SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Publikasi Jurnal & Penelitian Teknik Informatika
Volume 2 Nomor 2, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode *Hybrid Cryptosystem*

Jamaludin

Politeknik Ganesha Medan
Medan, Indonesia
jamaludinmedan@gmail.com

Abstract— Pemilihan algoritma kriptografi simetris dapat melakukan proses enkripsi dan dekripsi dengan waktu yang singkat, namun pengamanan kunci kurang aman sehingga harus sering diubah. Sementara kriptografi asimetris justru sebaliknya, keamanan distribusi kunci dapat diatasi namun proses enkripsi dan dekripsi data lebih lambat. *Hybrid Cryptosystem* sering dipakai karena memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma simetris dan kemudahan transfer kunci menggunakan algoritma asimetrik sehingga meningkatkan pengamanan teks. Penggunaan *Hybrid Cryptosystem* dalam penelitian ini merupakan kombinasi dari algoritma *Hill Cipher* sebagai bagian algoritma simetri, dan dikombinasikan dengan algoritma RSA sebagai bagian algoritma asimetri untuk pengamanan pesan teks. Hasil penelitian dari kedua kombinasi algoritma *Hill Cipher* dan RSA bisa diterapkan untuk peningkatan pengamanan pada pesan teks dimana plain teks yang dikirim dienkripsi oleh algoritma *Hill Cipher* serta pengamanan kunci oleh algoritma RSA.

Kata Kunci : ***Kriptografi, Hybrid cryptosystem, Hill Cipher, RSA***

I. PENDAHULUAN

1.1. Latar Belakang

Kehidupan kita saat ini dilingkupi oleh kriptografi, mulai dari transaksi di mesin ATM, transaksi di bank, transaksi dengan kartu kredit, mengakses internet, sampai mengaktifkan peluru kendali pun menggunakan kriptografi. Begitu pentingnya kriptografi untuk keamanan informasi *(information security)*, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkan dengan kriptografi. [4].

Ada beberapa seni pengamanan data yang melalui suatu saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang sangat rahasia akan disandikan sedemikian rupa sehingga walaupun data tersebut dicuri oleh pihak yang tidak berhak, namun mereka tidak dapat mengetahui data yang sebenarnya, karena data yang mereka curi merupakan data yang sudah disandikan. Data asli yang akan dikirimkan dan dalam kriptografi sebagai plaintext, dan data yang telah disandikan disebut sebagai ciphertext.(Munir, 2006)

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetris *(symmetric-key cryptography)* dan kriptografi kunci asimetris *(asymmetric-key cryptography)*. Masing-masing memiliki kelebihan dan kekurangannya. Algoritma kriptografi simetris dirancang sehingga proses enkripsi dekripsi membutuhkan waktu yang singkat. Adapun kelemahannya adalah pengamanan kunci yang kurang aman dan kunci harus sering diubah. Sementara kriptografi asimetris justru sebaliknya, masalah keamanan pada distribusi kunci dapat diatasi namun proses enkripsi dan dekripsi data umumnya lebih lambat karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar dan ukuran ciphertext lebih besar daripada plaintext. [4].

Alasan untuk mengatasi kelemahan kedua jenis kriptografi kunci tersebut yaitu lemahnya pengamanan data serta lambatnya proses enkripsi dekripsi maka diperlukan penelitian dengan menggabungkan algoritma Hill Cipher salah contoh kriptografi kunci simetris dan RSA salah contoh kriptografi kunci simetris dengan metode *hybrid cryptosystem*, sehingga dari kombinasi kedua jenis algoritma kriptografi tersebut diharapkan akan

menghasilkan tingkat keamanan yang tinggi namun cepat dalam proses enkripsi dan dekripsi

Hybrid cryptosystem merupakan gabungan antara *cryptosystem* yang memakai *asymmetric cryptosystem* dan *cryptosystem* yang memakai *symmetric cryptosystem.* [8]. Dalam penggunaan algoritma hybrid, teknik enkripsi yang digunakan adalah enkripsi simetri dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi.

