BAB IV. ANALISIS dan PERANCANGAN

Tahap analisis dan perancangan merupakan tahap sistematis untuk menyesuaikan kegunaan dan tujuan pada aplikasi. Tahap awal pada tahap analisis dimulai dari analisis masalah, menganalisis sistem dengan menganalisis aplikasi sejenis, analisis fungsional dan non-fungsional. Sedangkan untuk tahap perancangan dimulai dengan melakukan perancangan sistem yang mencakup perancangan antar muka dan perancangan struktur menu yang nantinya akan digunakan untuk diterapkan pada aplikasi.

4.1 Analisis

Analisis sistem merupakan penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponenya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan, kebutuhan serta hambatan yang terjadi. Menentukan kebutuhan yang sesuai dengan kebutuhan-kebutuhan yang diharapkan, untuk melakukan analisis sistem dilakukan beberapa analisis yaitu:

a. Analisis Masalah
b. Analisis Sistem yang Berjalan
c. Analisis Aplikasi Kriptografi yang dibangun
d. Analisis Metode / Metode RSA
e. Analisis Kebutuhan Non-Fungsional
f. Analisis Kebutuhan Fungsional

4.1.1 Analisis Masalah

Analisis masalah adalah tahap penjabaran masalah yang ada sebelum aplikasi ini dibangun dan bertujuan untuk membantu pembangunan aplikasi kriptografi ini. Berikut adalah penjabaran dari masalah – masalah yang ada antara lain sebagai berikut:

1. Belum memiliki sendiri sistem Keamanan informasi antar karyawan Telkom Bojonegoro yang artinya bukan milik pihak ke 2 untuk mengkomunikasikan secara aman data data penting antar STO sehingga di khawatirkan berbagai faktor latar belakang seperti persaingan bisnis menggunakan data privasi untuk strategi bisnis pemasaran Telkom Bojonegoro maka dengan fakta yang ada dibutuhkan keamanan informasi dalam hal penyampaian data antar STO/cabang masih menggunakan sistem komunikasi aplikasi pihak ke 3 yang dikhawatirkan

Terjadi penyadapan data-data *critical* perusahan seperti daftar *Slot Odp (optical distribution point)* perdaerah pelanggan informasi *management* keuangan dan strategi cabang.

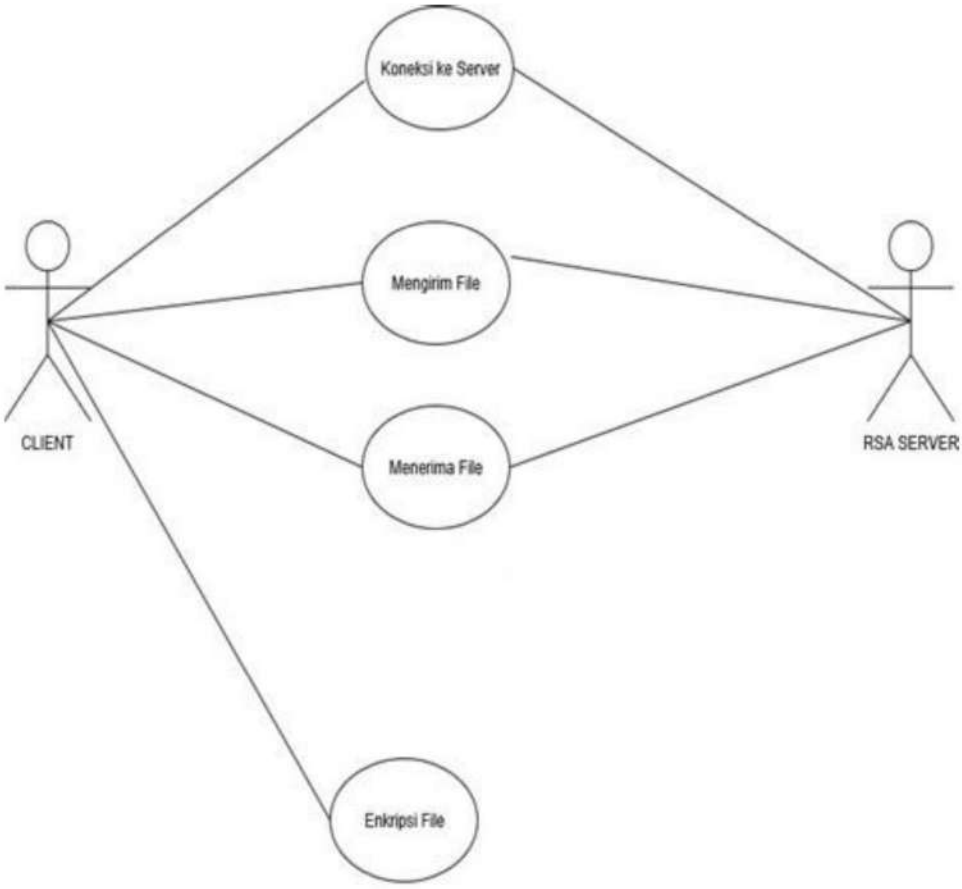
2. Sebuah data *text* penting biasanya menggunakan sistem pihak ke 2 yang bukan milik perusahaan maka pihak Telkom Bojonegoro mengajak untuk melakukan pengujian pembuatan sistem keamanan komunikasi berbasis *text* yang sangat aman antar cabang lokal kota Bojonegoro.

