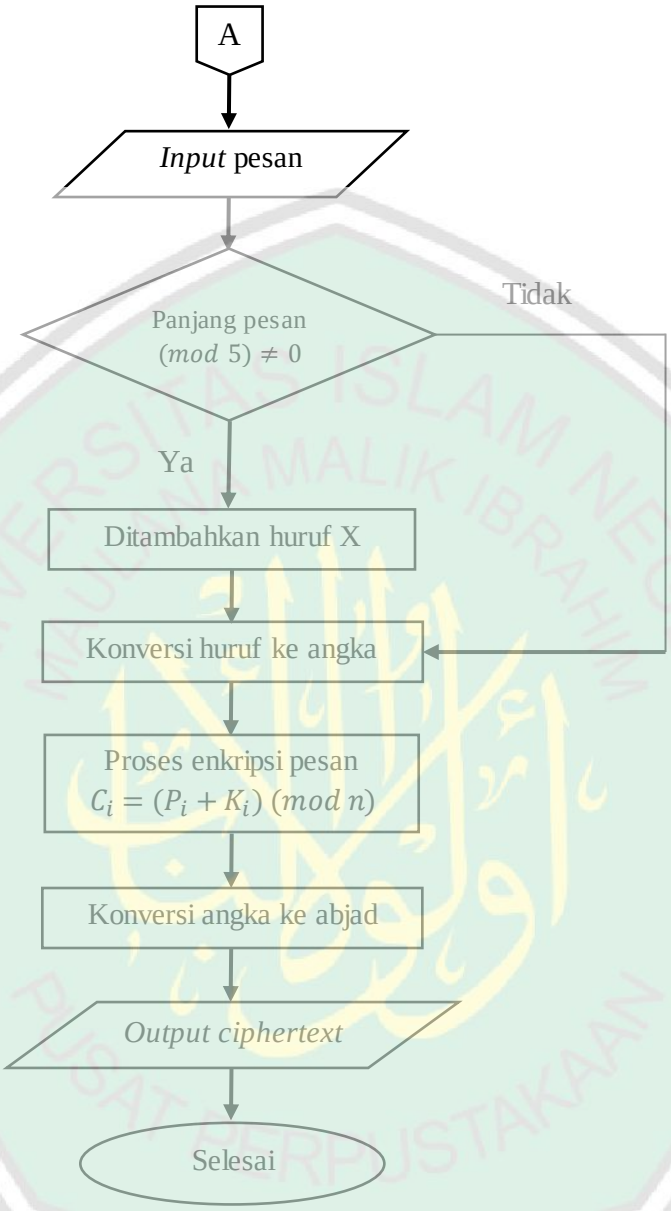
P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}
0	10	7	12	0	3	10	7	20	12	0	8	3	8	23
A	K	H	M	A	D	K	H	U	M	A	I	D	I	X

3.3 Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* dengan Menggunakan App Inventor pada Suatu Pesan

3.3.1 Halaman Enkripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* dengan Menggunakan App Inventor pada Suatu Pesan

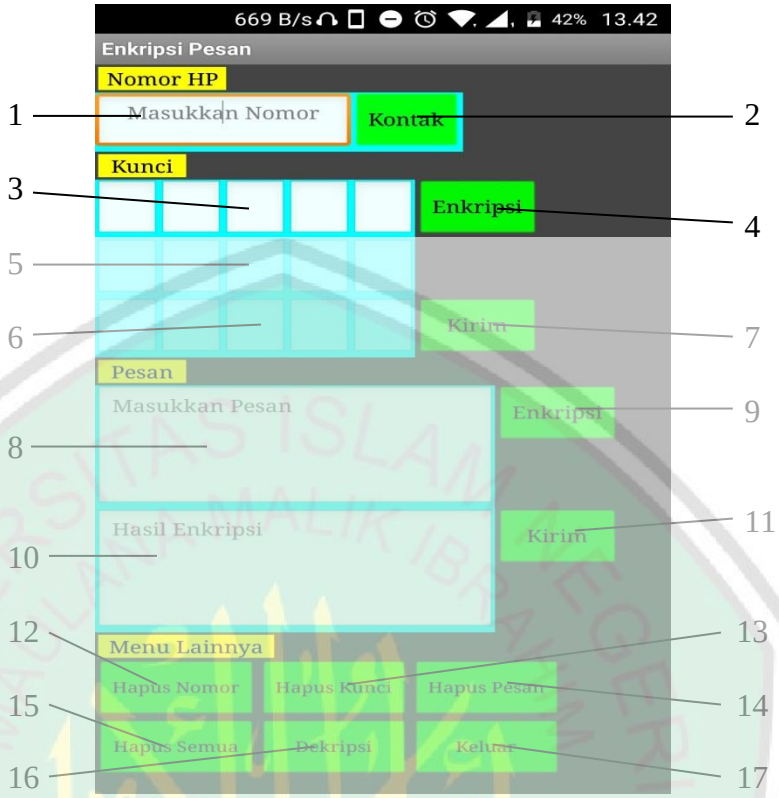
Pada bab ini aplikasi dibuat dengan menggunakan App Inventor. Sebelum membuat program Halaman Enkripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan, terlebih dahulu dibuat *flowchart*. Berikut adalah *flowchart* Halaman Enkripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan dengan Menggunakan App Inventor:





Gambar 3.3 *Flowchart* Halaman Enkripsi Aplikasi Algoritma *Hybrid*

Gambar tampilan Halaman Enkripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan dengan Menggunakan App Inventor ditunjukkan pada (Gambar 3.4) sebagai berikut:



Gambar 3.4 Tampilan Halaman Enkripsi Aplikasi Algoritma *Hybrid*

Pada (Gambar 3.4) di atas diketahui bahwa terdapat beberapa kolom dan tombol, berikut adalah kegunaan beberapa kolom dan tombol tersebut:

1. **Kolom Nomor** digunakan untuk memasukkan nomor *handphone* yang dituju.
2. **Tombol Kontak** digunakan untuk mencari nomor *handphone* pada kontak, kemudian dimasukkan ke dalam kolom nomor.
3. **Kolom Kunci** digunakan untuk memasukkan kunci (terdapat 5 kolom huruf pada kunci).
4. **Tombol Enkripsi Kunci** digunakan untuk mengonversi dan mengenkripsi kunci yang telah di *input*.
5. **Kolom Konversi Kunci** digunakan untuk keluaran konversi kunci.

