BAB II  
TINJAUAN PUSTAKA

## Kajian Ilmiah

RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika *modulo*. Baik kunci enkripsi maupun deskripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat). Kenyataannya, memfaktorkan bilangan non prima menjadi faktor primanya bukanlah pekerjaan yang mudah. Belum ada algoritma yang mangkus (efisien) yang ditemukan untuk pemfaktoran itu. Semakin besar bilangan non primanya, tentu semakin sulit pula pemfaktorannya. Semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA (Arifin, 2009).

Penelitian yang terkait dengan algoritma kriptografi RSA adalah aplikasi enkripsi sms dengan metode RSA pada smartphone berbasis android. Aplikasi SMS diterapkan pada *platform* android, karena *platform* android paling banyak digunakan oleh berbagai perangkat mobile. Aplikasi yang dibuat mampu melakukan enkripsi dan deskripsi terhadap alfabet, angka dan simbol-simbol. Aplikasi juga diharapkan mampu melindungi pesan rahasia yang dikirimkan saat dilakukan penyadapan terhadap perangkat *mobile* (Sasmita dkk, 2014).

RSA mempunyai proses enkripsi dan dekripsi yang menggunakan kunci berbeda. Proses dekripsi algoritma RSA sering mempunyai kendala dalam hal ukuran kunci dekripsi yang relatif besar sehingga memperlambat proses (Arief, 2016).

Penelitian dan beberapa referensi di bidang sistem pendukung keputusan yang telah dilakukan sebelumnya dipakai untuk mendasari penelitian ini, terutama berkenaan dengan metode yang dipergunakan.

Secara umum penelitian-penelitian yang telah dilakukan terdahulu dapat dirangkum pada (Tabel 2.1).

Tabel 2.1 Penelitian Terdahulu

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Peneliti** | **Tahun** | **Judul Penelitian** |
| 1 | Zainal Arifin | 2009 | Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman |
| 2 | I Gusti Made Arya Sasmita, dkk | 2014 | Aplikasi Enkripsi SMS Dengan Metode RSA Pada Smartphone Berbasis Android |
| 3 | Ashari Arief, dkk | 2016 | Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging |
| 4 | Elvand Andrian Manurung | 2017 | Enkripsi File Teks Menggunakan Algoritma Rivest-Shamir-Adleman (RSA) |

## Dasar Teori

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (*message*). Kriptografi telah banyak diimplementasikan di banyak hal. *Smart card*, Anjungan Tunai Mandiri (ATM), *Pay TV*, *Mobile Phone*, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanan-nya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti / dibaca manusia (*plaintext*) ke bentuk lain yang tidak dapat dimengerti / dibaca oleh manusia (*ciphertext*). Proses transformasi *plaintext* menjadi chipertext diistilahkan dengan enkripsi. Sedang proses pengembalian pesan *chipertext* menjadi *plaintext* diistilahkan dengan dekripsi (Primartha, 2011).

Sistem kriptografi kunci publik adalah bahwa kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Kunci untuk enkripsi bersifat publik (tidak rahasia) sehingga dinamakan kunci publik, sedangkan kunci dekripsi bersifat rahasia sehingga dinamakan kunci privat (kunci rahasia). Hasil kajian teknik enkripsi data dengan metode algoritma simetri menunjukan bahwa kelemahan-kelemahan pada metode simetri dengan kunci tunggal bisa diselesaikan dengan menggunakan metode lain yang disebut dengan metode kunci publik yang menggunakan 2 (dua) kunci yaitu *public key* dan *private key* (Listiyono, 2009).

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi (*encryption*) dan salah satu penemuan besar pertama dalam kriptografi kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat *up-to-date* (mutakhir) (Pahrizal dan Pratama, 2016).

Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Instittute of Technology*) pada tahun 1976. Ketiga peneliti tersebut adalah Ron Riverst, Adi Shamir, dan Leonard Adleman. Algoritma RSA digunakan untuk membangkitkan 2 kunci yaitu kunci publik dan kunci privat. Kunci publik adalah dua buah variabel bilangan (e,n) yang digunakan untuk mengenkripsi data. Sedangkan kunci privat adalah dua buah variabel bilangan (d,n) yang digunakan untuk melakukan dekripsi data. Nilai e, d dan n adalah nilai bilangan bulat positif. Keamanan algoritma RSA bergantung pada kesulitan memfaktorkan bilangan besar. “*We have proposed a method for implementing a publik-key cryptosystem whose security rests in part on the difficulty of factoring large numbers*” (R.L. Rivest, A.Shamir, and L. Adleman, 1977).

Algoritma kriptografi dapat dibagi ke dalam kelompok algoritma simetris dan algoritma asimetris. Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Algoritma simetris dapat dikelompokkan menjadi dua kategori, yaitu cipher aliran (*stream chiper*) dan cipher blok (*block chiper*). Cipher aliran merupakan algoritma kriptografi yang beroperasi dalam bentuk bit tunggal. Sedangkan algoritma kriptografi kategori cipher blok beroperasi dalam bentuk blok bit pada penelitian ini RSA menggunakan algoritma *chiper block* yang dimana setiap blok terdiri dari beberapa bit (1 blok terdiri dari 64 bit atau 128 bit) (Andriyanto dan Pardede, 2008).

Pada umumnya RSA menggunakan algoritma asimetris dimana pada proses enkripsi dan dekripsi mempunyai dua kunci yang berbeda, yaitu kunci umum (*public key*) yang digunakan untuk proses enkripsi yaitu perubahan data teks asli (*plaintext*) menjadi teks rahasia (*ciphertext*) yang sifatnya tidak rahasia, dan kunci pribadi (*private key*) yang digunakan untuk proses dekripsi yaitu pengembalian data teks rahasia (*ciphertext*) menjadi teks asli (*plaintext*) yang sifatnya rahasia dan masing-masing pihak memiliki kunci pribadi yang berbeda (Ginting dkk, 2015). Keamanan kunci privat dan kunci publik pada algoritma RSA sangat bergantung pada dua variabel p dan q dimana variabel ini di gunakan untuk menciptakan kedua kunci tersebut (Zainnudin dan Mulyana, 2016).

RSA merupakan suatu algoritma yang populer digunakan karena kesederhanaan, serta memiliki kecepatan proses yang tidak kalah cepat dibandingkan dengan algoritma kriptografi lainnya. Secara umum algoritma RSA banyak digunakan pada proses penyandian yang bersifat software aplikasi Sistem Pembangkitan Kunci pada Algoritma RSA sedangkan salah satu kelemahan sistem penyandian yang bersifat online adalah pengguna diharuskan terkoneksi dengan jaringan internet setiap ingin melakukan proses enkripsi dan dekripsi informasi rahasia (Busran, 2014).

Salah satu cara untuk mengamankan data atau informasi dengan Kriptologi. Kriptografi adalah studi keamanan (kerahasiaan). Algoritma kriptografi teknis terdiri dari substitusi dan transposisi teknis teknik. Teknik kriptografi dapat dipercaya untuk menangani masalah keamanan data atau informasi, karena selain menggunakan bahasa pemrograman komputer, kriptografi juga menggunakan rumus matematika, mulai dari rumus sederhana untuk formula kompleks. Dalam kriptografi terdapat dua konsep utama, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana data atau informasi diubah menjadi bentuk yang tidak dikenali sebagai informasi awalnya dengan menggunakan metode tertentu sedangkan dekripsi adalah mengubah kembali bentuk tersamar tersebut menjadi informasi awal (Pradipta, 2016).

Banyak cara yang dilakukan oleh pengembang TI dalam urusan keamanan, salah satunya menggunakan metode kriptografi. Kriptografi adalah sebuah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dimengerti atau dibaca, proses ini disebut dengan enkripsi. Untuk membacanya kembali maka lakukanlah proses dekripsi atau pengembalian ke tulisan aslinya. Hal ini banyak dimanfaatkan untuk menyamarkan dokumen-dokumen penting sehingga hanya orang-orang tertentu yang dapat membuka dan membacanya. Selain itu membuat dokumen tersebut aman apabila jatuh ke pihak lain. Seiring dengan perkembangannya, kriptografi mulai dimanfaatkan untuk menyamarkan *file-file* non dokumen seperti gambar, *video* maupun suara (Arief, 2015).

