

**PENGAMANAN ALAMAT LAMAN PEMULIHAN KATA SANDI
MENGUNAKAN ALGORITMA RSA (*RIVEST, SHAMIR, ADLEMAN*)
DAN *BEAUFORT CIPHER***

PROPOSAL SKRIPSI

Oleh
Riyan Fahmi Syihabuddin
NIM.17610066



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

DAFTAR ISI

DAFTAR ISI	ii
DAFTAR GAMBAR	iv
DAFTAR TABEL	v
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan	3
1.4 Manfaat	3
1.5 Batasan Masalah	3
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	5
2.1 Teori Bilangan	5
2.1.1 Bilangan Bulat.....	5
2.1.2 Keterbagian	5
2.1.3 Kongruensi	7
2.1.4 Sistem Residu	8
2.2 Kriptografi.....	9
2.2.1 Pengertian Kriptografi	9
2.2.2 Sejarah Kriptografi.....	9
2.2.3 Komponen-komponen Kriptografi	10
2.2.4 Kriptogrfi Klasik dan Modern.....	11
2.2.5 Macam-macam Algoritma Kriptografi.....	11
2.2.6 Beaufort Cipher	13
2.2.7 Kriptografi RSA	14
2.3 Use case Diagram	15
2.4 Laman (Website).....	15
2.5 Kajian Keislaman Tentang Keamanan.....	16
BAB III PEMBAHASAN	21
3.1 Algoritma RSA dan <i>Beaufort Cipher</i>	21

3.1.1 Algoritma Beaufort Cipher	21
3.1.2 Algoritma RSA.....	22
3.2 Proses Algoritma RSA dan Beaufart Cipher pada Alamat Laman Pemulihan Kata Sandi	23
3.2.1 Enkripsi Algoritma RSA dan Beaufart Cipher	23
3.2.2 Deskripsi Algoritma RSA dan Beaufort Cipher.....	27
3.3 Pengimplementasian Algoritma RSA dan Beaufort Cipher Pada Alamat Laman Pemulihan Kata Sandi.....	31

DAFTAR PUSTAKA

DAFTAR GAMBAR

Gambar 2. 1 Algoritma Simetris.....	12
Gambar 2. 2 Algoritma Asimetris	12
Gambar 2. 3 Algoritma Hybrid.....	13
Gambar 3. 1 Flowchart Enkripsi Algoritma Hybrid	23
Gambar 3. 2 Flowchart Dekripsi Algoritma	27
Gambar 3. 3 Laman Login	31
Gambar 3. 4 Laman Lupa Password	32
Gambar 3. 5 Pesan dari Email Admin.....	32
Gambar 3. 6 Laman Pemulihan Kata Sandi	33

DAFTAR TABEL

Tabel 2. 1 Simbol pada Activity Diagram	15
---	----

BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem keamanan dalam bidang teknologi informasi di era 4.0 sangat dibutuhkan. Salah satu contohnya adalah pengamanan data pribadi. Data pribadi yang dimaksud adalah informasi pribadi yang diunggah ke internet. Berbahaya sekali jika data-data rahasia yang seharusnya tidak perlu diketahui orang lain bocor, efeknya sangat fatal. Proses pengunggahan informasi di internet biasanya digunakan ketika kita tengah membuat sebuah akun pada suatu wadah (*platform*) tertentu. Walaupun saat mengakses laman akun tersebut diberi syarat untuk mengisi kata sandi yang telah dibuat, seseorang terkadang lupa akan kata sandi yang telah dibuat. Permasalahan tersebut menjadikan diperlukannya sebuah sistem untuk memulihkan kata sandi tersebut namun tetap dengan suatu sistem keamanan. Upaya pengamanan tersebut dapat dilakukan dengan mengubah alamat laman pemulihan sandi. Proses pengamanan tersebut dapat dilakukan dengan pemanfaatan bidang ilmu matematika yaitu bidang ilmu kriptografi.

Kriptografi adalah bidang ilmu matematika dimana fokus ilmunya mempelajari bagaimana mengubah suatu data menjadi sebuah kode tertentu agar tidak sembarang orang mengetahui informasi yang diberikan. Konsep dasar 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 dibagi menjadi tiga macam menurut kuncinya yaitu simetris, asimetris, dan *hybrid*. Pertama, algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Kedua, 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 teks maupun karakter.

Fokus penelitian merujuk pada penganalisaan sistem pengamanan alamat laman pemulihan kata sandi menggunakan algoritma *Hybrid RSA (Rivest, Shamir, Adleman)* dan *Beufart Cipher*, dimana RSA adalah algoritma asimetris dan *Beufart Cipher* adalah algoritma simetris. Secara umum konsep kriptografi algoritma *hybrid* adalah pengubahan karakter yang akan diubah menjadi bentuk karakter yang tidak dimengerti dengan menggunakan kunci simetris biasa, kemudian kunci simetris diubah menjadi kunci simetris kode dengan menggunakan kunci umum, sehingga seseorang yang tidak mempunyai kunci simetris kode dan kunci rahasia tidak mengetahui kunci simetris biasa dan maksud karakter alamat laman yang tertera. Sedangkan sistem akan mengubah kunci simetris kode menjadi kunci simetris biasa dengan menggunakan kunci rahasia, sehingga proses penampilan laman pemulihan kata sandi dan proses pengubahan kata sandi akun dapat dibaca oleh sistem.

Berbicara konsep kriptografi, Allah dalam surat An-Nisa' ayat 58 berfirman:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا.....

Artinya:

“Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya”(QS. An-Nisa': 58).

Ayat tersebut menjelaskan betapa pentingnya pengamanan sebuah pesan. Hal ini berkesinambungan dengan fokus penelitian dimana pengamanan sebuah pemulihan kata sandi harus diterapkan, karena tidak semua orang berhak mengakses akun orang lain. Data-data yang telah tersimpan haruslah hak konsumsi pribadi. Berdasarkan paparan-paparan yang telah dijelaskan, muncullah inspirasi untuk membuat penelitian pengamanan alamat laman pemulihan kata sandi menggunakan algoritma RSA dan *Beaufart Cipher*.

1.2 Rumusan Masalah

Rumusan masalah yang diangkat dalam penelitian ini adalah:

1. Bagaimana proses Algoritma dengan menggunakan RSA dan *Beufort Cipher*?
2. Bagaimana proses enkripsi dan dekripsi Algoritma RSA dan *Beufart Chiper* dalam alamat laman pemulihan kata sandi?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Mengetahui proses Algoritma *Hybrid* dengan menggunakan RSA dan *Beaufart Cipher*.
2. Mengimplementasikan Algoritma *Hybrid* RSA dan *Beaufart Cipher* pada pengamanan alamat laman pemulihan kata sandi.

1.4 Manfaat

Manfaat yang dapat diperoleh dari kegiatan penelitian ini diantaranya adalah:

1. Menambah wawasan bidang ilmu kriptografi khususnya Algoritma *Hybrid* dengan menggunakan RSA dan *Beaufart Cipher*.
2. Berkontribusi terhadap perkembangan sistem keamanan bidang teknologi dan informasi di Indonesia.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini ada tiga yaitu:

1. Implementasi enkripsi dan dekripsi hanya berdasarkan *Hybrid* RSA dan *Beaufort Cipher*.
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. Pengimplementasian hanya terbatas pada alamat laman pemulihan kata sandi.