Pemilihan *Hill* Cipher dikarenakan sandi *Hill* Cipher merupakan sandi yang kuat sehingga susah untuk diserang secara *brute* force dan mampu bertahan terhadap analisis frekuensi disebabkan substitusi yang tidak beragam. Kelemahan utama dari *Hill* Cipher adalah digunakannya persamaan linier dengan matriks sebagai operasi substitusi. Apabila penyerang mampu mengumpulkan pasangan teks asli dan teks sandi yang menggunakan kunci yang sama, penyerang dapat menemukan kunci *Hill* Cipher dengan menyelesaikan system persamaan linier. [5]. Sedangkan pemilihan algoritma RSA sebagai kriptografi kunci asimetris karena dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, algoritma yang paling popular adalah algoritma RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar. Oleh karena alasan tersebut RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. [1].

1.2. Tujuan Penelitian

Adapun tujuan penelitian ini adalah : untuk mengkombinasikan algoritma *Hill Cipher*, dan RSA sehingga akan meningkatkan pengamanan yang lebih baik dari hasil kombinasi tersebut.

1.3. Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian tesis ini adalah :

1. Memberikan pemahaman tentang konsep dasar kriptografi jenis simetris dan asimetris dalam hal ini penulis memilih *Hill Cipher* dan RSA
2. Memberikan pemahaman tentang konsep *hibrid cryptosystem*

II. LANDASAN TEORI

2.1. Konsep Kriptografi

Kriptografi berasal dari bahasa Yunani : *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan dan *graphia* berarti "*writing*" (tulisan). Menurut terminologi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. [4].

Selain berdasarkan sejarah yang membagi kriptografi menjadi kriptografi klasik dan kriptografi modern, maka berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetris *(symmetric-key cryptography)* dan kriptografi kunci asimetris *(asymmetric-key cryptography).* [4].

2.2. Perbandingan Kriptografi Kunci Simetris dan Kunci Asimetris

Kunci asimetris atau kunci pablik dan kunci simetris merupakan dua jenis kriptografi yang berbeda dan memecahkan jenis permasalahan yang berbeda pula. Proses enkripsi pada kriptografi simetris sangat baik namun sangat rentan pada pengamanan datanya yang dienkripsi. Kunci asimetris dapat mengerjakan apa yang tidak dapat dikerjakan pada kriptografi simetris yaitu sangat baik pada manajemen kunci. [8].

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan dengan kunci enkripsi. Untuk *public key cryptography,* diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibanding enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar. Namun enkripsi asimetris lebih lama dibanding enkripsi simetris, *public key cryptography* sangat berguna untuk *key management* dan *digital signature.* [2].

2.3. Hibrid Cryptosystem

Hybrid cryptosystem merupakan gabungan antara *cryptosystem* yang memakai *asymmetric cryptosystem* dan *cryptosystem* yang memakai *symmetric cryptosystem.* (Schneier, 1996). Dalam penggunaan algoritma hybrid, teknik enkripsi yang digunakan adalah enkripsi simetri dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi.

Hybrid cryptosystem adalah sebuah teknik yang menggunakan beberapa cipher yang berbeda untuk memanfaatkan masing-masing kelebihannya. Sebuah *Hybrid cryptosystem* dibangun dengan menggunakan dua pembagi cryptosystem yaitu kunci public dan kunci simetris. [7].