Syarat-syarat yang ada pada pembangkitan Kunci RSA adalah :

1. Pilih nilai p dan q yang dimana kedua nilai bilangan tersebut merupakan bilangan prima acak besar.
2. Hitung nilai n dari hasil p\*q (dimana nilai n digunakan pada proses pembangkitan kunci publik dan kunci privat).
3. Hitung nilai Q(n) = (p-1) \* (q-1) yang dimana nilai Q(n) berfungsi sebagai proses menentukan nilai kunci publik dan privat.
4. Pilih nilai e dimana 1 < e < Q(n) dan e adalah relatif prima dengan Q(n), relatif prima artinya nilai PBB (kunci publik, Q(n)) = 1.
5. Buat sebuah kunci privat d, dimana d menggunakan persamaan d = 1+kQ(n)/e dan k adalah salah satu bilangan bulat 1,2,3, ,..Q(n).

### 2.2.1 Mekanisme Kriptografi

Enkripsi adalah proses untuk mengubah pesan yang tidak disandikan (*plaintext*) ke dalam bentuk yang tidak dapat dibaca (*ciphertext*), dekripsi adalah proses untuk mengubah pesan yang tidak dapat dibaca kedalam bentuk yang dapat dibaca. Proses enkripsi dan dekripsi diatur oleh kunci kriptografi tertentu. Urutan proses kerja secara umum dapat digambarkan pada Gambar 2.2 sebagai berikut:

Plaintext

Enkripsi

Ciphertext

Dekripsi

Plaintext

Kunci Enkripsi

Kunci Dekripsi

Gambar 2.2 Mekanisme Kriptografi

### 2.2.2 Macam Macam Algoritma Kriptografi Modern

Algoritma kriptografi dibagi menjadi 2 bagian berdasarkan kunci yang dipakainya, yaitu Algoritma Simetris (menggunakan satu kunci untuk enkripsi dan deskripsinya) dan Algoritma Asimetris (menggunakan dua kunci yang berbeda untuk enkripsi dan dekripsinya).

1. Algoritma Simetris

Algoritma ini disebut simetris karena memiliki *key* atau kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini juga sering disebut algoritma kunci tunggal atau algoritma satu kunci. *Key* dalam algoritma ini bersifat rahasia atau *private key* sehingga algoritma ini juga disebut dengan algoritma kunci rahasia (Prayudi, 2005).

Algoritma yang memakai kunci simetris di antaranya adalah :

* + 1. Data encryption Standard (DES)
    2. RC2,RC4,RC5,RC6
    3. International Data Encryption Algorithm (IDEA)
    4. One Time Pad (OTP)
    5. A5
    6. Dan lain sebagainya.

Proses algoritma simetri dapat dilihat pada Gambar 2.3.

 Gambar 2.3 Proses Algoritma Simetri

1. Algoritma Asimetris

Algoritma ini disebut asimetris karena kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Kunci yang digunakan untuk enkripsi adalah kunci publik atau *public key* sehingga algoritma ini juga disebut dengan algoritma kunci publik. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia atau *private key* (Prayudi, 2005).

Algoritma yang memakai kunci publik di antaranya adalah :

* 1. Digital Signature Algorithm (DSA)
  2. Diffie-Hellman (DH)
  3. RSA
  4. ElGamal
  5. Elliptic Curve Cryptography (ECC)
  6. Dan lain sebagainya.

Proses algoritma asimetris dapat dilihat pada Gambar 2.4.

Gambar 2.4 Proses Algoritma Asimetris

### 2.2.3 Algoritma Cipher Pada Proses Asimetris Dan Simetris

1. Stream Cipher

*Stream cipher* (aliran cipher) Merupakan suatu cipher yang berasal dari hasil XOR dimana digit *plaintext* digabungkan dengan *keystream*. Dalam *stream cipher*, masing-masing digit *plaintext*-nya di enkripsi satu per satu dengan digit yang sesusai dari *keystream*.

