Semantika
Seminar Nasional Teknologi Informatika

Implementasi Algoritma RSA dengan Kunci *EM2B* dalam Mengenkripsi Pesan

Elwinus H. A. Mendrofa
Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara
elwin_mendrofa@students.usu.ac.id

Elwin Yunith Purba
Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara
elwinpurba.manorsa@gmail.com

Muhammad Zarlis
Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara
m.zarlis@usu.ac.id

Abstrak

Canggihnya teknologi membuat manusia semakin ketinggalan dalam mengikuti perkembangan zaman. Pekerjaan yang serba cepat menjadi cirikhas manusia yang menerapkan teknologi dalam setiap usahanya. Namun ketergantungan manusia terhadap teknologi menjadi ancaman bila tidak disertai pengetahuan serta kehati-hatian. Ketergantungan manusia dalam menggunakan jaringan internet untuk bertukar informasi harus lebih diperhatikan. Saat ini telah banyak terjadi pencurian data atau informasi yang mengakibatkan kerugian besar. Salah satu upaya mengatasi hal ini perlu ditingkatkan sistem keamanan data pada jaringan komputer. RSA merupakan algoritma kriptografi modren yang sering digunakan untuk pengamanan data, sampai saat ini masih belum ada yang bisa memecahkannya. Para peneliti masih terus mengembangkan algoritma ini karena belum mampu mengenkripsi plainteks yang panjang sehingga RSA hanya digunakan untuk mengenkripsi kunci simetri. Berbeda dengan algoritma lainnya proses enkripsi dan dekripsi RSA sangat lambat dibandingkan algoritma lainnya. Kolaborasi algoritma RSA dengan Kunci EM2B memberikan keamanan yang kuat pada pesan serta mampu mengatasi masalah waktu eksekusi enkripsi dan dekripsi.

Kata kunci ***:Kriptografi, RSA, EM2B, Enkripsi, Dekripsi***

I. LATAR BELAKANG

Media teknologi masih menjadi pusat perhatian hingga saat ini. Hampir semua jenis pekerjaan dan kegiatan manusia di dalamnya terdapat peran teknologi. Manfaat yang bisa diperoleh dari canggihnya sebuah teknologi membuat manusia

tergesa-gesa untuk segera memiliki dan menguasai tekonologi yang sesuai dengan bidang dan kebutuhannya.

Dari sekian banyaknya keuntungan yang diperoleh dari penggunan teknologi, tidak sedikit pula peluang kerugian yang terkandung di dalamnya baik itu kerugian kecil maupun kerugian besar bahkan dapat mengakibatkan seseorang kehilangan segalanya. Beberapa bentuk kerugian akibat kelalaian dalam mengendalikan teknologi antara lain, kerusakan data, ketidak tersediaan data pada saat dibutuhkan, serta kurangnya sistem keamanan yang mengakibatkan data hilang atau dicuri, dan beberapa fator yang lainnya. Kurangnya system keamanan menjadi faktor masalah yang paling banyak ditemukan hingga saat ini. Beberapa individu hingga lembaga pemerintahan pernah mengklaim bahwa adanya interfensi pihak ketiga yang berusaha menyalah gunakan informasi tersebut. Direktur Utama BRI Suprajarto memaparkan beberapa kasus penipuan yang dialami oleh bank yang dipimpinnya. Dari mulai *skimming* atau pencurian data ATM nasabah hingga modus pencurian akun email untuk penyalah gunaan fasilitas *internet banking (sumber:* http://bisniskeuangan.kompas.com/read/2017/04/04/070000026/pencurian.data.nasabah.potret.carut-marut.perbankan. Beberapa contoh kasus lainnya peretasan pada tahun 2016 yang lalu antara lain Ransomware emerges sebagai sebuah ancaman Cyber tertinggi di bidang bisnis, UK sebagai peringkat ke dua, dan 412 juta pengguna account terpapar oleh ancaman cyber ini, termasuk keamanan dari data Bank dan Rumah Sakit. Kasus ini diakibatkan oleh lemahnya system keamanan data mereka. Untuk itu diperlukan sebuah system keamanan komputer. Keamanan data pada computer sangat penting sekali untuk memproteksi data dari pihak-pihak yang tidak berhak untuk memeriksa data yang ada pada computer mereka [1]. Hal ini menandakan bahwa keamanan data yang dimiliki oleh suatu perusahaan ataupun pribadi masih sangat lemah sampai saat ini. Keamanan data berhubungan dengan daerah yang berisiko tinggi seperti data yang ada pada Server atau Harddisk [2]. NIST Computer Security Handbook [NIST95] mendefinisikan istilah keamanan komputer sebagai berikut: Perlindungan yang diberikan pada sistem informasi otomatis untuk mencapai tujuan yang sesuai untuk menjaga integritas, ketersediaan, dan kerahasiaan sumber daya sistem informasi (termasuk perangkat keras, perangkat lunak, Firmware, informasi / data, dan telekomunikasi) [3].