Pada sistem hibrid ini enkripsi/dekripsi pesan menggunakan kriptografi kunci simetris, sedangkan kunci simetris dienkripsi/dekripsi dengan menggunakan kunci publik. Kunci simetris (yang disebut juga kunci sesi) dibangkitkan oleh salah satu pihak dan mengenkripsi pesan dengan kunci tersebut. Selanjutnya kunci sesi dienkripsikan dengan kunci publik penerima lalu dikirim bersama-sama dengan pesan yang sudah dienkripsi. Penerima mula-mula mendekripsikan kunci sesi dengan kunci privatnya, lalu mendekripsikan pasan dengan kunci sesi tersebut. Kriptografi hibrid sering dipakai karena memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma simetris dan kemudahan transfer kunci menggunakan algoritma asimetris. Hal ini mengakibatkan peningkatan kecepatan tanpa mengurangi kenyamanan serta keamanan.

2.4. Hill Cipher

Hill cipher diciptakan pada tahun 1929 oleh seorang ahli matematika bernama Lester S. Hill dalam sebuah jurnal yang bernama : The Amercian Mathematic Monthy. *Hill cipher* merupakan cipher berjenis poly grafik pertama. Sebuah poly grafik adalah sebuah cipher dimana *plaintext* dibagi dalam sebuah group yang berdekatan dari panjang n, dan kemudian setiap group ditransformasikan ke dalam sebuah group yang berbeda dari n. Hill cipher menggunakan matrik dengan rumus C = K x P (mod m), dimana C representasidari C, P merupakan representasi plain teks sedang K adalah kunci. Kunci K pada bentuk matriks. Demikian juga untuk proses dekrisi dengan invers matriks $K^{-1.}$ [6].

Hill cipher merupakan sandi *polyalphabet* dengan menggunakan metode substitusi dengan perhitungan perkalian matrik. Kunci *Hill cipher* adalah sebuah matrik K berukuran n x n yang digunakan untuk mensubstitusi n alfabet sekaligus. Matrik K harus memiliki invers dan nilai matriks K juga harus memiliki invers perkalian pada Z_{NCHARS} dengan NCHARS adalah jumlah alfabet pada sistem alfabet yang digunakan. [5].

Hill cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas cipherteks saja. Namun, teknik ini bukan berarti tanpa cela, *hill cipher* dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas cipherteks dan potongan berkas plainteks. Teknik kriptanalisis ini disebut *known-plaintext attack*

Dasar dari teknik *Hill cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *Hill cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *hill cipher* adalah matriks *n* x *n* dengan *n* merupakan ukuran blok. Jika matriks kunci kita sebut dengan *K*, maka matriks *K* adalah sebagai berikut :

$$K = \begin{bmatrix} k_{11} & k_{12} & k_{1m} \\ k_{21} & k_{22} & k_{2m} \\ k_{m1} & k_{m2} & k_{mn} \end{bmatrix}$$

Matriks *K* yang menjadi kunci ini harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse* K^{-1} sehingga : $K \,.\, K^{-1} = 1$ (1)
Kunci harus memiliki invers karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi. [3].

2.5. RSA

Dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, algoritma yang paling popular adalah algoritma RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar. Oleh karena alasan tersebut RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. [1].

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 penerapanpenerapannya yang sangat up-to-date (mutakhir).

Enkripsi pada RSA adalah sebagai berikut.

1. *Plaintext* : $M < n$.
2. *Ciphertext* : $C = Me \pmod n$.

Dekripsi pada RSA adalah sebagai berikut.

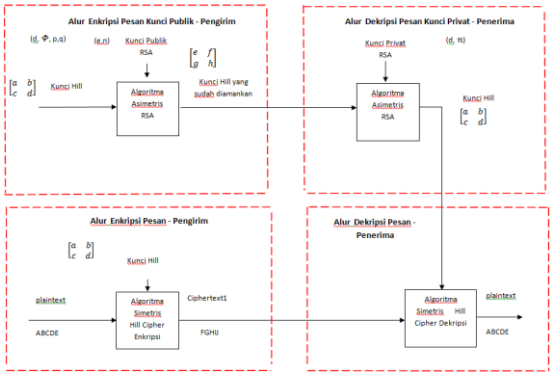
1. *Ciphertext* : *C*.
2. *Plaintext* : $M = Cd \pmod n$.