1. Block Cipher

Merupakan suatu algoritma yang mana input dan output nya berupa satu blok, dan setiap blok terdiri dari beberapa bit (1 blok terdiri dari 64 bit atau 128 bit). *Block cipher* mempunyai banyak aplikasi, aplikasi tersebut di gunakan untuk memberikan layanan *confidentiality* (kerahasiaan), integritas data atau authentication (pengesahan pemakai), dan juga bisa memberikan layanan keystream generator untuk *stream cipher*.

### 2.2.4 Algoritma Rivest-Shamir-Adleman (RSA)

RSA merupakan salah satu kriptografi asimetris, algoritma asimetris di rancang sedemikian rupa sehingga kunci yang di pakai untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi. Lebih jauh lagi, kunci dapat dihitung dari kunci enkripsi. algoritma ini disebut algoritma kunci publik karena kunci enkripsi dapat dibuat publik sehingga orang lain dapat mengetahuinya, namun hanya orang tertentu dan sekaligus pemilik kunci dekripsi yang dapat melakukan dekripsi pesan tersebut. Dalam hal ini kunci enkripsi sering disebut dengan kunci publik dan kunci dekripsi sering disebut dengan kunci privat. Kunci privat kadang-kadang sering disebut kunci rahasia (Susanto dan Tritanto, 2011).

Rumus enkripsi :

C = Me mod n................................................................................................. 2.1

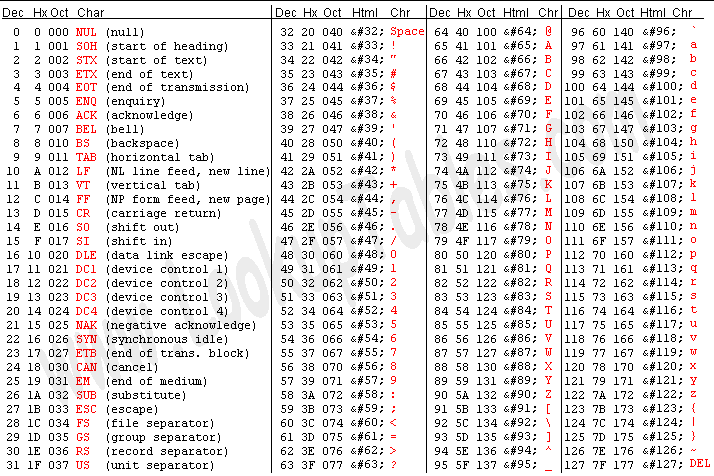
Rumus dekripsi :

M = Cd mod n = (Me)d mod n = Med mod n.................................................... 2.2

Besaran-besaran yang digunakan pada algoritma RSA :

1. p dan q bilangan acak prima (rahasia)
2. n = p\*q (tidak rahasia)
3. Qn = (p-1)\*(q-1) (rahasia)
4. e = 1 < e < Q(n) (kunci enkripsi) (tidak rahasia)
5. d = 1+kQ(n)/e (kunci dekripsi) (rahasia)
6. M (*plaintext*) (rahasia)
7. C (*ciphertext*) (tidak rahasia)

Jika didapat p = 11 dan q = 13 yang akan digunakan dalam proses enkripsi dan dekripsi dengan plaintext “TEKNIKINFORMASI”, yaitu dengan cara :

1. p = 11, q = 13, nilai p dan q merupakan bilangan prima acak.
2. n = 143, nilai n didapat dengan rumus n = p\*q.
3. Q(n) = 120, nilai Qn didapat dengan rumus Qn = (p-1)\*(q-1).
4. e = 7, nilai e didapat dengan rumus e = 1 < e < Q(n).
5. d = 103, nilai d didapat dengan rumus d = 1+kQ(n)/e.