4.1.2 Analisis Sistem yang Berjalan

Berdasarkan hasil pengamatan dan wawancara langsung didapatkan prosedur yang dilakukan pihak perusahaan dalam proses mengamankan datanya. Secara garis besar terdapat beberapa tahapan yang dilakukan seperti berikut:

1. Pihak *Server* mengirimkan kunci publik ke pihak cabang untuk kemudian digunakan sebagai kunci untuk mengenkripsi *palintext*.
2. Algoritma RSA pada sistem akan mengkodekan *plaintext* menjadi *chiper text* atau data acak yang tidak dapat dibaca oleh pihak lain.
3. Pada tahap akhir *server* atau cabang pusat akan men*decode chiper* menjadi *plaintext* dengan menggunakan pasangan kunci nya yaitu kunci privat.

Use Case adalah gambaran *graphical* dari beberapa atau semua *actor, use case*, dan interaksi diantaranya yang memperkenalkan suatu sistem. yang menggambarkan interaksi antara pengguna dengan sistem yang dirancang beserta fungsionalitas yang diberikan oleh sistem. Use case Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro untuk Meningkatkan Keamanan Sistem Jaringan dapat di lihat pada gambar 4.1:

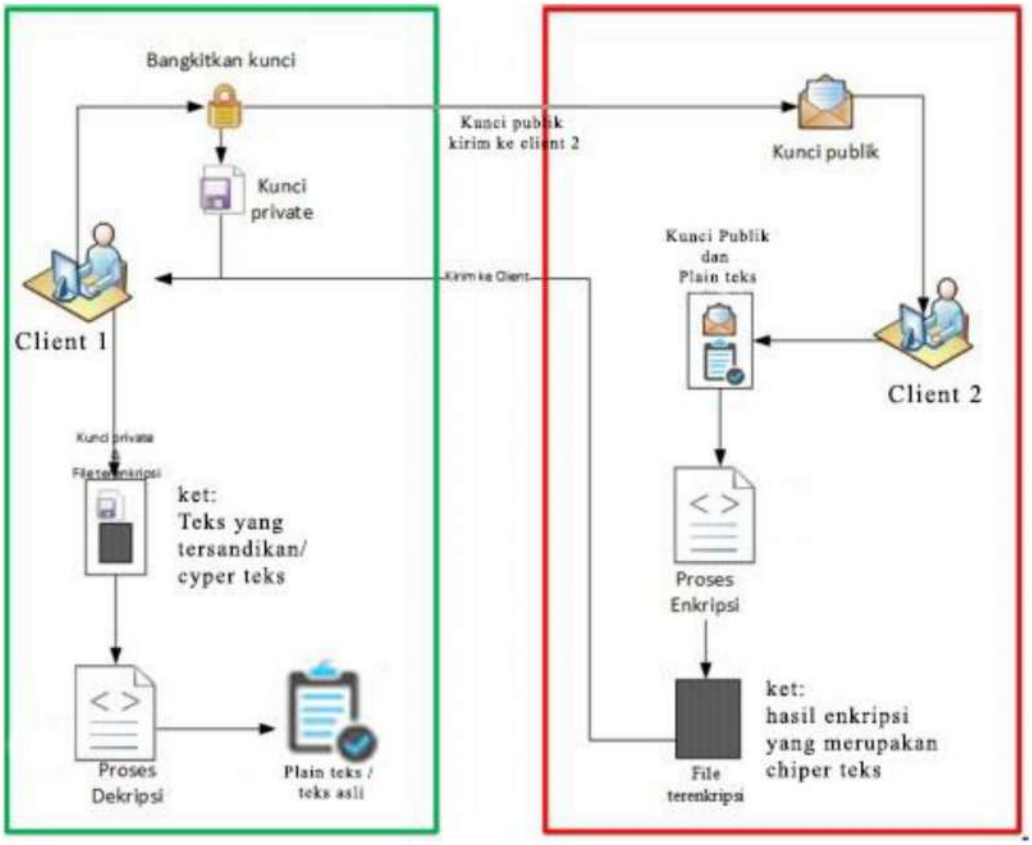


Gambar 4. 1 Diagram *Use Case*

4.1.3 Analisis Aplikasi Kriptografi yang Akan Dibangun

Aplikasi yang dibangun adalah sebuah aplikasi yang dapat melakukan kriptografi terhadap data. Proses kriptografi ini dilakukan agar data digital tidak bisa dilihat menggunakan aplikasi pembuka teks. Hal ini bisa dilakukan dengan asumsi bahwa setiap data yang akan telah dikenakan algoritma kriptografi akan mengalami pertambahan nilai sehingga data tidak dapat dibaca oleh aplikasi pembuka data biasa. Selain itu juga akan diberikan penyisipan nilai pada data digital sehingga data digital hanya dapat dibuka beberapa kali saja.