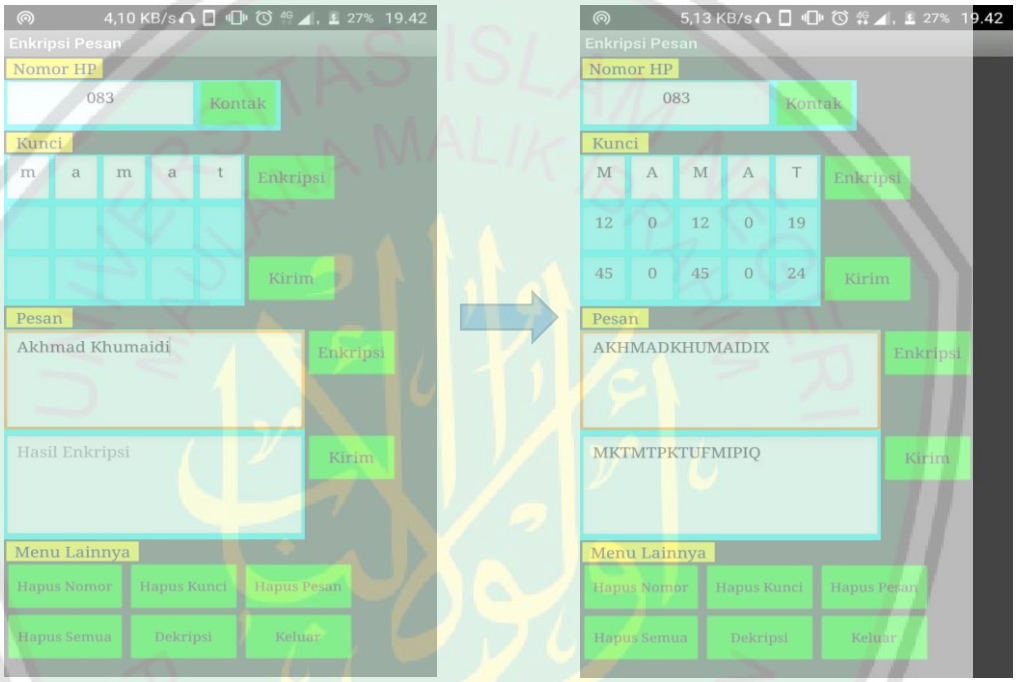
6. **Kolom Enkripsi Kunci** digunakan untuk keluaran enkripsi kunci.
7. **Tombol Kirim Kunci** digunakan untuk mengirim enkripsi kunci.
8. **Kolom Pesan** digunakan untuk membuat pesan yang akan dikirim.
9. **Tombol Enkripsi Pesan** digunakan untuk mengenkripsi pesan.
10. **Kolom Enkripsi Pesan** digunakan untuk keluaran hasil enkripsi pesan.
11. **Tombol Kirim Pesan** digunakan untuk mengirim enkripsi pesan.
12. **Tombol Hapus Nomor** digunakan untuk menghapus nomor *handphone*.
13. **Tombol Hapus Kunci** digunakan untuk menghapus kunci beserta *output*nya.
14. **Tombol Hapus Pesan** digunakan untuk menghapus pesan beserta *output*nya.
15. **Tombol Hapus Semua** digunakan untuk menghapus semua, baik itu nomor *handphone*, kunci, maupun pesan beserta *output*nya.
16. **Tombol Dekripsi** digunakan untuk menuju ke halaman dekripsi pesan.
17. **Tombol Keluar** digunakan untuk keluar dari aplikasi.

Adapun cara untuk menggunakan Halaman Enkripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan dengan Menggunakan App Inventor yaitu sebagai berikut:

1. Masukkan nomor *handphone* pada kolom nomor atau klik tombol kontak.
2. Masukkan kunci pada kolom kunci dengan setiap kolomnya berisi satu huruf.
3. Klik tombol enkripsi kunci, maka secara otomatis huruf pada kolom kunci akan menjadi kapital serta akan muncul *output* konversi dan enkripsi kunci pada kolom konversi dan enkripsi kunci.
4. Klik tombol kirim kunci untuk mengirim enkripsi kunci.
5. Masukkan pesan yang akan dikirim.

6. Klik tombol enkripsi pesan, maka secara otomatis pesan akan menjadi kapital dan menambahkan huruf X jika panjang pesan tidak sama dengan perulangan panjang kunci pesan, serta akan menampilkan *output* enkripsi pesan pada kolom enkripsi pesan.
7. Klik tombol kirim untuk mengirim enkripsi pesan.

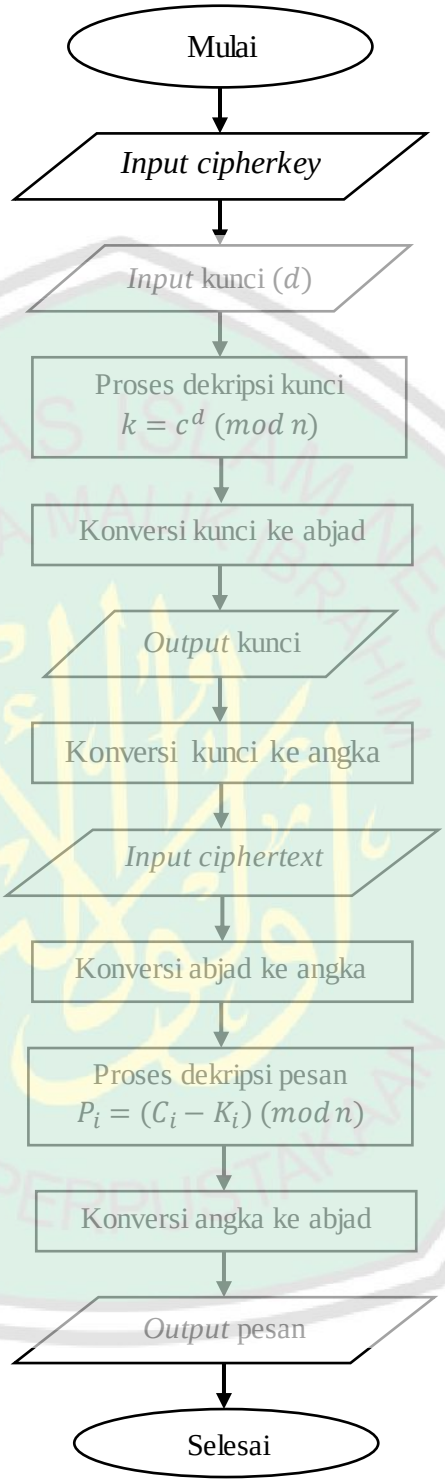
Untuk lebih jelasnya lihat contoh pada (Gambar 3.5) di bawah ini:



Gambar 3.5 Halaman Enkripsi Aplikasi Algoritma *Hybrid* pada Suatu Pesan

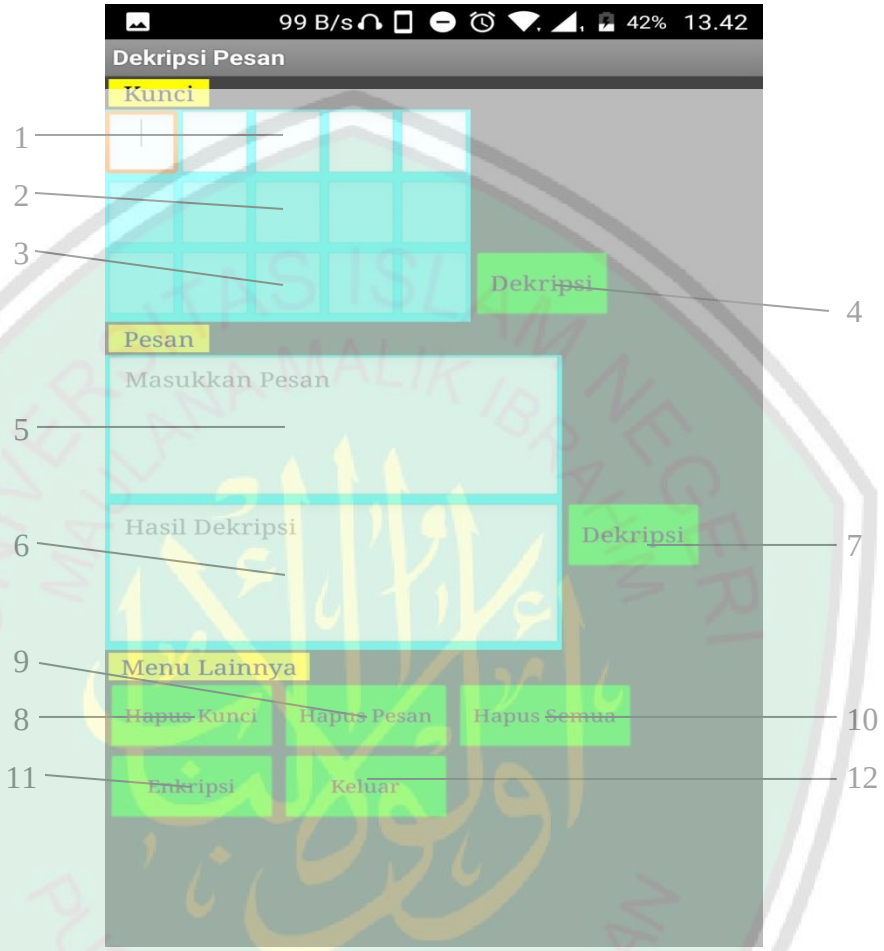
3.3.2 Halaman Dekripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* dengan Menggunakan App Inventor pada Suatu Pesan

Pada bab ini aplikasi dibuat dengan menggunakan App inventor. Sebelum membuat program Halaman Dekripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan, terlebih dahulu dibuat *flowchart*. Berikut adalah *flowchart* Halaman Dekripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan dengan Menggunakan App Inventor:



Gambar 3.6 *Flowchart* Halaman Enkripsi Aplikasi Algoritma *Hybrid*

Gambar tampilan Halaman Enkripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan dengan Menggunakan App Inventor ditunjukkan pada (Gambar 3.7) sebagai berikut:



Gambar 3.7 Tampilan Halaman Dekripsi Aplikasi Algoritma Hybrid

Pada (Gambar 3.7) di atas diketahui bahwa terdapat beberapa kolom dan tombol, berikut adalah kegunaan beberapa kolom dan tombol tersebut:

1. **Kolom Kunci Terenkripsi** digunakan untuk memasukkan kunci enkripsi yang telah diterima (terdapat 5 kolom nomor pada kunci enkripsi).
2. **Kolom Dekripsi Kunci** digunakan untuk keluaran dekripsi kunci.
3. **Kolom Konversi Kunci** digunakan untuk keluaran konversi dekripsi kunci.

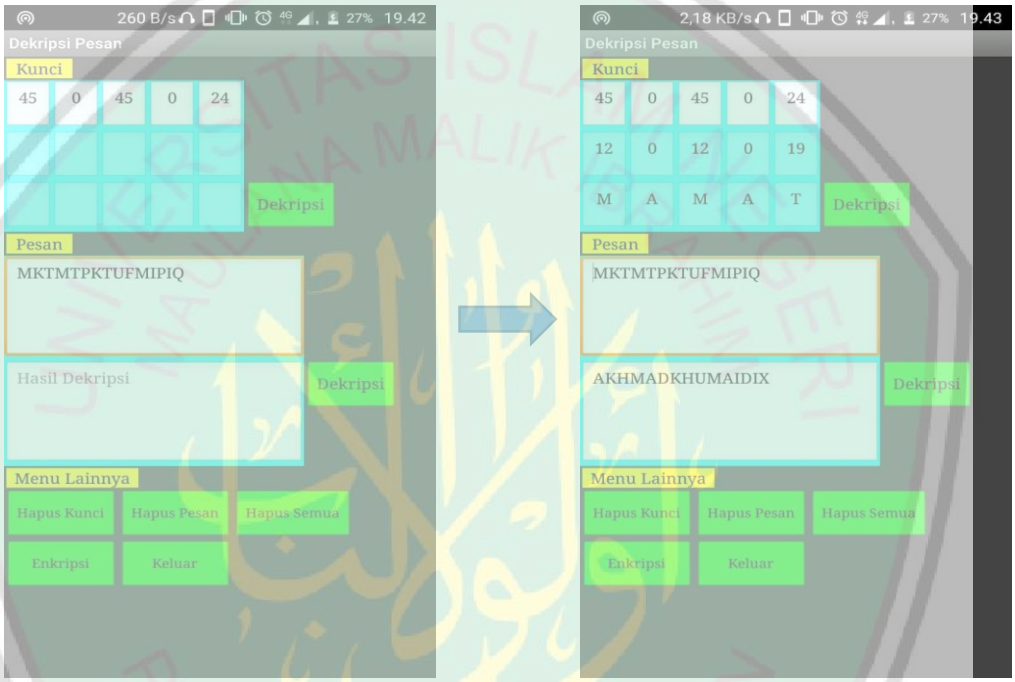
4. **Tombol Dekripsi Kunci** digunakan untuk mendekripsi dan mengonversi kunci yang telah diterima atau terenkripsi.
5. **Kolom Pesan Terenkripsi** digunakan untuk memasukkan pesan terenkripsi atau pesan yang telah diterima.
6. **Kolom Dekripsi Pesan** digunakan untuk keluaran hasil dekripsi pesan.
7. **Tombol Dekripsi Pesan** digunakan untuk mendekripsi pesan.
8. **Tombol Hapus Kunci** digunakan untuk menghapus kunci terenkripsi beserta *output* dekripsinya.
9. **Tombol Hapus Pesan** digunakan untuk menghapus pesan terenkripsi beserta *output* dekripsinya.
10. **Tombol Hapus Semua** digunakan untuk menghapus semua, baik itu kunci terenkripsi maupun pesan terenkripsi beserta *output* dekripsinya.
11. **Tombol Enkripsi** digunakan untuk menuju ke halaman enkripsi pesan.
12. **Tombol Keluar** digunakan untuk keluar dari halaman dekripsi pesan.