Informasi merupakan hal yang sangat penting untuk menjaga kelangsungan dan kestabilan suatu kegiatan. Keamanan informasi juga berupaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [4]. Kurangnya pengamanan sebuah informasi dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pola serangan yang dilakukan untuk mencuri informasi sangat bervariasi ada yang memanfaatkan kelalaian pengguna yang sah hingga melakukan pemaksaan untuk masuk ke dalam sistem informasi itu sendiri.

Pencurian informasi sering terjadi pada saat pengiriman pesan. Adanya orang ketiga yang berupaya untuk mengetahui informasi dari sipengirim ke penerima pesan. *Pelaku yang berusaha untuk mendapatkan informasi tanpa diketahui oleh pengirim pesan disebut sebagai Man in the Middle.* Pelaku bertujuan untuk memperoleh informasi guna mendapatkan keuntungan dengan menyalah gunakan informasi tersebut. Upaya lainnya, pelaku mengubah informasi yang diperoleh dari si pengirim pesan, kemudian dikirimkan kembali kepada penerima pesan, dengan tujuan agar informasi yang disampaikan tidak sesuai dengan maksud dari si pengirim pesan. Hal ini terjadi karena tidak adanya autentikasi dari penerima pesan untuk mengetahui apakah pesan tersebut dikirim oleh pengirim yang sebenarnya. Demikian halnya si pengirim pesan merasa bahwa pesan yang dikirim telah disampaikan dengan baik. Akibatnya bisa mengakibatkan hal-hal yang tidak diinginkan oleh kedua belah pihak.

Penanganan masalah seperti ini telah banyak detemukan oleh peneliti sebelumnya. Mereka bertujuan untuk mencegah terjadinya masalah-masalah tersebut agar data atau informasi yang dikirim melalui jaringan internet dapat diamankan dari pihak yang tidak bertanggung jawab. Salah satu cara yang dapat dilakukan untuk mengatasi masalah tersebut yaitu dengan melakukan enkripsi terhadap pesan atau informasi menggunakan algoritma kriptografi.

Saat ini algoritma kriptografi klasik maupun algoritma modren masih banyak dikembangkan oleh para ilmuan, hal ini disebabkan karena masih sangat sulit untuk dipecahkan. Salah satu diantaranya adalah algoritma RSA. Algoritma RSA

merupakan algoritma enkripsi yang memiliki kunci yang sangat dimana hingga saat ini masih belum ditemukan cara untuk memecahkannya. Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi factor-faktor prima pada saat membangkitkan kuncinya. Semakin banyak digit bilangan yang digunakan untuk menghasilkan kunci maka semakin sulit untuk mencari factor bilangan prima yang membangkitkan kunci tersebut. *Disamping beberapa keunggulan yang dimiliki oleh algoritma RSA, terdapat sedikit kekurangan dalam mengenkripsi pesan. RSA lebih lambat dari pada algoritma kriptografi lainnya. Dalam prakteknya, RSA tidak digunakan untuk mengenkripsi pesan tetapi mengenkripsi kunci simetri dengan kunci public penerima pesan*.

Untuk meningkatkan efektifitas dan efisiensi algoritma RSA ini, penelitian menerapkan algoritma kunci simetri yang disebut dengan algoritma Kunci EM2B. Algoritma Kunci EM2B berfungsi untuk mengenkripsi pesan dengan cara mengubah kunci asli kedalam kunci rahasia. Jika pesan lebih panjang dari kunci maka algoritma ini memberikan solusi dengan menambahkan metode *increament* pada indeks kunci hingga panjang karakter kunci tersebut sama dengan panjang karakter pesan.

Dari hasil penelitian ini diharapkan upaya penyalahgunaan pesan atau informasi dapat dihindari serta dapat meningkatkan kerahasiaan pesan yang tersimpan di dalam jaringan komputer maupun pada saat pengiriman pesan. Autentikasi pesan juga menjadi tujuan berikutnya dari penelitian ini, penerima pesan mampu mengidentifikasi keaslian pesan yang diterima dengan cara mengetahui pesan asli yang diperoleh dari hasil dekripsi melalui kunci yang telah disepakati sebelumnya. Pengirim pesan juga tidak dapat menyangkal bahwa pesan yang dia kirim pesan kepada pihak penerima pesan adalah benar.

