PERANCANGAN APLIKASI MEMO MENGGUNAKAN ALGORITMA KRIPTOGRAFI CAESAR CIPHER DAN RSA BERBASIS ANDROID

Muhammad Aziz Fatchur Rachman [1)]

[1)] Magister Teknik Informatika, Universitas Amikom Yogyakarta
Jl. Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta Indonesia 55283
Email : ziva.mafra@gmail.com

Abstrak. *Di era serba digital saat ini, perkembangan teknologi memiliki pengaruh yang besar terhadap aktifitas yang kita lakukan sehari-hari, tak terkecuali menulis memo ataupun catatan singkat. Penggunaan alat tulis konvensional pun ikut beralih ke digital dengan menggunakan Smartphone. Namun kebanyakan dari kita menulis memo menggunakan smartphone hanya sebatas menulis dan menyimpannya tanpa ada pengamanan terhadap data yang kita simpan. Ini mengakibatkan peluang tercurinya informasi yang disimpan semakin besar. Maka dari itu faktor keamanan sangat dibutuhkan untuk menjaga kerahasiaan data yang kita simpan. Dengan algoritma kriptografi, kita dapat mengamankan data dengan proses enkripsi dimana proses ini mengubah isi data secara terstruktur dengan metode tertentu sehingga data tersebut tidak dapat diketahui isinya tanpa suatu kunci tertentu untuk merekonstruksi kembali isi data kebentuk semula sebelum dilakukan proses enkripsi..Melihat hal ini mendorong penulis untuk merancang aplikasi Memo dengan kriptografi menggunakan algoritma Caesar Cipher dan RSA berbasis android.*

Kata kunci : *Caesar Cipher, Memo, RSA* .

1. Pendahuluan

1.1. Latar Belakang

Di era serba digital ini, perkembangan teknologi informasi berpengaruh besar terhadap aktifitas yang dilakukan manusia. Beberapa aktivitas kita salah satunya yaitu menulis memo atau catatan singkat, tidak lagi membutuhkan buku dan pena. Kita tidak lagi kerepotan untuk menulis sesuatu baik itu berupa ide, informasi penting dan lain sebagainya pada saat santai ataupun terdesak. Dengan menggunakan *smartphone* kita dapat menulis dan menyimpan catatan kita dimanapun dan kapanpun.
Saat ini banyak orang yang menulis catatannya di *smartphone,* akan tetapi isi dari catatan yang ditulis hanya sebatas tersimpan tanpa suatu pengamanan. Jadi, orang lain dapat dengan mudah membaca isi dari catatan yang telah tersimpan tanpa sepengetahuan kita. Dengan kriptografi yang merupakan ilmu dan seni penyandian data, kita dapat menjaga keamanan informasi yang kita tulis dengan proses enkripsi dan dekripsi data. Proses enkripsi ini adalah suatu proses mengubah karakter tulisan secara acak dengan menggunakan metode tertentu sehingga tulisan tidak dapat dimengerti tanpa kunci tertentu untuk mengembalikan susunan tulisan tersebut. Hal ini mendorong penulis untuk mendesain aplikasi *Memo* berbasis android dengan menggunakan algoritma kriptografi sehingga kerahasiaan isi *Memo* yang ditulis dapat terjaga.[1]

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana merancang aplikasi *Memo* menggunakan algoritma kriptografi Caesar Cipher dan RSA berbasis android?

1.3 Tujuan

Tujuan dari penelitian ini dimaksudkan untuk membuat aplikasi *Memo* berbasis android dengan menggunakan algoritma kriptografi Caesar Cipher dan RSA dalam proses enkripsi dan deskripsi untuk menjaga kerahasiaan data yang tersimpan.

1.4 Metodologi

Penelitian ini dihasilkan dengan mengelola beberapa metode dalam pengumpulan informasi. Adapun metode yang dipergunakan adalah sebagai berikut :

1. Metode Pengumpulan Data dilakukan dengan cara membaca referensi dari berbagai sumber dan buku yang diperoleh dari perpustakaan dan koleksi pribadi.
2. Motode Perancangan Sistem yang digunakan yaitu *(Unified Modelling Language) UML*.
3. Ujicoba Sistem dilakukan dengan cara pengujian di beberapa *mobile device* android