1.6 Metodologi Penelitian

Metode penelitian ini adalah metode kepustakaan (*library research*) yaitu menggunakan metode yang menggunakan studi literatur berkaitan dengan penelitian seperti buku, jurnal penelitian, skripsi dan laporan penelitian. Berikut langkah-langkah sebagai berikut:

1. Mencari penelitian-penelitian berhubungan dengan algoritma RSA dan *Beaufart Cipher*
2. Menjelaskan tentang algoritma RSA dan *Beaufart Cipher*.
3. Memberikan contoh serta langkah-langkah enkripsi dan dekripsi algoritma *Hybrid RSA* dan *Beaufart Cipher*.
4. Mengimplementasikan algoritma RSA dan *Beaufart Cipher* kedalam sebuah alamat laman pemulihan kata sandi.

1.7 Sistematika Penulisan

Sistematika penulisan penelitian ini terdiri dari empat bab dan masing-masing dari bab tersebut akan dibagi ke dalam subbab dengan rumusan sebagai berikut:

BAB I Pendahuluan

Pendahuluan terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II Kajian Pustaka

Kajian pustaka terdiri dari teori-teori dan konsep-konsep yang mendukung dalam proses penelitian. Teori dan konsep tersebut meliputi teori bilangan, konsep kriptografi, pangkalan data (*data base*), laman *website*, dan kajian keislaman tentang pengamanan informasi.

BAB III Pembahasan

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

BAB IV Penutup

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

BAB II TINJAUAN PUSTAKA

2.1 Teori Bilangan

Secara umum, teori bilangan merupakan kajian tentang sifat-sifat bilangan asli. Lebih spesifiknya, teori bilangan mempelajari tentang bilangan beserta sifat-sifatnya. Sebagai salah satu cabang matematika, teori bilangan disebut sebagai “aritmetika lanjut (*advanced arithmetics*)” 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 $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. 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)

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).

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 ($gcd = \text{greatest common divisor}$, $gcf = \text{greatest common factor}$) 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 y
 $d = (x_1, x_2, \dots, x_n)$ dibaca d adalah (pembagi) persekutuan terbesar dari x_1, x_2, \dots, 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).

Definisi 2.3

Bilangan a dan b dikatakan prima relatif jika $(a, b) = 1$

Teorema 2.2

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

2.1.3 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 $a \equiv b \pmod{m}$, 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 $a \not\equiv b \pmod{m}$, 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: $a \equiv b \pmod{m}$ jika dan hanya jika $b \equiv a \pmod{m}$ (Muhsetyo, 1997:138).

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

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

$a = b + km$, yang dalam hal ini adalah sembarang k adalah bilangan bulat.

Teorema 2.4

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

1. Refleksif $a \equiv a \pmod{m}$
2. Simetris, jika $a \equiv b \pmod{m}$, maka:
 $b \equiv a \pmod{m}$ dan $a - b \equiv 0 \pmod{m}$ adalah pernyataan yang ekuivalen
3. Transitif, jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$ maka $a \equiv c \pmod{m}$
 (Irawan, dkk, 2014:64-65).

Teorema 2.5

Jika $a \equiv b \pmod{m}$, maka $(a + c) \equiv (b + c) \pmod{m}$ (Irawan, dkk, 2014:65)

Teorema 2.6

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

Teorema 2.7

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

Teorema 2.8

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

2.1.4 Sistem Residu**Definisi 2.6**

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

- $(r_i, m) = 1$ ($i = 1, 2, \dots, k$).
- $r_i \not\equiv r_j \pmod{m}$ untuk semua $i \neq j$.
- Jika $(x, m) = 1$, maka $x \equiv r \pmod{m}$ (Muhsetyo, 1997:279).

Contoh:

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

- $r_1 = 1, (r_1, 6) = (1, 6) = 1$ dan $r_2 = 5, (r_2, 6) = (5, 6) = 1$
- $1 \not\equiv 5 \pmod{6}$
- $(7, 6) = 1 \rightarrow 7 \equiv 1 \pmod{6}$
 $(11, 6) = 1 \rightarrow 11 \equiv 5 \pmod{6}$.

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:

- Himpunan $\{1, 2, 3, 4\}$ adalah sistem residu tereduksi modulo 5 sehingga $\phi(5) = 4$

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).

Teorema 2.10 (Teorema Euler)

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

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

Teorema 2.11 (Teorema Kecil Fermat)

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

1. $a = 11; p = 2; \phi(2) = 1; 11^1 = 11 \equiv 1 \pmod{2}$
6. $a = 10; p = 3; \phi(3) = 2; 10^2 = 100 \equiv 1 \pmod{3}$

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, 2006).

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, 2006: 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. Deskripsi

Dekripsi merupakan kebalikan dari enkripsi yaitu pesan yang telah dienkrpsi 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 Kriptografi 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: yaitu teknik yang menggunakan permutasi karakter (Ariyus, 2006:16).

2. Kriptografi Modern

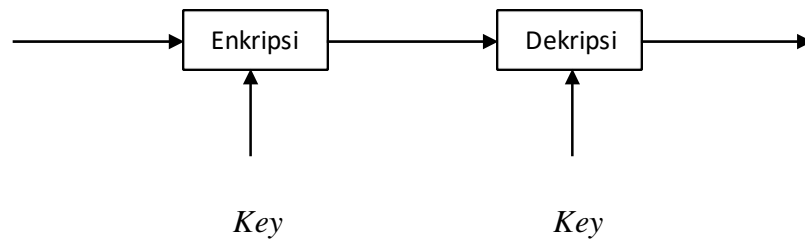
Kriptografi modern merupakan suatu algoritma yang digunakan pada zaman sekarang ini, yang mana kriptografi modern mempunyai kerumitan yang sangat kompleks, karena dalam menjalankannya memerlukan bantuan komputer (Ariyus, 2006: 16).

2.2.5 Macam-macam Algoritma Kriptografi

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

1. Algoritma Simetris

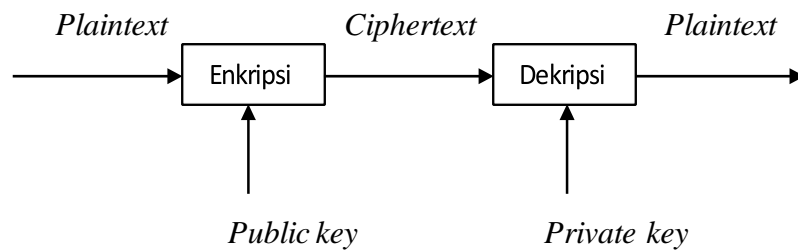
Algoritma Simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Lebih jelasnya perhatikan pada gambar 2.1 berikut:



Gambar 2. 1 Algoritma Simetris

2. Algoritma Asimetris

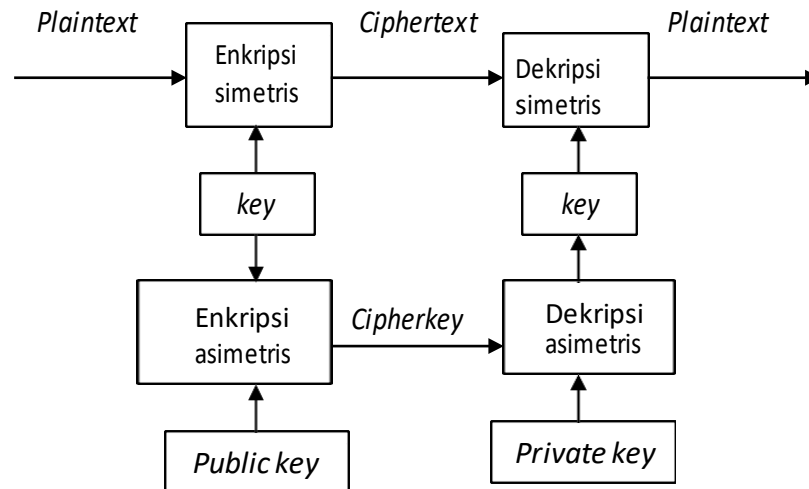
Algoritma Asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya, untuk enkripsi disebut kunci umum (*public key*) dan untuk dekripsi disebut kunci rahasia (*private key*). Contoh algoritma asimetris yang terkenal yaitu algoritma RSA (merupakan singkatan dari nama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



Gambar 2. 2 Algoritma Asimetris

3. Algoritma Hybrid

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



Gambar 2. 3 Algoritma Hybrid

2.2.6 Beaufort Cipher

Beaufort Cipher adalah cipher substitusi *polyalphabetic* yang mirip dengan *Vigenère Cipher*. *Beaufort cipher* pada awalnya diusulkan oleh Giovanni Sestri pada tahun 1710 dan kemudian diberikan nama oleh Sir Francis Beaufort. Algoritma *Beaufort Cipher* menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut bisa lebih pendek ataupun sama dengan panjang *plaintext*. Jika panjang kunci kurang dari panjang *plaintext*, maka kunci tersebut akan diulang secara periodik hingga kunci tersebut sama dengan *plaintext*. Rumus substitusi *Beaufort Cipher*.

$$f_i(a) = (k_i - a) \bmod n$$

Rumus dekripsi *Beaufort Cipher*

$$f_i^{-1}(c) = (k_i - c) \bmod n$$

Dimana :

f_i = nilai desimal karakter ke $-i$

c = nilai desimal karakter *chipertext*

a = nilai decimal karakter *plaintext*

k_i = nilai decimal karakter kunci ke $-i$

n = jumlah huruf

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).

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

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

Rumus dekripsi

$$M = C^d \bmod n = (M^e)^d \bmod n$$

$$\begin{aligned} \text{Dihitung } \Phi(n) &= (p - 1)(q - 1) \\ &= M^{ed} \bmod n \end{aligned}$$

Pembangkitan kunci pada algoritma RSA: Memilih p, q dimana p dan q adalah bilangan prima dihitung:

$$n = p \times q$$

Memilih bilangan integer e dimana

$$\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$$

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





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

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

2.3 Use case Diagram

Menurut Rosa dalam jurnal (Sari dan David, 2017) mengungkapkan “*Activity Diagram* menggambarkan *work flow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis. Perlu diperhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas dapat dilakukan oleh sistem”. Simbol-simbol yang digunakan dalam *activity diagram* sebagai berikut:

Tabel 2. 1 Simbol pada Activity Diagram

Simbol	Deskripsi
Simbol <i>Start</i> 	Simbol <i>start</i> untuk menyatakan awal dari suatu proses.
Simbol <i>Stop</i> 	Simbol <i>stop</i> untuk menyatakan akhir dari suatu proses.
Simbol <i>Decision</i> 	Simbol <i>decision</i> digunakan untuk menyatakan kondisi dari suatu proses.
Simbol <i>Action</i> 	Simbol <i>action</i> menyatakan aksi yang dilakukan dalam suatu arsitektur sistem

2.4 Laman (Website)

Website merupakan sebuah jenis aplikasi yang menggunakan teknologi browser untuk menjalankan sebuah aplikasi tersebut dengan di akses melalui jaringan *portable* (Pablo, 2017). Sedangkan pengertian aplikasi berbasis *website* yang lainnya memiliki pengertian aplikasi berbasis *website* merupakan sebuah program yang tersimpan pada sebuah server kemudian dikirim melalui internet dan diakses dengan melalui tampilan muka *browser* (Budiman, 2016). Aplikasi ini merupakan sistem paling banyak digunakan di masa ini, mengingat *website* merupakan sebuah *platform* yang sangat sering digunakan dalam kehidupan sehari-hari. Orang yang ahli dalam bidang ini pun sangat dibutuhkan utamanya dalam

sistem pemerintahan, perkantoran, kedinasan, maupun organisasi-organisasi tertentu.

2.5 Kajian Keislaman Tentang Keamanan

Kenikmatan aman adalah merupakan nikmat yang luar biasa. Sebab dengan keamanan itu kita bisa ibadah *enak*, dengan keamanan itu rezeki pun jadi *enak* juga. Bayangkan kalau rezekinya banyak tapi tidak aman, nyawa akan terancam, pasti sebanyak apapun harta tersebut tapi kalau keadaannya tidak aman kita tidak akan bisa menikmati rezeki. Kalau kita badannya sehat, kuat, tapi tidak aman, tetap saja kita tidak bisa menikmati kehidupan. Oleh karena itu, aman merupakan nikmat. Maka kewajiban kita adalah banyak-banyak mengingat nikmat Allah. Sebagaimana Allah swt berfirman:

يَا أَيُّهَا الَّذِينَ آمَنُوا اذْكُرُوا نِعْمَةَ اللَّهِ عَلَيْكُمْ ۝ (9)

Artinya:

“Wahai orang-orang yang beriman, ingatlah nikmat Allah yang Allah berikan kepada kalian itu.” (QS. Al-Ahzab[33]: 9)

Hal-hal yang berkaitan dengan kenikmatan-kenikmatan dari keamanan yang Allah berikan kepada kita.

1. Nikmat keamanan lebih besar dari nikmat rezeki

Allah swt berfirman dalam surat Al-Baqarah ayat 126:

وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا بَلَدًا آمِنًا وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ مَنْ آمَنَ مِنْهُمْ بِاللَّهِ وَالْيَوْمِ
الْآخِرِ

Artinya:

“Dan ingatlah ketika Nabi Ibrahim berkata, ‘Wahai Rabb, jadikan negeri ini negeri yang aman (yaitu Mekah) dan berikan rezeki penduduknya.’” (QS. Al-Baqarah[2]: 126)

Nabi Ibrahim yang diminta pertama kali adalah aman dulu, kemudian yang kedua Nabi Ibrahim minta supaya penduduknya dikasih rezeki. Maka di sini Nabi Ibrahim mendahulukan keamanan daripada rezeki. Hal ini karena 2 sebab yaitu karena kalau aman rezeki juga banyak, kalau tidak perang, untuk perputaran perekonomian pun juga mudah. Dengan adanya keamanan petani juga aman, bisa bercocok tanam. Adanya keamanan, orang berdagang juga aman, tidak ada yang

merampok, tidak ada yang mengambil. Bayangkan kalau misalnya perang, tidak aman, perekonomian bakal macet. Maka di sini didahulukan, Nabi Ibrahim minta keamanan dulu. Sebab yang kedua, walaupun ada rezeki tapi kalau tidak ada keamanan, maka pada waktu itu kita tidak bisa menikmati rezeki. Maka penting sekali kita berusaha menjaga keamanan.