Adapun cara untuk menggunakan Halaman Dekripsi Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* pada Suatu Pesan dengan Menggunakan App Inventor yaitu sebagai berikut:

1. Masukkan kunci yang telah diterima atau terenkripsi, pada kolom kunci terenkripsi (kunci berisi 5 kolom nomor).
2. Klik tombol dekripsi kunci, maka secara otomatis nomor pada kolom kunci terenkripsi akan menjadi kapital serta akan muncul *output* dekripsi dan konversi kunci pada kolom dekripsi dan konversi kunci.

3. Masukkan pesan yang telah diterima atau terenkripsi pada kolom pesan terenkripsi.
4. Klik tombol dekripsi pesan, maka secara otomatis pesan terenkripsi akan menjadi kapital serta akan menampilkan *output* dekripsi pesan pada kolom dekripsi pesan.

Untuk lebih jelasnya lihat contoh pada (Gambar 3.8) di bawah ini:



Gambar 3.8 Halaman Dekripsi Aplikasi Algoritma *Hybrid* pada Suatu Pesan

Hasil akhir dari penelitian ini dapat dibuktikan bahwa baik secara manual maupun secara program aplikasi diperoleh hasil yang sama. Link download Aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* klik di bawah ini: https://drive.google.com/open?id=1-p6UQEpxtUWhmo_8iJ0kbpPamX4HulIe

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan hasil pembahasan, dapat diperoleh kesimpulan sebagai berikut:

1. Algoritma *hybrid* RSA dan *vigenere cipher* adalah algoritma yang menggabungkan dua buah algoritma yaitu algoritma RSA dan algoritma *vigenere cipher* dimana algoritma RSA berfungsi untuk mengamankan kunci dari algoritma *vigenere cipher* sedangkan algoritma *vigenere cipher* berfungsi untuk mengamankan suatu pesan.
2. Algoritma *hybrid* RSA dan *vigenere cipher* terdiri dari dua proses yaitu proses enkripsi dan dekripsi, proses enkripsi digunakan untuk mengamankan kunci dan pesan dengan cara mengubah ke bentuk yang tidak dapat dimengerti sedangkan proses dekripsi digunakan untuk mengubah kembali ke bentuk asal kunci dan pesan yang terenkripsi.
3. Penyandian pesan dengan Algoritma *Hybrid* RSA dan *Vigenere Cipher* dapat dibuat program aplikasi dengan menggunakan App Inventor, serta aplikasi Algoritma *Hybrid* RSA dan *Vigenere Cipher* tersebut dapat digunakan oleh orang lain untuk mengamankan suatu pesan dengan mudah.

4.2 Saran

Pada penelitian ini membahas tentang algoritma *hybrid* RSA dan *vigenere cipher* untuk mengamankan pesan. Untuk penelitian selanjutnya, disarankan untuk menggunakan algoritma kriptografi lainnya yang tingkat keamanannya lebih tinggi atau menggunakan aplikasi program komputer yang lainnya.

DAFTAR PUSTAKA

Abdussakir. 2009. *Matematika 1 Kajian Integratif Matematika dan Al-Qur'an*. Malang: UIN Malang Press.

Ad-Dimasyqi, Al-Imam Abul Fida Isma'il Ibnu Katsir. 2000. *Tafsir Ibnu Katsir Juz 5*. Terjemahan Bahrun Abu Bakar. Bandung: Sinar Baru Algensindo.

Ad-Dimasyqi, Al-Imam Abul Fida Isma'il Ibnu Katsir. 2001. *Tafsir Ibnu Katsir Juz 9*. Terjemahan Bahrun Abu Bakar. Bandung: Sinar Baru Algensindo.

Ariyus, Dony. 2006a. *Computer Security*. Yogyakarta: C.V Andi Offset.

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

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi Teori dan Implementasi*. Yogyakarta: C.V Andi Offset.

Ginting, Albert, dkk. 2015. Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, 3 (2): 253-258.

Harahap, Muhammad Khoiruddin. 2016. Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad. *Jurnal Nasional Informatika dan Teknologi Jaringan*, 1 (1): 61-64.

Irawan, Wahyu Henky, dkk. 2014. *Pengantar Teori Bilangan*. Malang: UIN-Maliki Press.

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

Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika.