III. METODOLOGI PENELITIAN

3.1. Prosedur Penelitian

Metode yang digunakan dalam penelitian ini menggunakan *Hybrid Cryptosystem* dengan menggunakan kombinasi Algoritma Hill Cipher yang merupakan contoh dari kriptografi simetris dan Algoritma RSA merupakan contoh kriptografi asimetris. Untuk menguji kebenaran pengembangan algoritma *hybrid cryptosystem,* disini penulis memberikan contoh kunci untuk kunci *Hill Cipher* yaitu $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Adapun skema alur pengembangan algoritma *Hybrid Cryptosystem* ini dapat dilihat pada gambar 3.1.



Gambar 3.1. Alur pengembangan algoritma kombinasi *Hill Cipher* dan *RSA* menggunakan metode *Hybrid Crytosystem*

Untuk menyederhanakan proses enkripsi dan dekripsi pada pengembangan algoritma *Hybrid Cryptosystem* serta pembangkitan kunci, di bagi menjadi 4 alur :

1. Alur proses enkripsi pesan - pengirim
2. Alur proses dekripsi pesan - penerima
3. Alur proses enkripsi kunci public - pengirim
4. Alur proses dekripsi kunci privat - penerima

3.1.1. Alur Proses Enkripsi Pesan – Pengirim

Pada proses enkrpsi pesan, teks yang dapat dibaca *(plaintext)* ABCDE dienkripsi oleh Algoritma Simetris Hill Cipher dengan menggunakan kunci Hill $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ hasilnya dalam bentuk teks yang tersandikan *ciphertext* FGHIJ yang akan dikirim ke penerima nantinya.

3.1.2. Alur Proses Dekripsi Pesan – Penerima

Ciphertext FGHIJ hasil enkripsi Algoritma Hill Cipher Enkripsi, kemudian didekripsi oleh Algoritma Simetris Hill Dekripsi dengan menggunakan kunci Hill $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ hasil deskripsi kunci algoritma RSA menghasilkan plaintext ABCDE yang bisa dibaca oleh penerima.

3.1.3. Alur Proses Enkripsi Kunci – Pengirim

Kunci Hill $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dienkripsi menggunakan Algoritma Asimetris RSA dengan kunci public RSA menghasilkan kunci $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$ yang nanti akan dikirim ke penerima.

3.1.4. Alur Proses Dekripsi Kunci – Penerima

Kunci Hill sudah diamankan dienkripsi menggunakan Algoritma Asimetris RSA dengan kunci private RSA menghasilkan kunci Hill. Kemudian kunci tersebut didekripsikan menggunakan kunci private RSA maka dihasilkan kunci Hill yang digunakan untuk membangkitkan Algoritma Simetris Hill Cipher Dekripsi.

IV. HASIL DAN PEMBAHASAN

4.1. Pengantar

Pada bab ini akan dijelaskan mengenai hasil penelitihan penulis terhadap beberapa pesan teks, dari hasil penelitian tersebut nantinya dapat ditarik suatu kesimpulan, apakah pesan yang dikirimkan dapat terjaga kerahasiannya dan cepat dalam proses enkripsi maupun dekripsinya.

Untuk mengimplementasikan penerapan kedua algoritma di atas, maka perlu dilakukan analisis dan proses uji coba.

4.2. Proses Analisis

Sebelum membuat hasil simulasi perlu dilakukan proses analisis dengan perhitungan pada proses enkripsi dan dekripsi kombinasi algoritma *Hill Cipher* dan *RSA*. Hasil dari perhitungan yang benar, menjadi dasar pada pembuatan program hasil simulasi. Proses analisis ini juga bertujuan untuk mempermudah dalam perbaikan atau penambahan pada system tersebut.