1.5 Tinjauan Pustaka

Upik (2016), dalam papernya yang membahas tentang implementasi 4 algoritma kriptografi klasik untuk proses enkripsi dan deskripsi . Persamaan dengan penelitian yang penulis lakukan yaitu sama-sama aplikasi enkripsi berbasis android. Sedangkan perbedaannya yaitu implementasi yang penulis terapkan tidak pada aplikasi sederhana yang hanya melakukan proses enkripsi dan deskripsi pada textbox yang disediakan melainkan pada aplikasi *Memo*. Dan juga algoritma yang penulis gunakan yaitu algoritma Caesar Cipher dan RSA.[2]

Aedhoh (2016), dalam papernya yang membahas tentang implementasi algoritma kriptografi RC6 untuk mengenkripsi dan mendeskripsi data yang tersimpan di diary agar tidak dapat dibaca dan disalahgunakan oleh orang lain. Persamaan dengan penelitian yang penulis lakukan yaitu sama-sama aplikasi enkripsi berbasis android. Sedangkan perbedaannya yaitu implementasi yang penulis terapkan tidak pada aplikasi *Diary*, melainkan pada aplikasi *Memo*. Dan juga algoritma yang penulis gunakan yaitu kombinasi algoritma kriptografi klasik dan modern, Caesar Cipher dan RSA. [3]

Rionald (2015), dalam papernya yang membahas tentang implementasi algoritma kriptografi RC6 untuk proses enkripsi dan deskripsi dalam pengiriman SMS. Persamaan dengan penelitian yang penulis lakukan yaitu sama-sama aplikasi enkripsi berbasis android. Sedangkan perbedaannya yaitu implementasi yang penulis terapkan tidak pada aplikasi SMS melainkan pada aplikasi *Memo*. Dan juga algoritma yang penulis gunakan yaitu kombinasi algoritma kriptografi klasik dan modern, Caesar Cipher dan RSA. [4]

1.5.1 Memo

Memo ialah pesan atau catatan yang ditulis secara singkat, padat dan jelas serta mudah dipahami. Memo tebagi menjadi 2 yaitu memo resmi dan memo tidak resmi (bersifat pribadi).

1.5.2 Caesar Cipher

Algoritma caesar cipher merupakan teknik penyandian pertama di dunia dengan menggunakan teknik substitusi. Algoritma klasik ini juga dikenal dengan algoritma ROT3 Pada awalnya teknik ini digunakan oleh Julius Caesar untuk berkomunikasi dengan tentaranya di garis depan. Agar pesannya aman, Caesar melindungi data yang dikirim dengan melakukan pergeseran pada setiap huruf dalam pesannya atau pun mengubah huruh menjadi angka, contohnya: [5]

HA : a b c d e f g h i j k l m n o p q r s t u v w x y z
S : d e f g h i j k l m n o p q r s t u v w x y z a b c
Atau
HA : a b c d e f g h i j k l m n o p q r s t u v w x y z
S : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
HA = Huruf Asli
S = Sandi

Penerapannya :
P : KRIPTOGRAFI
C : ???

Proses penyandian Caesar Cipher dengan melakukan pergeseran 3 huruf seperti pada HA dan HS, maka teks cipher yang didapat adalah :

C : NULSWRJUDIL

Pada perkembangannya algoritma caesar memberikan suatu gagasan baru untuk menggunakan kunci lain yang disebut poly-alphabetic, dimana kuncinya bisa jadi nama, alamat atau apa saja yang diinginkan oleh pengirim pesan. Sebagai contoh:

HA : a b c d e f g h i j k l m n o p q r s t u v w x y z
Kunci : merapi. Maka,
HS : m e r a p i b c d f g h j k l n o q s t u v w x y z

1.5.3 RSA

Algoritma RSA ini merupakan salah satu algoritma kriptografi modern asimetris yang populer. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar sehingga ini menjadi alasan kenapa RSA dianggap algoritma yang aman. Algoritma RSA dibuat pada tahun 1976 oleh 3 orang peneliti yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman dari MIT (Massachussets Institute of Technology).

RSA mengekspresikan teks asli yang dienkripsi dengan blok-blok yang mana setiap blok memiliki nilai bilangan biner yang diberi simbol "n", blok teks asli "M" dan blok teks kode "C". Dalam melakukan proses enkripsi data atau pesan "M", pesan dibagi ke dalam blok-blok numerik yang lebih kecil daripada "n" (data biner dengan pangkat terbesar). Jika bilangan prima yang panjangnya 200 digit, dapat ditambah beberapa bit 0 dikiri bilangan untuk menjaga agar pesan tetap kurang dari nilai "n".