Separah apapun kondisi perekonomian yang penting aman terlebih dahulu. Karena ketika perekonomian morat-marit terkadang banyak orang yang kemudian pikirannya pendek. Akhirnya melakukan pencurian, perampokan dan yang lainnya. Akhirnya tidak aman. Sudah tidak aman, perekonomian yang terpuruk akan ditambah terpuruk lagi. Akan tetapi jika perekonomian terpuruk tapi aman, insaallah sedikit demi sedikit bisa diperbaiki.

2. Allah mengungkit-ungkit tentang nikmat keamanan

Allah berfirman:

أَوَلَمْ نُمْكِّنْ لَهُمْ حَرَمًا آمِنًا يُجْبَىٰ إِلَيْهِ ثَمَرَاتُ كُلِّ شَيْءٍ

“Bukankah -kata Allah- Kami telah memapankan keamanan untuk negeri Haram itu, dimana buah-buahan pun didatangkan kepadanya.” (QS. Al-Qashash[28]: 57)

Di sini Allah menyebutkan dalam redaksi pengingatan bawah ini nikmat buat kamu, ingat sama kamu, jangan dilupakan! Karena nikmat aman itu luar biasa. Allah juga berfirman dalam Surat Al-Ankabut ayat 67:

أَوَلَمْ يَرَوْا أَنَّا جَعَلْنَا حَرَمًا آمِنًا وَيُتَخَطَّفُ النَّاسُ مِنْ حَوْلِهِمْ أَفَبِالْبَاطِلِ يُؤْمِنُونَ
وَبِنِعْمَةِ اللَّهِ يَكْفُرُونَ ﴿٦٧﴾

“Apakah mereka tidak melihat bahwa Kami sudah menjadikan negeri Haram itu aman, sementara negeri-negeri di sekelilingnya banyak orang yang diculik dan dibunuh. Apakah mereka beriman kepada yang bathil dan mereka kafir kepada nikmat-nikmat Allah?” (QS. Al-Ankabut[29]: 67)

Di sini Allah mengingatkan tentang nikmat aman, “Wahai kaum musyrikin Quraisy, apa kalian tidak ingat bahwa di Mekah ternyata benar-benar aman dibandingkan di negeri-negeri sekitar Mekah yang tidak aman, banyak penyamun, banyak pencuri dan yang lainnya.” Maka dari itu, Allah berfirman:

الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَآمَنَهُمْ مِنْ خَوْفٍ ﴿٤﴾

“Yang telah memberikan kepada mereka makanan saat kelaparan dan memberikan keamanan di saat ketakutan.” (QS. Qurasy[106]: 4)

Hal itu nikmat Allah yang besar. Allah juga berfirman dalam Al-Baqarah ayat 125:

وَإِذْ جَعَلْنَا الْبَيْتَ مَثَابَةً لِّلنَّاسِ وَأَمْنًا

“Dan ingatlah ketika Kami telah menjadikan Ka’bah ini sebagai tempat manusia berkumpul dan keamanan untuk mereka.” (QS. Al-Baqarah[2]: 125)

Allah juga mengingatkan nikmat keamanan kepada para sahabat Nabi.

Allah berfirman dalam surat Al-Anfal ayat 26:

وَاذْكُرُوا إِذْ أَنْتُمْ قَلِيلٌ مُّسْتَضْعَفُونَ فِي الْأَرْضِ تَخَافُونَ أَنْ يَتَخَطَّفَكُمُ النَّاسُ فَآوَاكُمْ وَأَيَّدَكُمْ بِنَصْرِهِ وَرَزَقَكُمْ مِنَ الطَّيِّبَاتِ لَعَلَّكُمْ تَشْكُرُونَ (٢٦)

“Dan ingatlah disaat dulu jumlah kalian sedikit kalian pun ditindas, kalian pun merasa takut untuk diculik dan dibunuh oleh manusia, lalu Allah memberikan kepada kalian perlindungan, Allah pun membela kalian bahkan Allah memberikan rezeki kepada kalian perkara-perkara yang thayyib agar kalian bersyukur.” (QS. Al-Anfal[8]: 26)

Kita diingatkan nikmat Allah yang besar ini. Maka -kata Ibnul Qayyim- diantara perkara yang menimbulkan syukur kepada Allah yaitu banyak mengingat kenikmatan. Dan nikmat aman nikmat yang sangat besar sekali.

Terkadang ada orang berkata, “Tapi pemimpin kita dzalim, banyak korupsi, nggak aman negara ini.” Kita katakan, “Ya Akhi, mana yang lebih besar mudharatnya, kita memberontak kepada pemimpin malah menimbulkan kekacauan dimana-mana akhirnya tidak aman sama sekali, atau kita sabar sambil kita mendoakan mereka?”

Maka dari itu ingat bahwa nikmat iman itu sesuatu yang luar biasa. Demikian pula bahwa seluruh manusia meminta kepada Allah keamanan. Bahkan para Nabi saja minta kepada. Ini dia Nabi Yusuf berkata kepada kedua orang tuanya:

فَلَمَّا دَخَلُوا عَلَى يُوسُفَ آوَى إِلَيْهِ أَبَوَيْهِ وَقَالَ ادْخُلُوا مِصْرَ إِن شَاءَ اللَّهُ أَمِينٌ (٩٩)

Ketika keluarga Nabi Yusuf, ayah ibunya, kakak dan adik-adiknya masuk semuanya ke kota Mesir, maka Nabi Yusuf pun kemudian menyambut mereka dan berkatalah, “Silakan masuk kota Mesir insyaAllah kalian aman.” (QS. Yusuf[12]: 99)

Allah pun berfirman menyebutkan tentang Nabi Musa yang ketakutan saat dikejar oleh Firaun, beliau ketakutan dan pergi ke Madyan. Kemudian Nabi Musa pun diberi ketenangan:

وَلَا تَخَفْ ۚ إِنَّكَ مِنَ الْآمِنِينَ

“Kamu jangan takut, kamu termasuk orang-orang yang aman.” (QS. Al-Qashash[28]: 31)

Nabi Musa ketika disuruh pergi untuk mendakwahi Firaun, Nabi Musa khawatir lalu Allah pun juga mengatakan, “Jangan takut, engkau termasuk orang-orang yang aman.”

3. Ibadah tidak bisa kita lakukan dengan khusyu' tanpa ketenangan

Ibadah tidak bisa kita lakukan dengan enak, dengan damai, dengan khusyu', dengan tenang, kecuali dengan adanya keamanan. Kalau kita beribadah dalam keadaan tidak aman, kira-kira tenang *nggak* ibadah kita? Kita shalat takut ditembak, kita shalat motor kita takut dicuri orang, misalnya banyak *curanmor* (pencurian sepeda motor), pulang dari masjid motornya hilang. Bagaimana ternyata banyak pembunuh?