4.2.1. Proses Enkripsi Pesan Text – Pengirim Menggunakan Kriptografi Hill Cipher

Langkah-langkah dalam perhitungan proses enkripsi pesan text – pngirim menggunakan Kriptografi *Hill Cipher* adalah sebagai berikut :

1. Plaintext : POLGAN
   Ambil secara acak kunci enkripsi e dengan syarat : GCD (det(e),N) = 1

   Misal kunci yang dimasukkan :

$$e = \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}$$

   Sehingga : det (e) = 3.5 – 6.1 = 15 – 6 = 9

   GCD(9,26) harus sama dengan 1

   26 mod 9 = 8,
   9 mod 8 = 1,
   8 mod 1 = 0

   Karena GCD (det(e),N) = 1 sehingga
   $e = \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}$ bisa dipakai sebagai kunci

2. Enkripsi plaintext dengan matrik e konversikan huruf ke nomor abjad

P	O	L	G	A	N
15	14	11	6	0	13
M_1		M_2		M_3	

C_1 = $(M_1 \times e) \pmod N$
= $((15 \quad 14) \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}) \pmod{26}$
= (15*3 + 14*1 15*6 + 14*5) (mod 26)
= (59 mod 26 160 mod 26)
= (7 4)
= **(H E)**

C_2 = $(M_2 \times e) \pmod N$
= $((11 \quad 6) \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}) \pmod{26}$
= (11*3 + 6*1 11*6 + 6*5) (mod 26)
= (39 mod 26 96 mod 26)
= (13 18)
= **(N S)**

C_3 = $(M_3 \times e) \pmod N$
= $((0 \quad 13) \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}) \pmod{26}$
= (0*3 + 13*1 0*6 + 13*5) (mod 26)
= (13 mod 26 65 mod 26)
= (13 13)
= **(N N)**

Jadi C :

H	E	N	S	N	N
7	4	13	18	13	13
C_1		C_2		C_3	

Jadi hasil enkrkipsi pesan algoritma Hill Cipher adalah ciphertext1 = **HENSNN**

4.2.2. Proses Dekripsi Pesan Text – Penerima Menggunakan Kriptografi Hill Cipher

Langkah-langkah dalam perhitungan proses dekripsi pesan text – penerima menggunakan Kriptografi *Hill Cipher* adalah sebagai berikut :

1. Cipertext1 : **HENSNN**

H	E	N	S	N	N
7	4	13	18	13	13
D_1		D_2		D_3	

Kunci $e = \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}$

d = $\frac{1}{3.5-6.1} x \begin{bmatrix} 5 & -6 \\ -1 & 3 \end{bmatrix} \pmod{26}$

d = $\frac{1}{9} x \begin{bmatrix} 5 & -6 \\ -1 & 3 \end{bmatrix} \pmod{26}$

d = $9^{-1} x \begin{bmatrix} 5 & -6 \\ -1 & 3 \end{bmatrix} \pmod{26}$

d = $3 \times \begin{bmatrix} 5 & -6 \\ -1 & 3 \end{bmatrix} \pmod{26}$

d = $\begin{bmatrix} 15 & -18 \\ -3 & 9 \end{bmatrix} \pmod{26}$

= $\begin{bmatrix} 15 & 8 \\ 23 & 9 \end{bmatrix} \pmod{26}$

Dekripsi pesan cipher

C_1 = (H E) = (7 4)
P_1 = D_1 x d mod N
= (7 4) $\begin{bmatrix} 15 & 8 \\ 23 & 9 \end{bmatrix} \pmod{26}$
= (7*15 + 4*23 7*8 + 4*9) (mod 26)
= (197 92) mod 26
= **(15 14) = (P O)**

C_2 = (N S) = (13 18)

P_2 = D_2 x d mod N
= (13 18) $\begin{bmatrix}15 & 8\\23 & 9\end{bmatrix}$ mod 26

= (13*15 + 18*23 13*8 + 18*9) (mod 26)
` = (609 266) mod 26
= (116) = (L G)