Besaran yang digunakan pada algoritma RSA:

1. p dan q bilangan prima (rahasia)
2. r = p * q (tidak rahasia)
3. $\phi(r) = (p - 1)(q - 1)$ (rahasia)
4. *PK* (kunci enkripsi) (tidak rahasia)
5. *SK* (kunci dekripsi) (rahasia)
6. *X* (teks asli) (rahasia)
7. *Y* (teks kode) (tidak rahasia)

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa :

$$a^{\phi(r)} \equiv 1 \pmod r \quad \text{.....(1)}$$

yang dalam hal ini:

1. a harus relatif prima terhadap r.
2. $\phi(r) = r(1 - 1/p1)(1 - 1/p2) \ldots (1 - 1/pn)$, yang dalam hal ini p1, p2, ..., pn adalah faktor prima dari r.
   $\phi(r)$ adalah fungsi yang menentukan beberapa banyak bilangan 1, 2, 3, ..., r yang relatif prima terhadap r.

Berdasarkan sifat $a^m \equiv b^m \pmod r$ untuk m bilangan bulat ≥ 1 maka persamaan (1) dapat ditulis menjadi:

$$a^{(m^\phi)(r)} \equiv 1^m \pmod r$$

atau

$$a^{(m^\phi)(r)} \equiv 1 \pmod r \quad \text{.....(2)}$$

bila a diganti dengan *X* maka persamaan (2) menjadi:

$$X^{(m^\phi)(r)} \equiv 1 \pmod r \quad \text{.....(3)}$$

Berdasarkan sifat $ac \equiv bc \pmod r$ maka bila persamaan (3) dikali dengan *X* menjadi:

$$X^{(m^\phi)(r)+1} \equiv X \pmod r \quad \text{.....(4)}$$

Yang dalam hal ini *X* relatif prima terhadap r.

Misalkan *SK* dan *PK* dipilih sedemikian rupa sehingga

$$SK * PK \equiv 1 \pmod{\phi(r)} \quad \text{.....(5)}$$

Atau

$$SK * PK \equiv m\phi(r) + 1 \quad \text{.....(6)}$$

Sulihkan (6) ke dalam persamaan (4) menjadi:

$$X^{SK * PK} \equiv X \pmod r \quad \text{.....(7)}$$

Persamaan (7) dapat ditulis kembali menjadi:

$$(X^{SK})^{PK} \equiv X \pmod r \quad \text{.....(8)}$$

Yang artinya perpangkatan *X* dengan *PK* diikuti dengan perpangkatan dengan *SK* menghasilkan *X* semula.

Berdasarkan persamaan (8) maka enkripsi dan dekripsi dirumuskan sebagai berikut:

$$E_{PK}(X) = Y \equiv X^{PK} \bmod r \quad \text{.....(8)}$$
$$D_{SK}(Y) = X \equiv Y^{SK} \bmod r \quad \text{.....(9)}$$

Karena *SK* * *PK* = *PK* * *SK*, maka enkripsi diikuti dengan dekripsi ekuivalen dengan dekripsi diikuti enkripsi:

$$E_{SK}(D_{SK}(X)) = D_{SK}(E_{PK}(X)) \equiv Y^{SK} \bmod r \quad ....(10)$$

Oleh karena $X^{PK} \bmod r \equiv (X + mr)^{PK} \bmod r$ untuk sembarang bilangan bulat m, maka tiap teks asli *X*, *X*+r, *X*+2r, . . . menghasilkan teks kode yang sama. Dengan kata lain, transformasinya adalah dari banyak ke satu. Agar transformasinya ke satu maka *X* harus dibatasi dalam himpunan {0, 1, 2, . ., r-1} sehingga enkripsi dan dekripsi tetap benar seperti pada persamaan (8) dan (9).[6]

2. Pembahasan

2.1. Analisis Kebutuhan Fungsional

Kebutuhan fungsional merupakan jenis kebutuhan yang menjelaskan fungsi-fungsi yang nantinya dapat dilakukan sistem. Adapun kebutuhan fungsional aplikasi *Memo* Kriptografi Caesar Cipher dan RSA ini adalah sebagai berikut :

1. Sistem dapat melayani Registrasi akun.
2. Sistem dapat melayani *Login User*.
3. Sistem dapat membuat *Memo* berupa *text*.
4. Sistem dapat melakukan enkripsi *text*.
5. Sistem dapat melakukan dekripsi *text*.
6. Sistem dapat menampilkan daftar *Memo* yang tersimpan.
7. Sistem dapat membaca *Memo* yang ditampilkan.
8. Sistem dapat melakukan *edit* dan *delete Memo*.