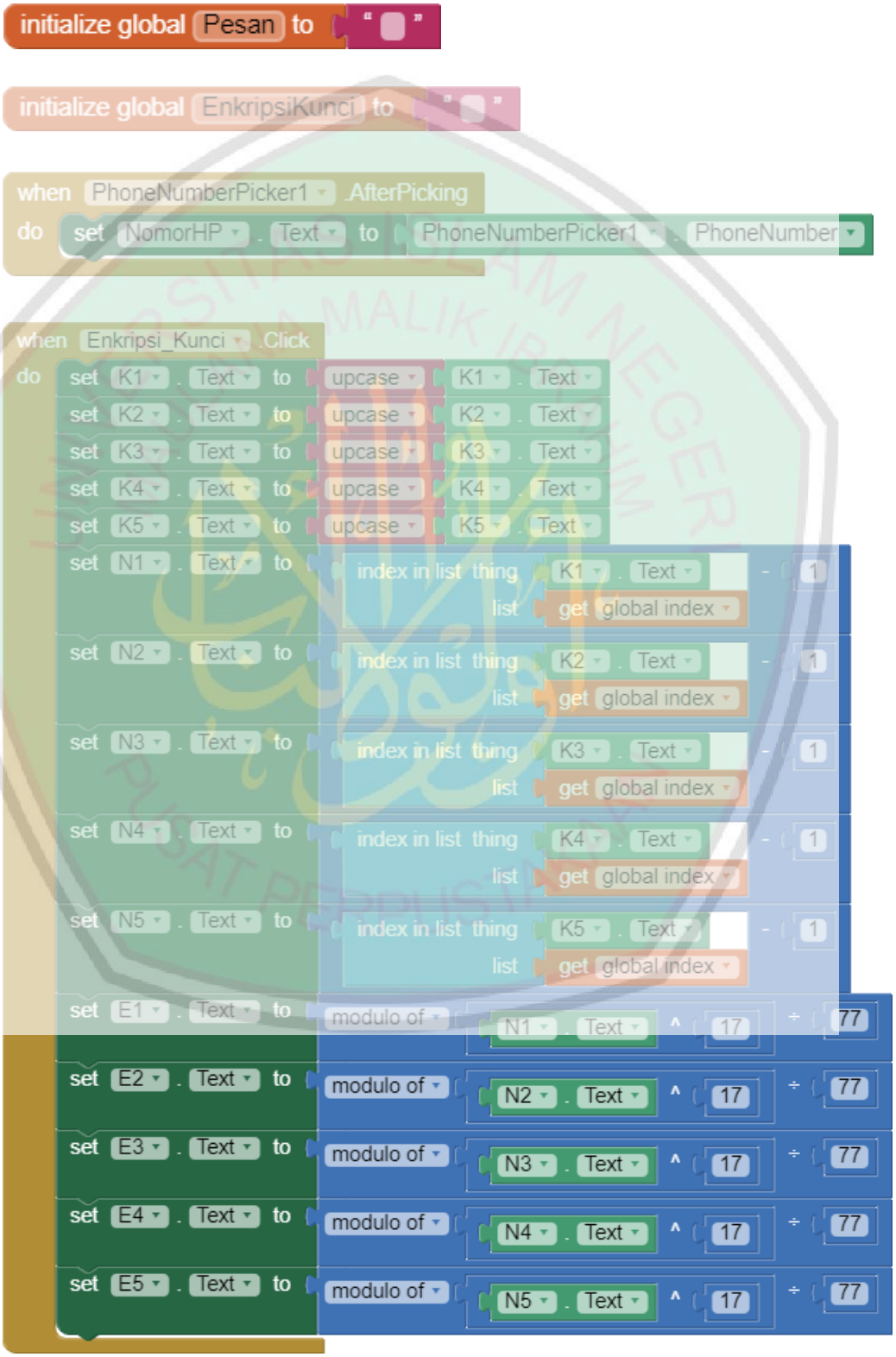
Munir, Rinaldi. 2012. *Matematika Diskrit*. Bandung: Informatika.

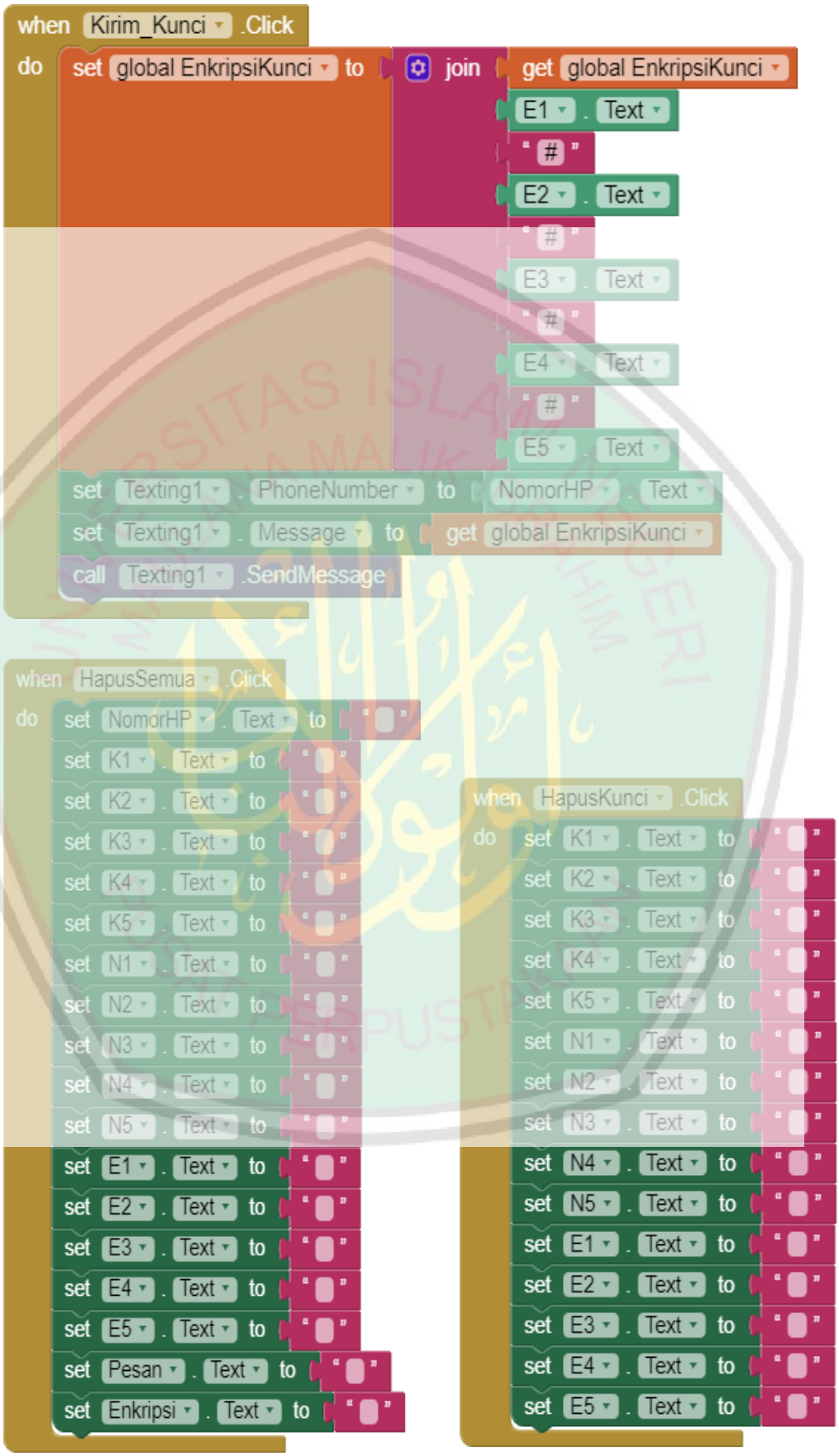
Prasetiyo, Ahmad Fajar. 2014. *App Inventor untuk Pemula*. Tangerang: Surya University