Allah Ta'ala berfirman dalam surat Al-Baqarah:

حَافِظُوا عَلَى الصَّلَوَاتِ وَالصَّلَاةِ الْوُسْطَىٰ وَقُومُوا لِلَّهِ قَانِتِينَ (٢٣٨) فَإِنْ خِفْتُمْ فَرَجَالًا أَوْ رُكْبَانًا فَإِذَا أَمِنْتُمْ فَأَذْكُرُوا اللَّهَ كَمَا عَلَّمَكُم مَّا لَمْ تَكُونُوا تَعْلَمُونَ (٢٣٩)

“Jagalah oleh kalian shalat 5 waktu terutama shalat ashar. Dan berdirilah kepada Allah dengan khusyu'. Dan jika kalian merasa ketakutan silakan shalat dalam keadaan berjalan ataupun berkendara. Dan Apabila kalian telah aman maka berdzikirlah kepada Allah sesuai dengan yang Allah ajarkan kepada kalian.” (QS. Al-Baqarah[2]: 239)

Pada ayat ini Allah mengatakan kalau keadaannya takut silakan shalatnya terserah sambil berlari/sambil berjalan/ sambil naik kendaraan, tapi kalau kalian

sudah aman lakukan shalat sesuai dengan yang diajarkan oleh Allah Subhanahu wa Ta'ala. Artinya kalau aman ibadah pun juga enak. Kita bisa melakukan shalat sesuai dengan syarat-syaratnya. Tapi kalau tidak aman kita tidak bisa melakukan shalat sesuai dengan syaratnya.

Disaat aman dakwah pun akan semakin mudah untuk menyebar. Lihat bagaimana ketika Nabi Musa berdakwah di bawah Tirani Firaun, susah, sulit sekali, tidak aman. Tapi ketika Allah selamatkan Nabi Musa dan kaumnya dan Allah tenggelamkan Firaun dan tentaranya dalam laut merah, aman. Akhirnya banyak manusia yang masuk ke dalam agama Nabi Musa 'Alaihih Shalatu was Salam. Makanya keamanan itu adalah nikmat yang sangat besar sekali.

BAB III

PEMBAHASAN

3.1 Algoritma RSA dan *Beaufort Cipher*

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

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

3.1.1 Algoritma *Beaufort Cipher*

Beaufort Cipher adalah cipher substitusi *polyalphabetic* yang mirip dengan *Vigenère Cipher*. *Beaufort cipher* pada awalnya diusulkan oleh Giovanni Sestri pada tahun 1710 dan kemudian diberikan nama oleh Sir Francis Beaufort. Algoritma *Beaufort Cipher* menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut bisa lebih pendek ataupun sama dengan panjang *plaintext*. Jika panjang kunci kurang dari panjang *plaintext*, maka kunci tersebut akan diulang secara periodik hingga kunci tersebut sama dengan *plaintext*. Rumus substitusi *Beaufort Cipher*.

$$f_i(a) = (k_i - a) \bmod n$$

Rumus dekripsi *Beaufort Cipher*

$$f_i^{-1}(c) = (k_i - c) \bmod n$$

Dimana :

f_i = nilai desimal karakter ke $-i$

c = nilai desimal karakter *chipertext*

a = nilai decimal karakter *plaintext*

k_i = nilai decimal karakter kunci ke $-i$

n = jumlah huruf

3.1.2 Algoritma RSA

Algoritma RSA merupakan algoritma asimetris yang menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya. 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 $d \equiv e^{-1} \text{ mod } \Phi(n)$, dan $d < \Phi(n)$, sehingga

$$ed \equiv e \cdot e^{-1} \pmod{\Phi(n)} \quad (\text{Teorema 2.6})$$

$$ed \equiv 1 \pmod{\phi(n)} \quad (\text{Definisi Identitas})$$

$$\phi(n) | ed - 1 \quad (\text{Definisi 2.5})$$

$$ed - 1 = \phi(n) \cdot t \quad (\text{Definisi 2.1})$$

$$ed = \phi(n) \cdot t + 1 \quad (\text{kedua ruas ditambah 1})$$

$$d = \frac{\phi(n) \cdot t + 1}{e} \quad (\text{kedua ruas dibagi dengan } e)$$

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

$$c = k^e \pmod{n}$$

Rumus dekripsi RSA

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

Keterangan:

e = Kunci umum.

d = Kunci rahasia.

c = *Cipherkey*.

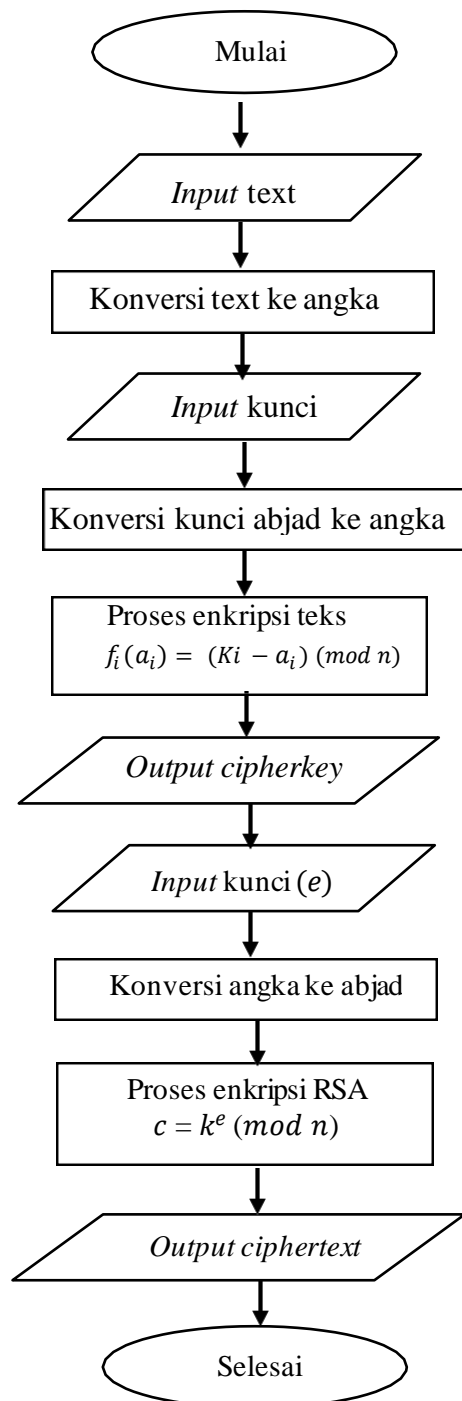
N = nilai $(p + 1)(q - 1)$

k = *Plainkey*.