Untuk lebih jelasnya proses yang akan terjadi dalam aplikasi yang akan dibangun dapat dilihat pada gambar 4.2 adalah sebagai berikut:



Gambar 4. 2 Proses Kriptografi Terhadap Data

Hal yang dilakukan gambar 4.2 adalah interaksi antara pihak *Client* 2 dan pihak *Client* 1 pada program keamanan data di Telkom Bojonegoro. Proses pertama yang dilakukan adalah proses diluar sistem yaitu saat pihak *client* 2 meminta sebuah desain maka pihak perusahaan akan mengirimkan sebuah aplikasi dekripsi yang dilengkapi dengan menu pembangkit kunci. Selanjutnya adalah proses yang termasuk dalam cakupan aplikasi:

a. Pertama pihak *client* 2 membangkitkan kunci privat dan kunci publik. Kunci privat disimpan pihak *client* 2 dan kunci privat harus dijaga dengan baik karena kunci ini akan digunakan untuk proses dekripsi. Jika kunci ini berhasil didapatkan oleh pihak lain maka data akan mudah didekripsi sehingga rancangan bisa dilihat oleh pihak yang tidak berkepentingan.
b. Kunci publik yang telah dibangkitkan ditahap pertama akan dikirimkan ke pihak perusahaan. Kunci ini berguna untuk melakukan proses enkripsi data. Pengiriman ini bisa dilakukan melalui jaringan lain diluar aplikasi. Kunci ini sifatnya aman karena jika kunci publik berhasil diambil maka pihak lain tidak dapat melakukan proses dekripsi karena proses dekripsi hanya menggunakan kunci privat.

c. Tahapan ketiga adalah ketika kunci publik telah didapatkan oleh pihak perusahaan maka pihak perusahaan akan melakukan pencarian data yang akan dikirimkan kepada *client* 1.

d. Setelah gambar dan kunci siap maka keduanya akan dimasukkan kedalam aplikasi enkripsi. Pada proses ini akan dienkripsi dengan menyisipkan nilai pembatas dekripsi pada salah satu indeks *array byte*. Pada proses enkripsi ini akan menghasilkan suatu *file*.