Sumber : [www.Lookup](http://www.Lookup) Tables.com

Gambar 2.5 Tabel *ASCII*

*Plaintext* : “TEKNIKINFORMASI”

Kode *ASCII* dari *Plaintext*

Tabel 2.2 Hasil Enkripsi

| Char | ASCII |
| --- | --- |
| T | 84 |
| E | 69 |
| K | 75 |
| N | 78 |
| I | 73 |
| K | 75 |
| I | 73 |
| N | 78 |
| F | 70 |
| O | 79 |
| R | 82 |
| M | 77 |
| A | 65 |
| S | 83 |
| I | 73 |

Tabel 2.2 menunjukan nilai *ASCII* dari setiap karakter yang akan di enkripsi yaitu “84,69,75,78,73,75,73,78,70,79,82,77,65,83,73”. Selanjutnya proses enkripsi dilakukan dengan cara sebagai berikut :

Enkripsi (*cipher code*) = (*Character*)e mod n.

Sehingga didapatkan data seperti di tunjukkan dalam Tabel 2.3

Tabel 2.3 Enkripsi *Code*

| Plain Text | Ascii | e | n | Pangkat | chiper char | Chiper Text |
| --- | --- | --- | --- | --- | --- | --- |
| T | 84 | 7 | 143 | 29,509,034,655,744 | 72 | H |
| E | 69 | 7 | 143 | 7,446,353,252,589 | 108 | L |
| K | 75 | 7 | 143 | 13,348,388,671,875 | 114 | R |
| N | 78 | 7 | 143 | 17,565,568,854,912 | 78 | N |
| I | 73 | 7 | 143 | 11,047,398,519,097 | 83 | S |
| K | 75 | 7 | 143 | 13,348,388,671,875 | 114 | R |
| I | 73 | 7 | 143 | 11,047,398,519,097 | 83 | S |
| N | 78 | 7 | 143 | 17,565,568,854,912 | 78 | N |
| F | 70 | 7 | 143 | 8,235,430,000,000 | 60 | < |
| O | 79 | 7 | 143 | 19,203,908,986,159 | 40 | ( |
| R | 82 | 7 | 143 | 24,928,547,056,768 | 69 | E |
| M | 77 | 7 | 143 | 16,048,523,266,853 | 77 | M |
| A | 65 | 7 | 143 | 4,902,227,890,625 | 65 | A |
| S | 83 | 7 | 143 | 27,136,050,989,627 | 8 | BackSpace |
| I | 73 | 7 | 143 | 11,047,398,519,097 | 83 | S |

*CipherText* yang dihasilkan adalah :

“H,L,R,N,S,R,S,N,<,(,E,M,A,Backspace,S”

Tabel 2.4 menunjukan nilai *ASCII* setiap karakter yang akan di dekripsi yaitu “72,108,114,78,83,114,83,78,60,40,69,77,65,8,83”. Selanjutnya proses dari dekripsi dilakukan dengan cara sebagai berikut :

Deskripsi (*Plaintext*) = (*Cipher code*)d mod n

Sehingga didapatkan data seperti di tunjukkan data dalam tabel 2.4

Tabel 2.4 Dekripsi *Code*

| Chiper Char | d | n | Hasil Pangkat | Hasil Mod | Plain Text |
| --- | --- | --- | --- | --- | --- |
| 72 | 103 | 143 | 5.4605E+224 | 84 | T |
| 108 | 103 | 143 | 1.1073E+246 | 69 | E |
| 114 | 103 | 143 | 7.6822E+248 | 75 | K |
| 78 | 103 | 143 | 8.779E+228 | 78 | N |
| 83 | 103 | 143 | 1.616E+232 | 73 | I |
| 114 | 103 | 143 | 7.6822E+248 | 75 | K |
| 83 | 103 | 143 | 1.616E+232 | 73 | I |
| 78 | 103 | 143 | 8.779E+228 | 78 | N |
| 60 | 103 | 143 | 1.4332E+215 | 70 | F |
| 40 | 103 | 143 | 7.0674E+193 | 79 | O |
| 69 | 103 | 143 | 3.1677E+222 | 82 | R |
| 77 | 103 | 143 | 1.8424E+228 | 77 | M |
| 65 | 103 | 143 | 2.3042E+219 | 65 | A |
| 8 | 103 | 143 | 1.8788E+109 | 83 | S |
| 83 | 103 | 143 | 1.616E+232 | 73 | I |

*PlainText* yang dihasilkan adalah :  
“T,E,K,N,I,K,I,N,F,O,R,M,A,S,I”