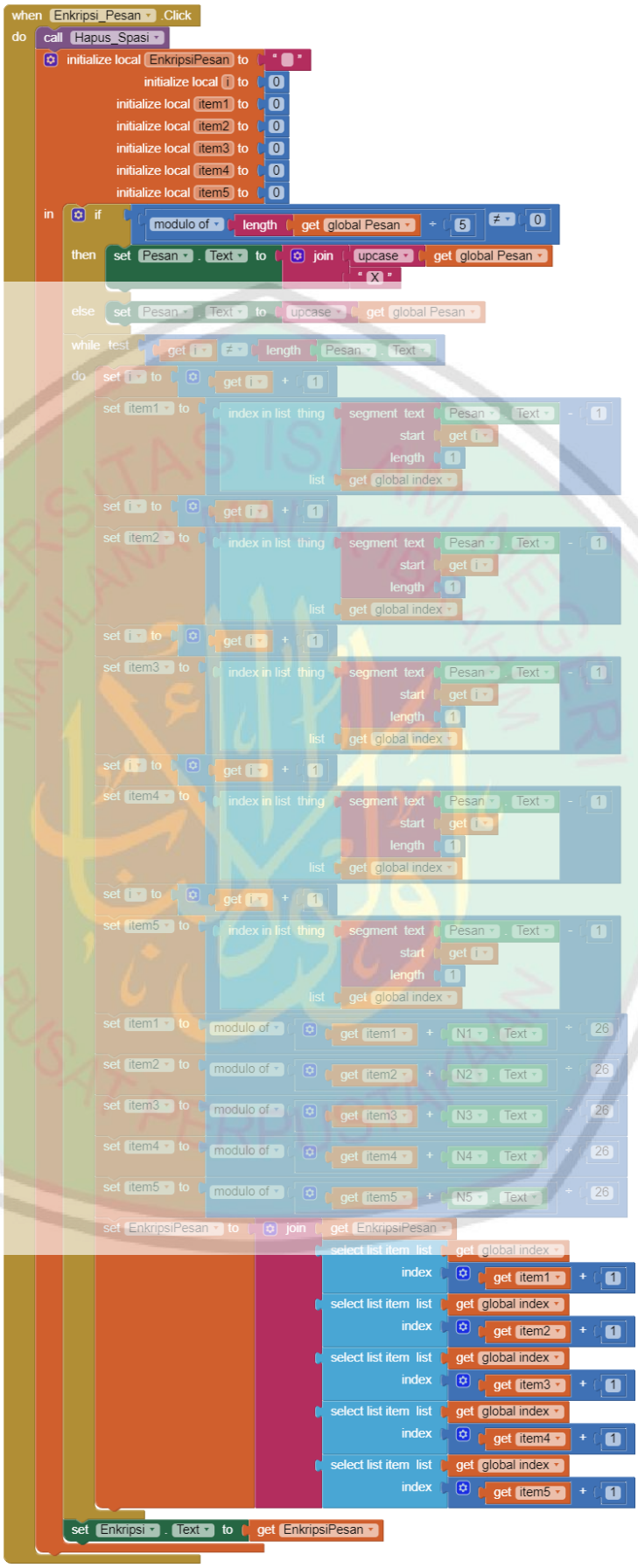
Wicaksono, kukuh nasrul. 2009. Modifikasi Vigenere cipher dengan Menggunakan Teknik Substitusi Berulang pada Kuncinya. (http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2008-2009/Makalah1/MakalahIF30581-2009-a002.pdf), diakses 15 Maret 2019.