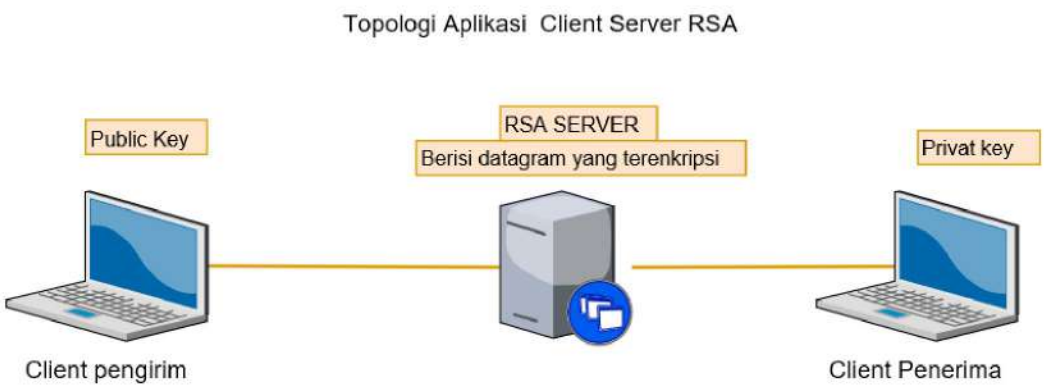
e. Ketika proses enkripsi telah dilakukan dan menghasilkan *file* terenkripsi maka selanjutnya pihak perusahaan akan mengirimkan *file* terenkripsi tersebut kepada pihak perusahaan.

f. *File* terenkripsi yang telah sampai pada pihak perusahaan akan digunakan pada proses dekripsi. Dengan menggunakan kunci privat yang telah disimpan sebelumnya dan *file* terenkripsi tersebut maka proses dekripsi dapat dilakukan. Proses dekripsi ini akan mengembalikan *file* terenkripsi menjadi *file* data semula. Pada proses enkripsi ini terdapat hal penting yaitu proses pengecekan batas dekripsi. Pengecekan ini akan menentukan *file* tersebut masih bisa dienkripsi ataukah tidak. Jika proses ini telah dilakukan maka akan menghasilkan *file* aslinya dan tahapan proses aplikasi ini pun selesai.

Sistem yang akan dibangun pada penelitian ini adalah aplikasi *file* transfer yang mengamankan data-data penting atau *Critical Data* dengan menarapkan Enkripsi yang di implementasikan menggunakan algoritma kriptografi RSA pada program Berbasis *file* transfer pada jaringan client server. Program sendiri berupa sebuah FTP *Client* dengan fungsi-fungsi dasar dalam FTP yaitu:

1. *Login (connect* dan *disconnect)*
2. *Upload*
3. Enkrip Dekrip
4. *Download*

Berikut merupakan gambar topologi aplikasi dapat dilihat pada gambar 4.3:



Gambar 4. 3 Topologi *Client Server* RSA

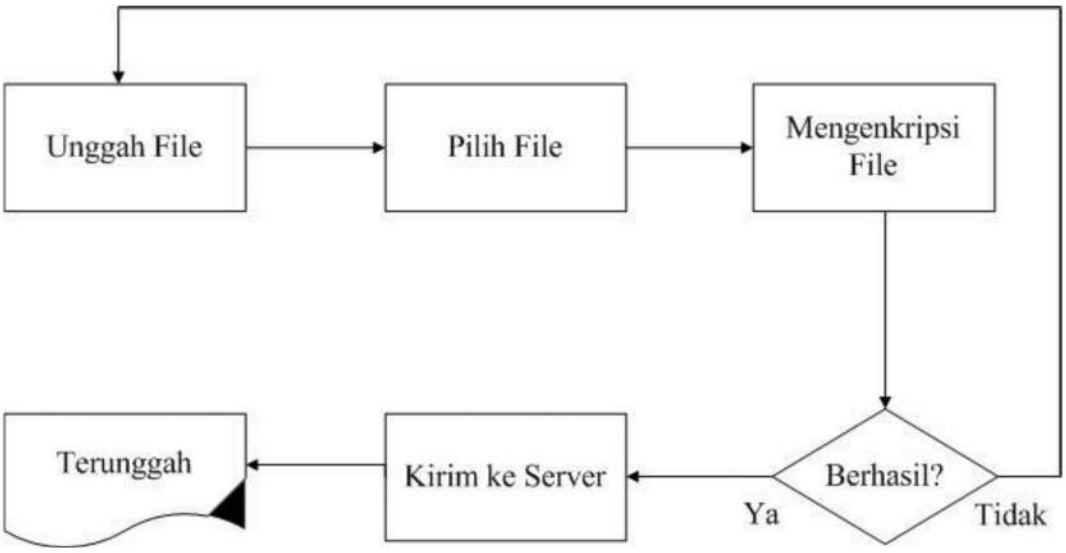
Keterangan:

Gambar 4.3 merupakan Topologi yang menggambarkan interaksi pengiriman data penting yang sudah tersandikan *(chipertext)* antara *node client* pengirim dan penerima dengan *server* pada sistem berbasis jaringan *client server.*

Sistem *client* akan mengenerate dua pasangan kunci (*key pair) public key* dan *privat key, pubic key* akan di serahkan ke *server* agar client pengirim pesan dapat mendekripsikan pesan *plaint text* dengan kunci tersebut. Lain halnya dengan *privat key* haruslah di rahasiakan dan di simpan oleh *client* penerima yang membangkitkan *keypair* tersebut, anda bisa menganalogikan bahwa *server* adalah kotak surat yang setiap orang bisa memasukan pesan atau surat ke kotak tersebut dengan kunci publik sedangkan untuk membuka kotak secara keseluruhan maka di butuhkan kunci pribadi yang hanya di pegang oleh pemilik kotak pesan tersebut. Selain itu fungsi dari topologi *client server* adalah memudahkan manajemen pengiriman data karena menggunakan jaringan publik sehingga lebih mudah untuk mengingat nama pengirim dan penerima dari pada harus mendelegasikan pesan tersebut dengan memasukan alamat *internet protocol/ip* satu persatu maka sistem dari server akan mengatur nya secara dinamis.

4.1.4 Proses Unggah

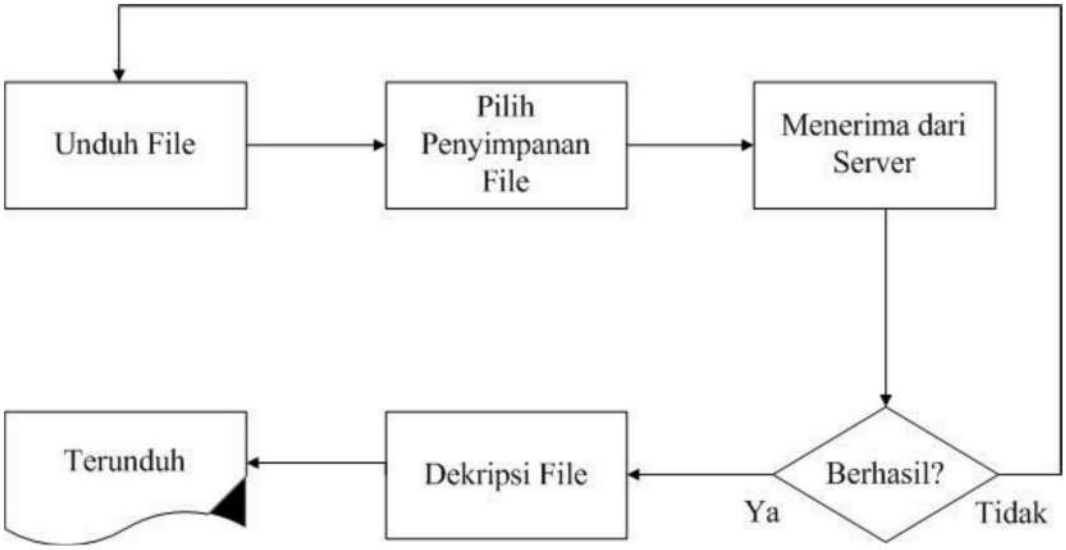
Pada bagian ini dijelaskan bagaimana alur diagram proses upload yang dilakukan oleh sistem. Algoritma kriptografi yang dipakai adalah RSA. Enkripsi dilakukan sesaat sebelum *file* akan dikirimkan ke server dapat dilihat pada gambar 4.4:



Gambar 4. 4 Diagram *Upload*

4.1.5 Proses *Download*

Pada proses *upload*, dilakukan enkripsi pada *file*. Jika *file* di *download*, hanya akan menghasilkan sebuah *chipper file*. Pada proses *download* ini akan dilakukan dekripsi untuk mengembalikan *file* ke bentuk semula. Proses *download* dapat dilihat pada gambar 4.5:

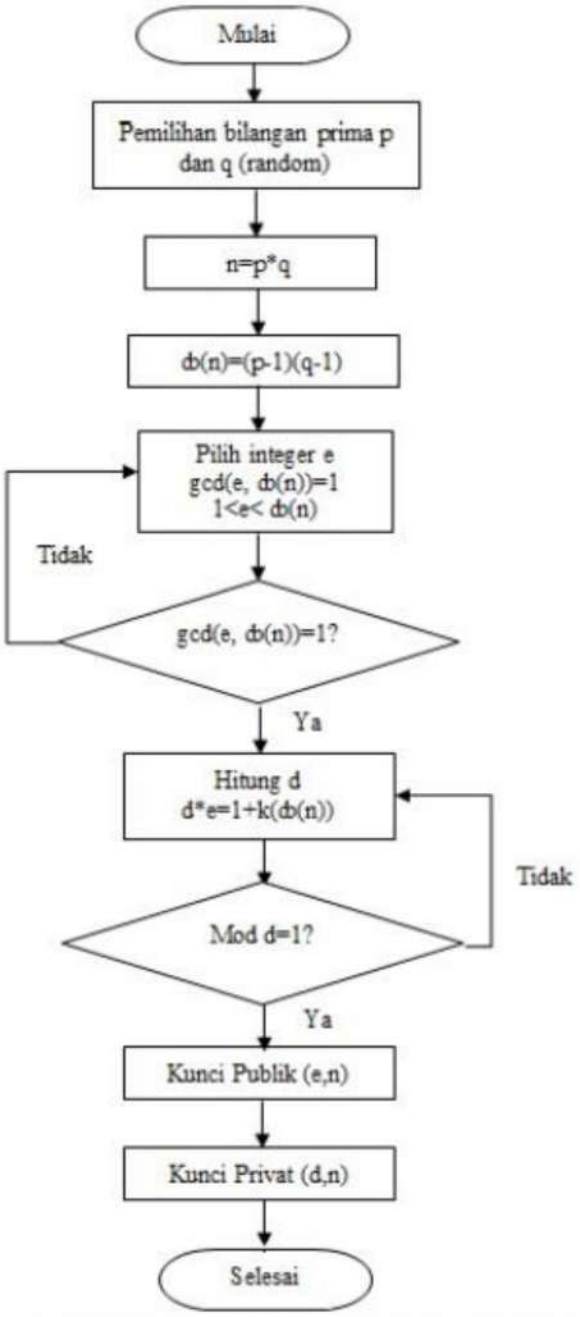


Gambar 4. 5 Diagram *Download*

4.1.6 Analisis Metode RSA

a. *Flowchart* Metode Algoritma Sistem

Gambar 4.5 merupakan diagram *Flowchart* yang menggambarkan implementasi Metode Algoritma kriptografi RSA pada sistem yang akan di buat oleh penulis dapat dilihat pada gambar 4.6:



Gambar 4. 6 *Flowchart* Algoritma RSA

Keterangan :

Pembangkit kunci :

- Pilih 2 bilangan prima besar seperti p, q dimana p tidak sama dengan q.
- Hitung M = p x q
- Hitung phi(M) = phi(p) * phi(q)
- Pilih sebuah integer 'e' dimana 1 < e < phi(M) dan 'e' serta phi(M) adalah *coprime*.
- Hitung 'd' *integer* sehingga (d * e) mod M = 1
- (P, e) adalah *public key* dimana P adalah *modulo* dan e adalah eksponen *encryption*.
- (P, d) adalah *private key* dimana P adalah *modulo* dan d adalah eksponen *decryption*.

Contoh Kunci yang telah di bangkitkan

Public Key e yang merupakan FPB dari modulus n:

Privat key Kunci privat:

(d * e) mod M = 1

Perhatikan bahwa $e \cdot d \equiv 1 \pmod{\varphi(n)}$ ekivalen dengan $e \cdot d = 1 + k\varphi(n)$, sehingga d dapat dihitung dengan

$$d = \frac{1 + k\varphi(n)}{e}$$

Algoritma enkripsi dan dekripsi :

$$C = M^e \bmod n \text{ (fungsi enkripsi)}$$

$$M = C^d \bmod n \text{ (fungsi dekripsi)}$$

C = *Cipherteks*

M = *Message / Plainteks*

e = kunci publik

d= kunci privat

n = modulo pembagi (akan dijelaskan lebih lanjut) [6].