3.2 Proses Algoritma RSA dan *Beaufart Cipher* pada Alamat Laman Pemulihan Kata Sandi

3.2.1 Enkripsi Algoritma RSA dan *Beaufart Cipher*

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



Gambar 3. 1 Flowchart Enkripsi Algoritma Hybrid

Setelah 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}
p	e	m	u	l	i	h	a	n	a	k	u	n	a	q
15	4	12	20	11	9	7	0	13	0	10	20	13	0	16

NB: huruf **a** dan **q** merupakan kode identik akun

3. Kunci atau *key* (K_i):

K_1	K_2	K_3	K_4	K_5
r	i	y	a	n
17	9	24	0	13

4. Proses Enkripsi 1 (Beaufart Chiper):

$$f_i(C) = (K_i - P_i) \bmod n$$

$$f_1(C) = (K_1 - P_1) \bmod n = (17 - 15) \bmod 26 = 2$$

$$f_2(C) = (K_2 - P_2) \bmod n = (9 - 4) \bmod 26 = 5$$

$$f_3(C) = (K_3 - P_3) \bmod n = (24 - 12) \bmod 26 = 12$$

$$f_4(C) = (K_4 - P_4) \bmod n = (0 - 20) \bmod 26 = -20 + 26 = 6$$

$$f_5(C) = (K_5 - P_5) \bmod n = (13 - 11) \bmod 26 = 2$$

$$f_6(C) = (K_6 - P_6) \bmod n = (17 - 9) \bmod 26 = 8$$

$$f_7(C) = (K_7 - P_7) \bmod n = (9 - 7) \bmod 26 = 2$$

$$f_8(C) = (K_8 - P_8) \bmod n = (24 - 0) \bmod 26 = 24$$

$$f_9(C) = (K_9 - P_9) \bmod n = (0 - 13) \bmod 26 = -13 + 26 = 13$$

$$f_{10}(C) = (K_{10} - P_{10}) \bmod n = (13 - 0) \bmod 26 = 13$$

$$f_{11}(C) = (K_{11} - P_{11}) \bmod n = (17 - 10) \bmod 26 = 7$$

$$f_{12}(C) = (K_{12} - P_{12}) \bmod n = (9 - 20) \bmod 26 = -11 + 26 = 15$$

$$f_{13}(C) = (K_{13} - P_{13}) \bmod n = (24 - 13) \bmod 26 = 11$$

$$f_{14}(C) = (K_{14} - P_{14}) \bmod n = (0 - 0) \bmod 26 = 0$$

$$f_{15}(C) = (K_{15} - P_{15}) \bmod n = (13 - 16) \bmod 26 = -3 + 26 = 23$$

5. Hasil Enkripsi 1 (Beaufart Chiper)

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
c	f	m	g	c	I	c	y	z	n	h	p	l	a	x
2	5	12	6	2	8	2	24	26	13	7	15	11	0	23

6. Proses Enkripsi Kunci Menggunakan algoritma Hybrid RSA

- Ambil sebarang bilangan prima $p = 3$ dan $q = 5$
- Hitung $n = 3 \times 5 = 15$
- Hitung $\Phi(n) = (3 - 1)(5 - 1) = 8$
- Pilih bilangan bulat $e = 7$ dimana $\gcd(8, 7) = 1$; $1 < 7 < 8$
- Proses Enkripsi

$$C_i = k_i^e \pmod{n}$$

$$C_1 = k_1^7 \pmod{15} = 2^7 \pmod{15} = 8$$

$$C_2 = k_2^7 \pmod{15} = 5^7 \pmod{15} = 5$$

$$C_3 = k_3^7 \pmod{15} = 12^7 \pmod{15} = 3$$

$$C_4 = k_4^7 \pmod{15} = 6^7 \pmod{15} = 6$$

$$C_5 = k_5^7 \pmod{15} = 2^7 \pmod{15} = 8$$

$$C_6 = k_6^7 \pmod{15} = 8^7 \pmod{15} = 2$$

$$C_7 = k_7^7 \pmod{15} = 2^7 \pmod{15} = 8$$

$$C_8 = k_8^7 \pmod{15} = 24^7 \pmod{15} = 9$$

$$C_9 = k_9^7 \pmod{15} = 26^7 \pmod{15} = 11$$

$$C_{10} = k_{10}^7 \pmod{15} = 13^7 \pmod{15} = 7$$

$$C_{11} = k_{11}^7 \pmod{15} = 7^7 \pmod{15} = 13$$

$$C_{12} = k_{12}^7 \pmod{15} = 15^7 \pmod{15} = 0$$

$$C_{13} = k_{13}^7 \pmod{15} = 11^7 \pmod{15} = 11$$

$$C_{14} = k_{14}^7 \pmod{15} = 0^7 \pmod{15} = 0$$

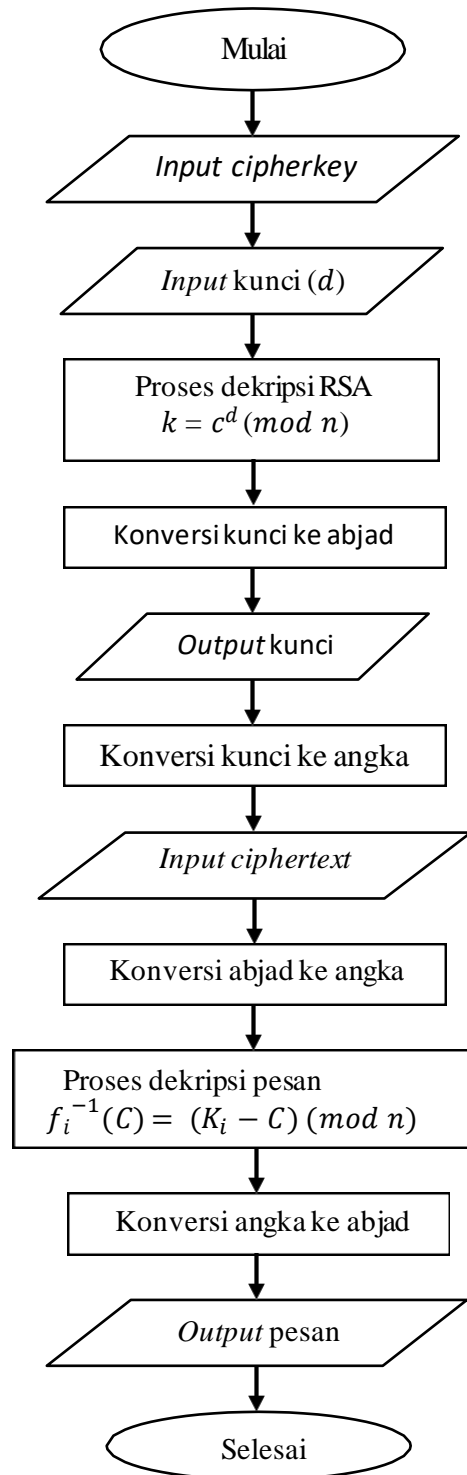
$$C_{15} = k_{15}^7 \pmod{15} = 23^7 \pmod{15} = 2$$

7. Hasil Enkripsi Hybrid RSA

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}
i	f	d	g	i	c	i	j	l	h	h	a	l	a	c
8	5	3	6	8	2	8	9	11	7	13	0	11	0	2

3.2.2 Deskripsi Algoritma RSA dan *Beaufort Cipher*

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



Gambar 3. 2 Flowchart Dekripsi Algoritma

Setelah membuat *flowchart* dekripsi algoritma *hybrid* RSA dan *Beaufort Cipher* pada suatu pesan, kemudian melakukan proses dekripsi pada kunci dengan menggunakan algoritma RSA dengan langkah-langkah sebagai berikut:

1. Ambil sebarang bilangan prima $p = 3$ dan $q = 5$
2. Hitung $n = 3 \times 5 = 15$
3. Hitung $\Phi(n) = (3 - 1)(5 - 1) = 8$
4. Pilih bilangan bulat $e = 7$ dimana $\gcd(8, 7) = 1$; $1 < 7 < 8$
5. Hitung d yaitu:

$$d \equiv 7^{-1} \pmod{\Phi(n)}, \text{dimana } d < \Phi(n)$$

$$7d \equiv 1 \pmod{8}$$

$$7d - 1 = 8t$$

$$7d = 8t + 1$$

$$d = \frac{8t + 1}{7}$$

Dengan mencoba nilai dari $t \in \mathbb{N}$ ditemukan t yang memenuhi adalah 6, sehingga:

$$d = \frac{8(6) + 1}{7}$$

$$d = 7 \quad \dots\dots\dots(d < 8)$$

6. Tabel Chiper

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
I	f	d	g	i	c	i	J	l	h	h	a	l	a	c
8	5	3	6	8	2	8	9	11	7	13	0	11	0	2

7. Proses Dekripsi RSA:

$$P_i = C_i^d \pmod{n}$$

$$P_1 = C_1^7 \pmod{15} = 8^7 \pmod{15} = 2$$

$$P_2 = C_2^7 \pmod{15} = 5^7 \pmod{15} = 5$$

$$P_3 = C_3^7 \pmod{15} = 3^7 \pmod{15} = 12$$

$$P_4 = C_4^7 \pmod{15} = 6^7 \pmod{15} = 6$$

$$P_5 = C_5^7 \pmod{15} = 8^7 \pmod{15} = 2$$

$$P_6 = C_6^7 \pmod{15} = 2^7 \pmod{15} = 8$$

$$P_7 = C_7^7 \bmod 15 = 8^7 \bmod 15 = 2$$

$$P_8 = C_8^7 \bmod 15 = 9^7 \bmod 15 = 24$$

$$P_9 = C_9^7 \bmod 15 = 11^7 \bmod 15 = 26$$

$$P_{10} = C_{10}^7 \bmod 15 = 7^7 \bmod 15 = 13$$

$$P_{11} = C_{11}^7 \bmod 15 = 13^7 \bmod 15 = 7$$

$$P_{12} = C_{12}^7 \bmod 15 = 0^7 \bmod 15 = 15$$

$$P_{13} = C_{13}^7 \bmod 15 = 11^7 \bmod 15 = 11$$

$$P_{14} = C_{14}^7 \bmod 15 = 0^7 \bmod 15 = 0$$

$$P_{15} = C_{15}^7 \bmod 15 = 2^7 \bmod 15 = 23$$

8. Hasil Deskripsi RSA

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
c	f	m	g	c	I	c	y	z	n	h	p	l	a	x
2	5	12	6	2	8	2	24	26	13	7	15	11	0	23

9. Plainkey Menggunakan Kunci *Beaufort Cipher*

Setelah kunci terdekripsi, kemudian pesan dapat di dekripsi dengan menggunakan algoritma *Beaufort Cipher*, berikut langkah-langkah proses dekripsi algoritma *Beaufort 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. Kunci atau *key* (K):

K ₁	K ₂	K ₃	K ₄	K ₅
r	i	y	A	n
17	9	24	0	13

3. Proses Deskripsi Beaufart Cipher

$$f_i^{-1}(C_i) = (K_i - C_i) \pmod{n}$$

$$f_1^{-1}(C_1) = (K_1 - C_1) \pmod{26} = (17 - 2) \pmod{26} = 15$$

$$f_2^{-1}(C_2) = (K_2 - C_2) \pmod{26} = (9 - 5) \pmod{26} = 4$$

$$f_3^{-1}(C_3) = (K_3 - C_3) \pmod{26} = (24 - 12) \pmod{26} = 12$$

$$f_4^{-1}(C_4) = (K_4 - C_4) \pmod{26} = (0 - 6) \pmod{26} = 20$$

$$f_5^{-1}(C_5) = (K_5 - C_5) \pmod{26} = (13 - 2) \pmod{26} = 11$$

$$f_6^{-1}(C_6) = (K_6 - C_6) \pmod{26} = (17 - 8) \pmod{26} = 9$$

$$f_7^{-1}(C_7) = (K_7 - C_7) \pmod{26} = (9 - 2) \pmod{26} = 7$$

$$f_8^{-1}(C_8) = (K_8 - C_8) \pmod{26} = (24 - 24) \pmod{26} = 0$$

$$f_9^{-1}(C_9) = (K_9 - C_9) \pmod{26} = (0 - 26) \pmod{26} = 13$$

$$f_{10}^{-1}(C_{10}) = (K_{10} - C_{10}) \pmod{26} = (13 - 13) \pmod{26} = 0$$

$$f_{11}^{-1}(C_{11}) = (K_{11} - C_{11}) \pmod{26} = (17 - 7) \pmod{26} = 10$$

$$f_{12}^{-1}(C_{12}) = (K_{12} - C_{12}) \pmod{26} = (9 - 15) \pmod{26} = 20$$

$$f_{13}^{-1}(C_{13}) = (K_{13} - C_{13}) \pmod{n} = (24 - 11) \pmod{26} = 13$$

$$f_{14}^{-1}(C_{14}) = (K_{14} - C_{14}) \pmod{n} = (0 - 0) \pmod{26} = 0$$

$$f_{15}^{-1}(C_{15}) = (K_{15} - C_{15}) \pmod{n} = (13 - 23) \pmod{26} = 16$$

5. Hasil dekripsi Beaufort Cipher:

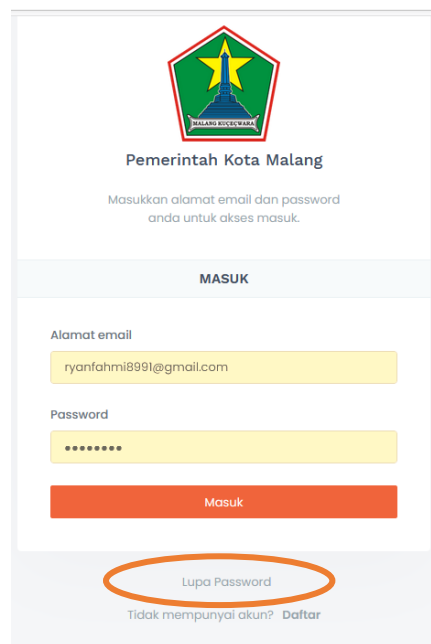
P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}
15	4	12	20	11	9	7	0	13	0	10	20	13	0	16
p	e	m	u	l	i	h	a	n	a	k	u	n	a	q

3.3 Pengimplementasian Algoritma RSA dan Beaufort Cipher Pada Alamat Laman Pemulihan Kata Sandi

Objek yang menjadi fokus penelitian dalam hal ini adalah akun user (pengguna) dari lembaga kemasyarakatan Kota Malang. Ketika user lupa akan kata sandi mereka, mereka hanya perlu untuk menekan fitur tombol lupa password. Tautan pemulihan akan dikirim melalui email, kemudian alamat laman proses pemulihan kata sandi akan dienkripsi. Setelah dienkripsi akan dilanjutkan dengan proses dekripsi yang dilakukan oleh sistem agar proses pemulihan kata sandi dapat bekerja. Berikut gambaran beserta alurnya.


Ketika pengguna (*user*) lupa password, pengguna (*user*) dapat mengikuti langkah-langkah sesuai penjelasan dibawah ini. Langkah-langkah tersebut adalah:

- a. Klik tulisan '*lupa password*' yang berada pada bagian bawah kotak untuk login.