2.2 Analisis Kebutuhan Non-Fungsional

Kebutuhan Non Fungsional adalah jenis kebutuhan yang menjelaskan tentang kebutuhan diluar sistem seperti kebutuhan Operasional, *Performance*, Keamanan, Politik dan Budaya. Adapun kebutuhan Oprasional Aplikasi *Memo* Kriptografi Caesar Cipher dan RSA ini adalah sebagai berikut :

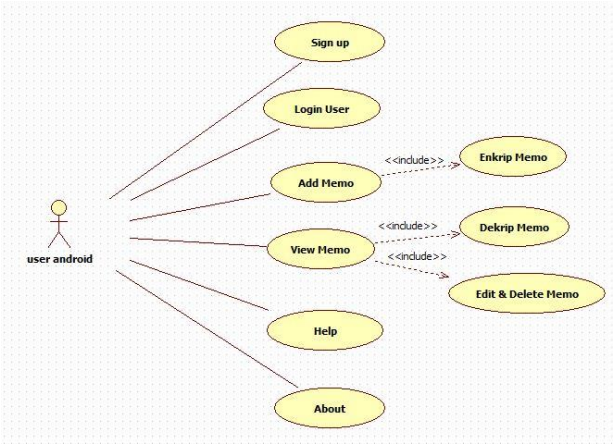
1. Kebutuhan Perangkat Keras
   Spesifikasi perangkat keras yang digunakan penulis dalam pembuatan Aplikasi *Memo* Kriptografi Caesar Cipher dan RSA ini adalah sebagai berikut :
   1. Processor Intel Core i5-5200U 2,2GHz.
   2. Memory (RAM) dengan Kapasitas 8GB.
   3. Harddisk dengan kapasitas 1TB.
   4. VGA Intel(R) HD Graphics 5500 2GB dan NVIDIA GeForce GT 940M 2GB.
2. Kebutuhan minimal device yang digunakan untuk menjalankan aplikasi adalah:
   1. *Smartphone* android atau *emulator* dengan versi minimal versi 5 (*Lolipop*).
   2. Memory (RAM) dengan Kapasitas 512MB.
3. Perangkat lunak yang digunakan dalam perancangan Aplikasi Memo Kriptografi Caesar Cipher dan RSA ini adalah sebagai berikut :
   1. Sistem operasi Windows 8.1 Entreprise 64Bit.
   2. Android Studio 1.5 64 bit.
   3. Android *Software Development Kit* (SDK).
   4. Memu Emulator

2.3 Perancangan UML

Use Case Diagram

Use case diagram merupakan metode berbasis teks yang menjelaskan apa yang akan dilakukan oleh sistem yang akan dibangun dan siapa yang berinteraksi dengan system dan menggambarkan serta mendokumentasikan proses yang kompleks. Adapun *Use case* Diagram Aplikasi *Memo* Kriptograsi Caesar Cipher dan RSA adalah sebagai berikut.

ISSN 2085-4218
ITN Malang, 3 Pebruari 2018



Gambar 1. *Use Case Diagram*

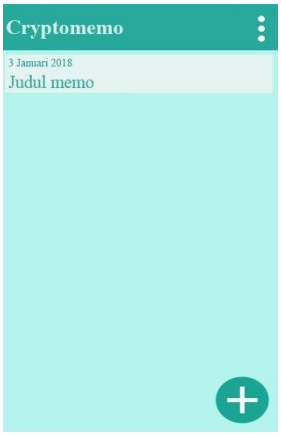
2.4 Tampilan Aplikasi

Berikut beberapa tampilan aplikasi memo yang dirancang.

Gambar 2. *Splash Screen*

Gambar 3. Registrasi

Gambar 4. *Login*



Gambar 5. Menu Utama

Gambar 6. *Menu Add Memo*

Gambar 7. *Menu View Memo*

2.5 Simulasi Proses Enkripsi dan Dekripsi Manual

Berikut contoh simulasi proses enkripsi dan dekripsi secara manual.

Text : MAKALAH
Key : KRIPTO
Ciphertext : ??