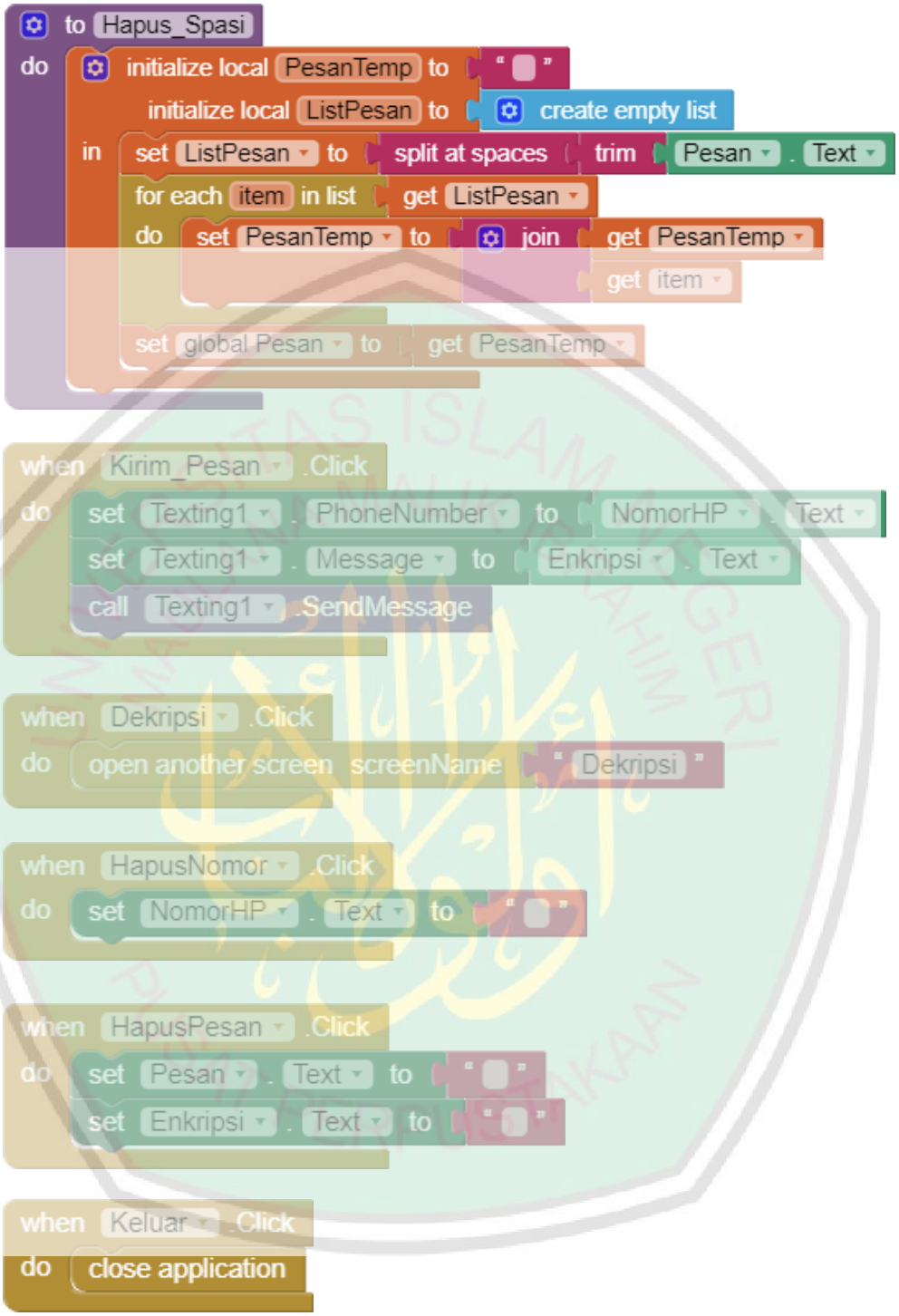
LAMPIRAN

1. Proses Enkripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher*

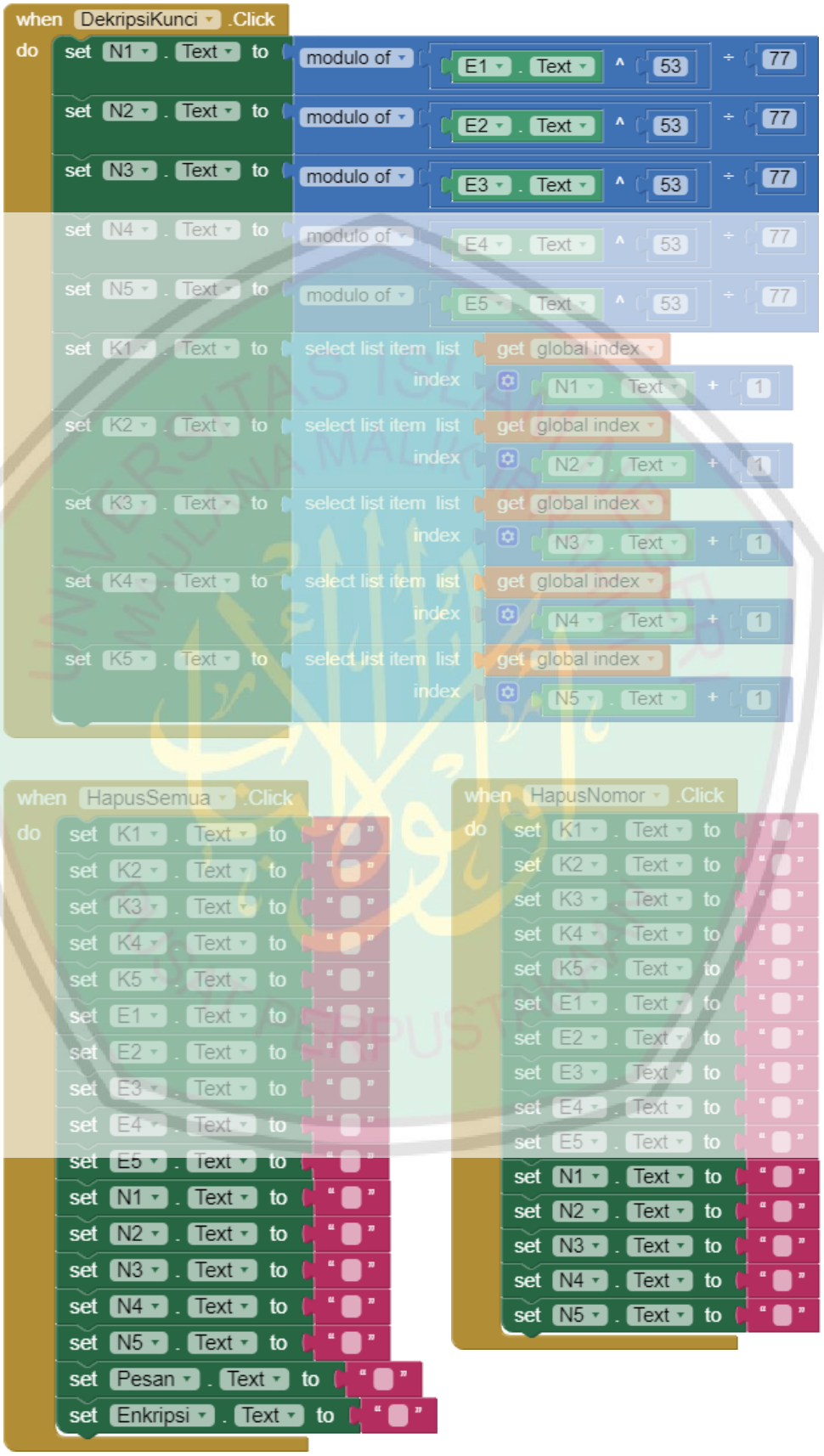


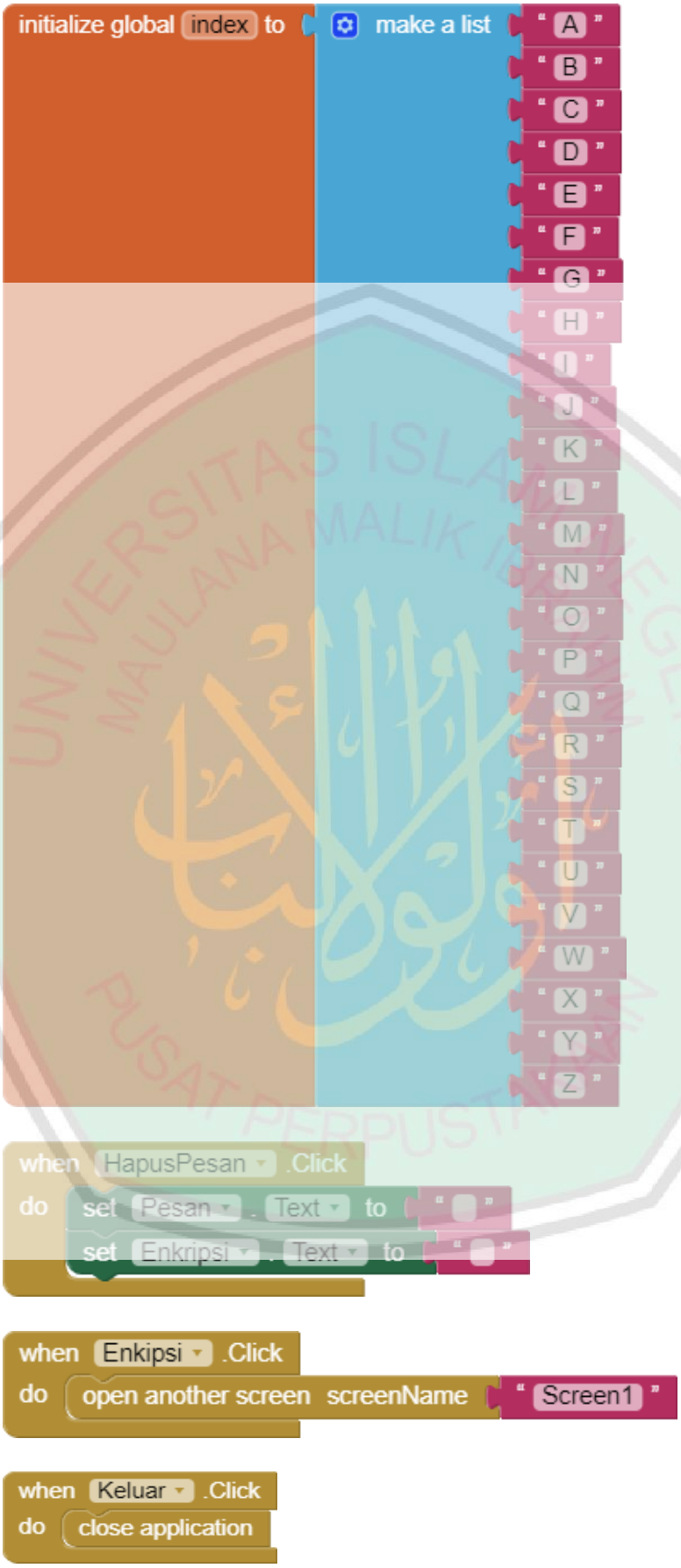


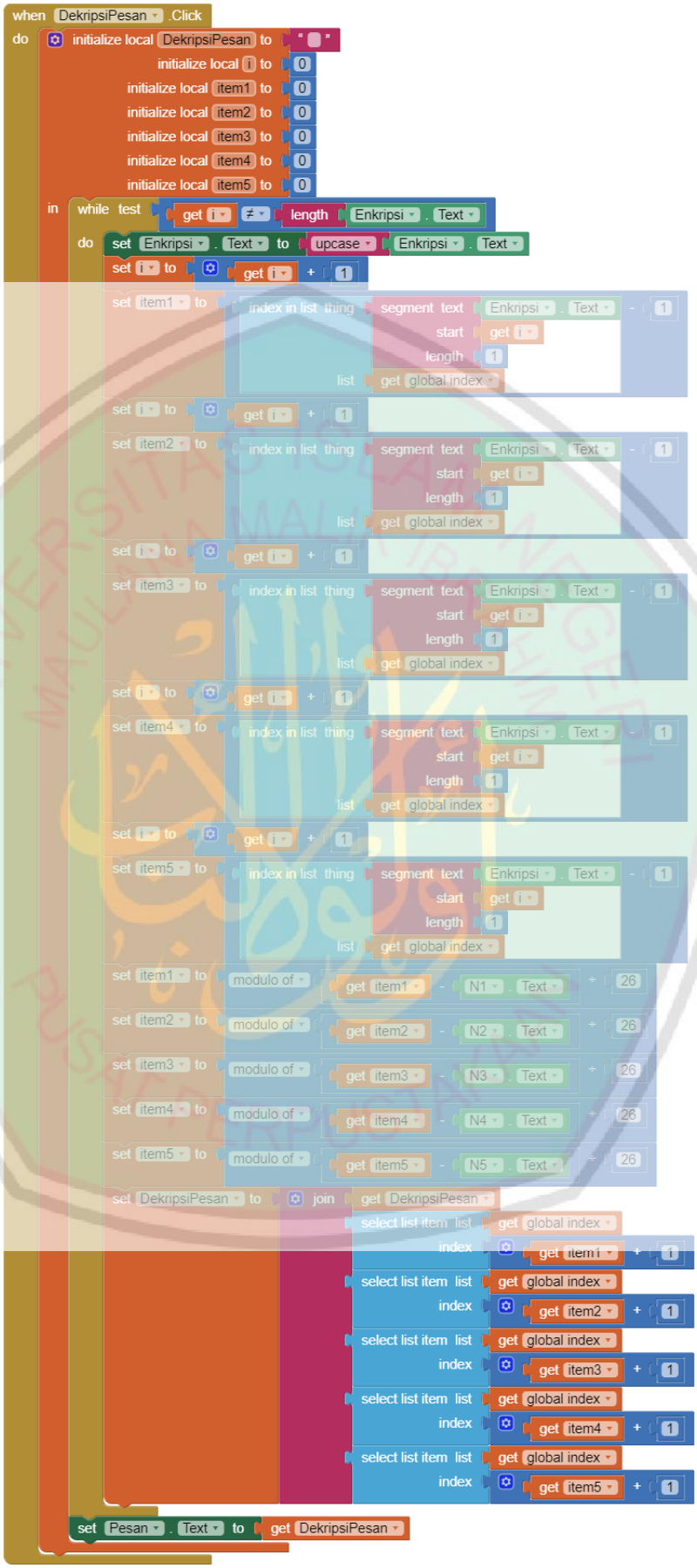




2. **Proses Dekripsi Algoritma *Hybrid* RSA dan *Vigenere Cipher***







RIWAYAT HIDUP

Akhmad Khumaidi, lahir di Kabupaten Pasuruan pada tanggal 30 Mei 1997, biasa dipanggil Mamat, tinggal di Desa Plinggisan RT 03 RW 02, Kecamatan Kraton, Kabupaten Pasuruan. Anak pertama dari Bapak Ismail dan Ibu Heni Masitoh.

Pendidikan dasarnya ditempuh di SDN 1 Plinggisan, Kecamatan Kraton, Kabupaten Pasuruan, dan lulus pada tahun 2009, setelah itu melanjutkan ke SMPN 6 Kota Pasuruan, Pohjentrek, Kecamatan Purworejo, Kota Pasuruan, dan lulus pada tahun 2012. Kemudian beliau melanjutkan pendidikan di MAN Kota Pasuruan, Purworejo, Kecamatan Purworejo, Kota Pasuruan, dan lulus pada tahun 2015. Pada tahun 2015 beliau menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil jurusan Matematika Fakultas Sains dan Teknologi.

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

BUKTI KONSULTASI SKRIPSI

Nama : Akhmad Khumaidi
NIM : 15610029
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Algoritma *Hybrid* RSA dan *Vigenere Cipher* untuk Mengamankan Pesan
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	23 April 2019	Konsultasi Bab I	1.
2.	30 April 2019	Konsultasi Bab I dan II	2.
3.	7 Mei 2019	ACC Bab I dan Bab II	3.
4.	15 Oktober 2019	Konsultasi Kajian Keagamaan	4.
5.	25 Oktober 2019	Konsultasi Kajian Keagamaan	5.
6.	9 Desember 2019	Konsultasi Bab III	6.
7.	12 Maret 2020	Konsultasi Bab III dan Bab IV	7.
8.	29 Januari 2020	Konsultasi Kajian Keagamaan	8.
9.	30 Maret 2020	ACC Kajian Keagamaan	9.
10.	30 Maret 2020	ACC Keseluruhan	10.

Malang, 30 Maret 2020
Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001