Gambar 3. 3 Laman Login

- b. Setelah itu tuliskan nama email yang sesuai dengan email yang dimiliki oleh si pengguna (*user*). Jika email sesuai, maka tautan '*Ubah Password*' akan terkirim langsung ke email pengguna. Jika email yang dimasukkan tidak sesuai maka akan ada tulisan peringatan bahwa email yang dimasukkan tidak terdaftar.



Pemerintah Kota Malang

Masukkan Alamat Email Anda dan kami akan mengirimkan instruksi untuk merubah password.

PULIHKAN PASSWORD

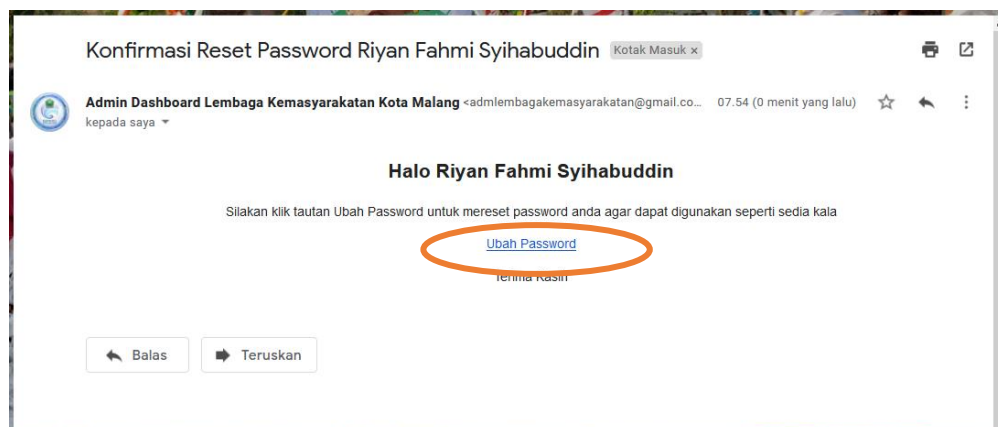
Alamat Email

ryanfahmi8991@gmail.com

Ganti Password

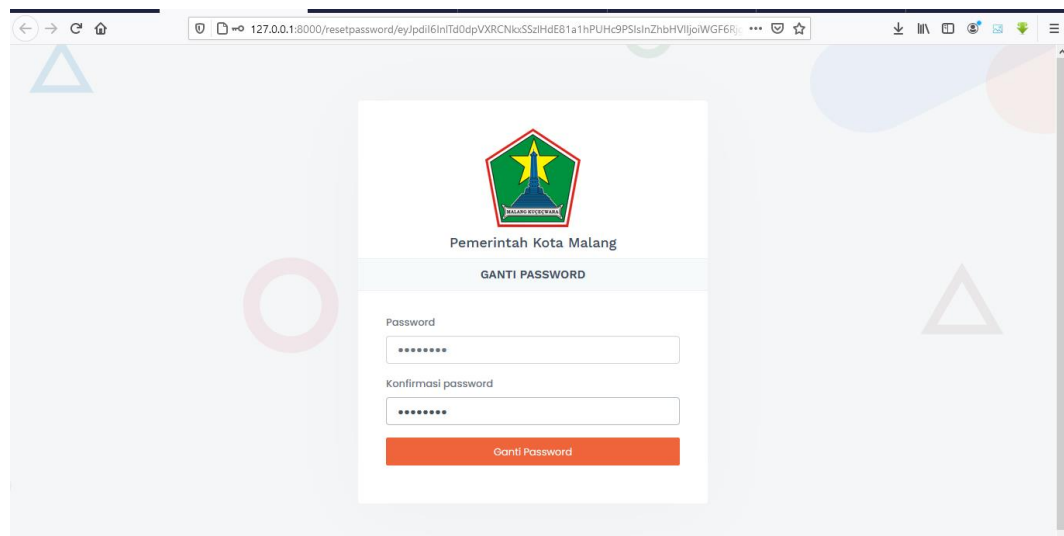
Gambar 3. 4 Laman Lupa Password

- c. Silakan pengguna untuk mengecek tautan ubah password yang telah terkirim ke email pengguna. Kemudian klik tautan ‘*Ubah Password*’



Gambar 3. 5 Pesan dari Email Admin

d. Masukkan password terbaru dua kali. Kemudian klik tombol ‘Ganti Password’.

The image shows a web browser window displaying a password reset interface. At the top, the browser's address bar shows a long URL. The page features the official logo of the Government of Malang, which is a green pentagon with a yellow star and the text 'MALANG KOTA SUDHANA' below it. Below the logo, the text 'Pemerintah Kota Malang' is displayed. The main heading of the form is 'GANTI PASSWORD'. There are two input fields: the first is labeled 'Password' and the second is labeled 'Konfirmasi password'. Both fields contain a series of dots to mask the input. At the bottom of the form is an orange button labeled 'Ganti Password'. The background of the page is light gray with faint geometric shapes like triangles and circles.

Gambar 3. 6 Laman Pemulihan Kata Sandi

e. Halaman akan langsung kembali ke menu login. Pengguna dapat masuk ke halaman Dashboard dengan menggunakan *password* terbaru.

Berdasarkan penjelasan diatas dapat kita ketahui bahwa laman pemulihan kata sandi telah terenskripsi, alamat laman tersebut nantinya akan di deskripsikan oleh sistem untuk menjalankan proses penggantian kata sandi.

DAFTAR PUSTAKA

- Ariyus. 2006. Kriptografi dan Pemanfaatannya. Surabaya: PT Cendikia Pratama.
- ArRaya, Dimas. 2015. *Dasar-Dasar Kriptografi* . Bandung: Gamal Press.
- Badan Kajian Keislaman. 2018. *Konsep keamanan dalam dunia islam*, <https://muslimhijrah.or.id/subject/16/kajiankeamanan.html>, diakses pada 20 November 2020 pukul 10.27.
- Hernanto, Budi. 2018. *Implementasi Algoritma RSA (Rivest, Shamir, Adleman) pada enkripsi pesan SMS* dalam Jurnal Teknik Informatika Volume 14 Nomor 1 (hlm. 27–34) , Lampung : Universitas Lampung.
- Hilman. (2016). *Perbedaan Aplikasi Berbasis Web, Aplikasi Berbasis Desktop, dan Aplikasi Berbasis Mobile*. Bandung: Ganesha Pratama.
- Khumaidi, Ahmad. 2018. *Pengimplementasian Algoritma Hybrid RSA (Rivest, Shamir, Adleman) dan Vigenere Cipher pada pesan teks*. Skripsi. Prodi Matematika. UIN Maulana malik Ibrahim. Malang.
- Munir, Rinaldi. 2016. *Matematika Diskrit*. Bandung: Program Studi Teknik Informatika ITB.
- Warma, I Putu. 2015. *Implementasi Metode Beaufort Cipher Dan Blowfish Cipher untuk Enkripsi SMS Pada Telepon Seluler Berbasis Android* dalam Jurnal Ilmiah Teknologi dan Rekayasa Volume 24 No. 2 (hlm 114 - 130). Depok: Fakultas Teknologi .Sekolah Tinggi Ilmu Komunikasi.