C_3 = (N N) = (13 13)
P_3 = D_3 x d mod N
= (13 13) $\begin{bmatrix}15 & 8\\23 & 9\end{bmatrix}$ mod 26

= (13*15 + 13*23 13*8 + 13*9) (mod 26)
= (494 221) mod 26
= (0 13) = (A N)

Jadi hasil deskripsi adalah

P	O	L	G	A	N
15	14	11	6	0	13
D_1		D_2		D_3	

Jadi hasil dekripsi pesan penerima algoritma Hill adalah plaintext = POLGAN

4.2.3. Proses Dekripsi Enkripsi Kunci – Pengirim Penerima Menggunakan Kriptografi RSA

Langkah-langkah dalam perhitungan proses dekripsi pesan kunci – pengirim menggunakan kriptografi *RSA* adalah sebagai berikut :

1. Ambil dua bilangan prima p dan q yang sangat besar
   Misal : P = 47, Q= 23

2. Hitung N = P . Q
   N = 47 . 23
   = 1081

3. Hitung $\Phi(n) = (P-1)(Q-1)$
   $\Phi(n) = (47-1)(23-1)$
   $\Phi(n) = 1012$

4. Ambil secara acak, kunci enkripsi e dengan syarat :
   - $1 < e < \Phi(n)$
   - e relative prima terhadap $\Phi(n)$,, sehingga GCD(e, $\Phi(n)$)=1

   Contoh yang memenuhi e = 17
   GCD(e, $\Phi(n)$) = 1
   GCD(17,1012) = 1

   1012 mod 17 = 9
   17 mod 9 = 8
   9 mod 8 = 1
   8 mod 1 = 0

   Sehingga e = 17 memenuhi syat tersebut di atas

5 Hitung kunci dekripsi d
e. d mod $\Phi(n) = 1$

D	e. d mod $\Phi(n) = 1$ 17.d. mod 1012 = 1
1	17.1.mod 1012 = 17
2	17.2. mod 1012 = 34
3	17.3. mod 1012 = 51
. . .	. . .
893	17.893 mod 1012 = 1

Setelah dilakukan perhitungan yang memenuhi syarat e. d mod $\Phi(n) = 1$, saat d hitungan ke 893

6. Publish pasangan kunci public = (e, N)
   = (17, 1081)

7. Simpan pasangan kunci privat = (d, *N*)
   = (893,1081)

Pengirim :

8. Dapatkan pasangan kunci public penerima
   Kunci public = (e,N) = (17,1081)

9. Tentukan kunci yang akan dienkripsi, dalam hal yang akan dienkripsi adalah kunci *Hill Cipher* $\begin{bmatrix}3 & 6\\1 & 5\end{bmatrix}$ yang merupakan masukan untuk Algoritma Asimetris RSA

   Enkripsi kunci *Hill Cipher*:

   $\begin{bmatrix}3 & 6\\1 & 5\end{bmatrix}$

10. Enkripsi kunci Hill dengan rumus :

    C = m^e mod N, sehingga

    m=3; C = m^e mod N
    = 3^{17} mod 1081
    = 660

    m=6; C = m^e mod N
    = 6^{17} mod 1081
    = 495

m=1 C = m^e mod N
= 1^{17} mod 1081
= **1**

m=5; C = m^e mod N
= 5^{17} mod 1081
= **38**

Sehingga hasil enkripsi kunci *Hill Cipher* :

$$\begin{bmatrix} 660 & 495 \\ 1 & 38 \end{bmatrix}$$

11. Kirim kunci *Hill Cipher* C ke penerima

12. Terima kunci *Hill Cipher* C dari pengirim

Dekripsi kunci *Hill Cipher* :