Proses enkripsi

a. Caesar Cipher

Huruf Asli : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Sandi : K R I P T O A B C D E F G H J L M N Q S U V W X Y Z
C1 : GKEKFKB

b. RSA

p : 7
q : 29
r : p * q : 203
ϕ(r) : (p - 1)(q - 1) : 168
PK : 11 (faktorisasi prima terbesar dari ϕ(r) kemudian naikkan 1 tingkat)
(SK * PK) mod ϕ(r) = 1, maka SK : 107
C1 : GKEKFKB » ASCII Desimal : 71 75 69 75 70 75 66
C2 : G » 71^{PK} mod r : 71^{11} mod 203 : 120
K » 75^{PK} mod r : 75^{11} mod 203 : 157
E » 69^{PK} mod r : 69^{11} mod 203 : 97
K » 75^{PK} mod r : 75^{11} mod 203 : 157
F » 70^{PK} mod r : 70^{11} mod 203 : 133
K » 75^{PK} mod r : 75^{11} mod 203 : 157
B » 66^{PK} mod r : 66^{11} mod 203 : 61

Hasil teks *Cipher* : 120 157 97 157 133 157 61

Proses dekripsi

a. RSA

p : 7
q : 29
r : p * q : 203
ϕ(r) : (p - 1)(q - 1) : 168
PK : 11 (faktorisasi prima terbesar dari ϕ(r) kemudian naikkan 1 tingkat)
(SK * PK) mod ϕ(r) = 1, maka SK : 107
Cipher : 120 157 97 157 133 157 61
D1 : G » 120^{SK} mod r : 120^{107} mod 203 : 71
K » 157^{SK} mod r : 157^{107} mod 203 : 75
E » 97^{SK} mod r : 97^{107} mod 203 : 69
K » 157^{SK} mod r : 157^{107} mod 203 : 75
F » 133^{SK} mod r : 133^{107} mod 203 : 70
K » 157^{SK} mod r : 157^{107} mod 203 : 75
B » 61^{SK} mod r : 61^{107} mod 203 : 66
D1 : 71 75 69 75 70 75 66

b. Caesar Cipher

D1 : 71 75 69 75 70 75 66 » konversikan ke huruf dari tabel ASCII desimal : G K E K F K B
Sandi : K R I P T O A B C D E F G H J L M N Q S U V W X Y Z
Huruf Asli : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D2 : M A K A L A H
Maka hasil *Plaintext*nya adalah : MAKALAH

3. Simpulan

Setelah melalui tahapan tahapan yang telah dijelaskan pada pembahasan sebelumnya makan dapat ditarik kesimpulan tentang Aplikasi *Cryptomemo* ini adalah:

1. Aplikasi *Cryptomemo* ini menggunakan algoritma kriptografi Caesar Cipher dan RSA. Aplikasi ini memiliki fitur pengamanan informasi ganda yaitu *Login Password* (dimana data login dilakukan proses enkripsi) dan Enkripsi isi *Memo* sehingga kerahasian data user dan data *Memo* lebih terjaga.
2. Aplikasi dapat berjalan dengan pada sistem operasi Android minimal versi 5 (*Lolipop*).
3. Setelah melakukan perhitungan secara namual, kombinasi algoritma dapat berjalan dengan baik.
4. Dengan memanfaatkan algoritma Caesar Cipher untuk proses memvariasikan keyword yang beragam, kelemahan algoritma RSA yang memiliki keyword hanya berupa angka dapat diatasi.
5. Kekuatan algoritma RSA yang terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima membuat keamanan data yang tersimpan menjadi aman (usaha untuk mencari faktor bilangan 200 digit membutuhkan wakti komputasi selama 4 milyar tahun dengan asumsi algoritma pemfaktoran adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 mili detik.
6. Penulis lebih menekankan pada proses enkripsi dan dekripsi data yang terjadi pada aplikasi guna mengamankan data yang tersimpan.

Daftar Pustaka

[1] D. Ariyus, Kriptografi : Keamanan Data dan Komunikasi, Yogyakarta: Penerbit Andi, 2006

[2] U. Paranita, “Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile,” dalam *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, Yogyakarta, 2016.

[3] A. S. Assaidi, “Perancangan Aplikasi Diary Menggunakan Algoritma Kriptografi RC6 Berbasis Android,” dalam *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, Yogyakarta, 2016.

[4] R. R. Mangundap, “ Aplikasi Secure Message Menggunakan Algoritma RC6 Berbasis Android,” *dalam e-Jurnal Spirit Pro Patria 2015*, Surabaya, 2015.

[5] D. Stiawan, Sistem Keamanan Komputer, Penerbit Elex Media Komputindo, 2005.

[6] D. Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Yogyakarta: Penerbit Andi, 2008.

Biodata Penulis

Muhammad Aziz Fatchur Rachman, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika Universitas AMIKOM Yogyakarta, lulus tahun 2017..Saat ini sedang menempuh pendidikan paska sarjana di Universitas AMIKOM Yogyakarta.