13. Dekripsi hasil enkripsi kunci *Hill Cipher* dengan rumus :

m = C^d mod N, sehingga

m = C^d mon N
= 660^{893} mod 1081
= **3**

m = C^d mon N
= 495^{893} mod 1081
= **6**

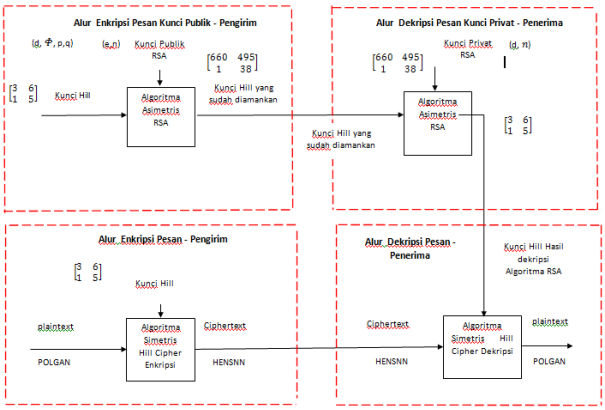
m = C^d mon N
= 1^{893} mod 1081
= **1**

m = C^d mon N
= 38^{893} mod 1081
= **5**

Jadi hasil dekripsi kunci penerima RSA adalah

$$\begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}$$

Sehingga setelah dilakukan perhitungan pada proses enkripsi dan dekripsi pada kombinasi Algoritma *Hill Cipher* dan *RSA* dapat dipetakan pada diagram skema seperti gambar 3.2.



Gambar 3.2.Hasil perhitungan kombinasi algoritma *Hill Cipher* dan RSA

V. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan pembahasan dari bab-bab terdahulu, maka dapat ditarik kesimpulan sebagai berikut :

1. Untuk memperkuat kriptografi bisa dilakukan dengan menggunakan metode *hibrid crytpsystem* dalam hal ini menggunakan Hill Cipher contoh dari kriptografi simetris dan RSA contoh dari kriptografi asimetris

2. Algoritma Hill Cipher dan RSA dapat dikombinasi sehingga nantinya dari kombinasi akan menghasilkan algoritma yang mempunyai tingkat kesulitan pengamanan data yang tinggi dan cepat dalam proses enkripsi maupun dekripsi

5.2. Saran

Berikut adalah saran-saran untuk pengembangan lebih lanjut terhadap penelitian ini :

1. Untuk pengembangan perlu dilanjutkan penelitian ini dengan melakukan pengamanan pada file
2. Untuk pengembangan pengamanan kunci Hill Cipher perlu dilanjutkan penelitian ini dengan membuat semua ordo matrik sehingga pengamanan lebih baik lagi
3. Hasil perancangan ini sebaiknya diterapkan dalam program sehingga akan bisa dilihat hasil pada proses enkripsi dan dekripsinya

DAFTAR PUSTAKA

[1] Ariyus, D, *"Pengatar Ilmu Kriptografi, Teori, Analisis Dan Implementasi"*, CV Andi Perbuanan, Yogyakarta, 2008
[2] Kromodimoeljo, S, , *Teori & Aplikasi Kriptografi*, SPK IT Consulting, 2010
[3] Mollin, R, "*An Introduction to Cryptography"*, Taylor & Francis Group, 2007
[4] Munir, R, "*Kriptografi"*. Penerbit Informatika, Bandung, 2006,
[5] Sadikin, R. "*Kriptografi untuk Keamanan Jaringan"*, CV Andi Offset, Yogyakarta, 2012
[6] Rahman M.N.A, Abidin A.F.A, Yusof MK & Usop N.S.M. 2013. Cryptografi : A new approach of classical Hill Cipher. *International Journal of Security and its Applications* **7**(2) : 179-190
[7] Ravindra K.G. & Parvinder S.. A new way to design and implementation of hybrid cryptosystem for security of the information in public network. *International Journal of Emerging Technology and Advanced Engineering*. **3**(8) : 108-115, 2013
[8] Schneier, B., *Applied Cryptography : Protocols, Algorithms, and Source Code in C*, 2nd Edition John Wiley & Sons Inc, 1996