II. TINJAUAN PUSTAKA

Ilmu kriptografi memiliki peran penting dalam menjaga kerahasiaan informasi baik yang ada di dalam komputer maupun pada saat melakukan transaksi data. Jadi tujuan kriptograpi adalah untuk membuat para hacker bekerja lebih keras untuk mencuri atau merusak data dari orang yang berhak terhadap suatu data [5].

Kriptografi adalah teknik yang diterapkan untuk enkripsi dan dekripsi [4]. Di bidang kriptografi ada beberapa teknik yang tersedia untuk enkripsi/dekripsi. Teknik ini umumnya dapat dikelompokkan menjadi dua kelompok besar, yaitu Kriptografi kunci konvensional dan publik [6]. Beberapa istilah dasar yang digunakan dalam kriptografi dibahas seperti di bawah ini :

a. Plainteks

Dalam kriptografi, plaintext adalah teks sederhana yang mudah dibaca sebelum dienkripsi menjadi ciphertext [7]. Data bisa dibaca dan dipahami tanpa ada ukuran khusus yang disebut plaintext [8].

b. Ciperteks

Dalam Kriptografi, transformasi pesan asli menjadi pesan yang tidak dapat dibaca sebelum transmisi dikenal sebagai teks sandi [9]. Ciperteks ini adalah pesan yang diperoleh dengan semacam operasi enkripsi pada teks biasa.

c. Enkripsi

Enkripsi adalah proses mengubah teks biasa menjadi teks sandi. Proses enkripsi memerlukan algoritma enkripsi dan kunci untuk mengubah teks biasa menjadi ciperteks [10]. Pada enkripsi kriptografi dilakukan pada pengirim terakhir.

d. Dekripsi

Dekripsi adalah proses kebalikan dari enkripsi.Dekripsi mengubah teks sandi menjadi teks biasa. Dalam dekripsi kriptografi dilakukan pada penerima akhir [11].

e. Kunci

Kunci adalah teks numerik atau alfanumerik yang digunakan untuk enkripsi teks biasa dan dekripsi teks sandi [12].

Untuk menentukan algoritma Kriptografi yang akan digunakan dalam sistem keamanan data selain pertimbangan kekuatan terhadap serangan Cryptanalis dan *Bruteforce* yang tidak kalah penting adalah pertimbangan kecepatan. Pada saat ini terdapat berbagai macam algoritma Kriptografi simetri maupun asimetri. Jika suatu algoritma Kriptografi dipercaya kuat namun diketahui lamba dalam proses penyandiannya maka tidak akan dijadikan pilihan oleh pengguna. Pertimbangan kecepatan ini akan menjadi lebih diutamakan lagi jika pemakaian algoritma Kriptografi menyangkut jaringan komputer terutama pada arsitektur clien-server [13].

RSA merupakan salah satu algoritma kriptografi modern yang hingga saat ini masih banyak dikembangkan oleh para peneliti. Algortima RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun

1976 . Nama RSA merupakan singkatan dari nama tiga orang penemunya, yaitu Rivest, Shamir, dan Adleman. Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat [14].
Algoritma RSA memiliki besaran-besaran sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. $n = p \times q$ (tidak rahasia)
3. $\varphi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
   Syarat: PBB(e, $\varphi(n)$) = 1
5. d (kunci dekripsi) (rahasia)
   d dihitung dari $d \equiv e^{-1} \bmod (\varphi(n))$
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Pembangkitan kunci :

1. Pilih dua bilangan prima, a dan b (rahasia)
2. Hitung $n = a\,b$.
   Besaran n tidak perlu dirahasiakan.
3. Hitung $\varphi(n) = (a-1)(b-1)$.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relatif prima terhadap $\varphi(n)$.
5. Hitung kunci dekripsi, d, melalui $ed \equiv 1 \pmod{m}$ atau $d \equiv e^{-1} \bmod (\varphi(n))$

Hasil dari algoritma di atas:

1. Kunci publik adalah pasangan (e, n)
2. Kunci privat adalah pasangan (d, n)

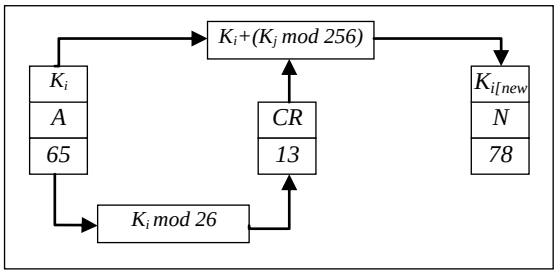
Algoritma kunci *EM2B* adalah sebuah algoritma yang berfungsi mengubah kunci utama menjadi kunci baru yang diubah kedalam karakter ASCII. EM2B merupakan inisial nama dari penemu algoritma ini *(Elwin Mendrofa, Elwin Manorsa, dan Boy Siahaan)* yang ditemukan pada tahun 2017. Algoritmna EM2B mengembangkan algoritma pembangkit kunci sederhana untuk mengenkripsi plainteks namun masih tertarik menggunakan kombinasi algoritma Vigenere Cipher. Sistem modulus dari penjumlahan plainteks dengan kunci menjadi sebuah keuntungan dalam kecepatan proses enkripsi. Algoritma EM2B juga memiliki algoritma *increment key* yang berfungsi jika panjang kunci lebih kecil dari panjang plainteks. *Increament key* merupakan metode untuk menambahkan panjang karakter kunci dengan menjumlahkan dua karakter kunci sebelumnya dan dimoduluskan dengan 256 berbasis huruf ASCII.

Algoritma EM2B memiliki persamaan sebagai berikut:

$$K_{i[new]} = K_i + (K_j \bmod 26) \bmod 256$$

Ket:

1. K_i = kunci utama
2. K_j = kunci utama mod 26
2. $K_{i[new]}$ = kunci baru yang dihasilkan



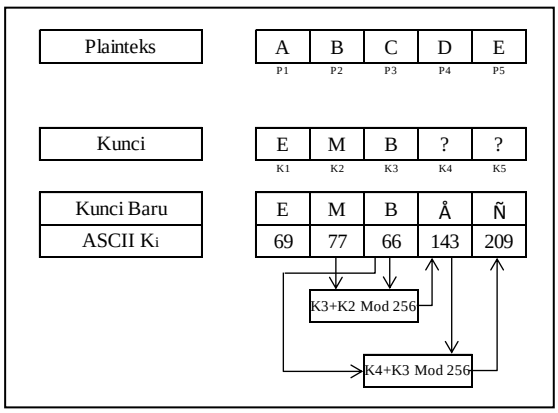
Gambar 1. Proses Algoritma EM2B

Sedangkan untuk algoritma *icreament key*:

$$IncK_i = K_{i[max]} + K_{i[max]-1} \bmod 256$$

Ket:

1. $K_{i[max]}$ = indeks kunci terakhir dalam ASCII
2. $IncK_i$ = increament kunci



Gambar 2. Proses *Increament Key*

Algoritma pendukung lainya adalah Vigener Chipher. Algoritma enkripsi jenis ini sangat

dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan ciphertext bisa dilakukan menggunakan substitusi angka maupun bujursangkar vigènere [15]. Karakter huruf yang digunakan pada *vigenere cipher* yaitu A, B, C, ..., Z dan disamakan dengan angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci secara berulang. Penulisan kunci secara berulang dilakukan hingga setiap karakter pada pesan memiliki pasangan sebuah karakter dari kunci. Selanjutnya karakter pada pesan dienkripsi menggunakan metode *caesar cipher* dengan nilai kunci yang telah dipasangkan dengan angka [16]. Proses enkripsi dapat dihitung dengan persamaan berikut [17] :

$$Ei=(Pi+Ki)\ mod\ 26$$

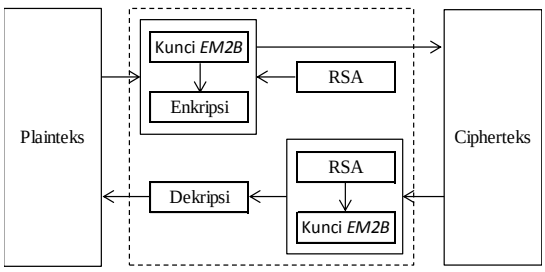
dimana Ei, Pi dan Ki merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Sedangkan proses dekripsi dapat menggunakan persamaan berikut :

$$Di=(Ci-Ki)\ mod\ 26$$

dengan Di adalah karakter hasil dekripsi, Ci adalah karakter *cipher text* atau sandi, Ki adalah karakter kunci.

III. METODE PENELITIAN

Delam merancang algoritma kriptografi, dibutuhkan sebuah ketelitian yang akurat. Tingkat keamanan menjadi kunci utama keberhasilan dari algoritma kriptografi itu sendiri. Efesiensi waktu juga perlu dipertimbangkan sebab jika proses enkripsi dan dekripsi membutuhkan waktu yang lama, akan berdampak buruk untuk mengenkripsi pesan dalam skala besar. Secara garis besar proses enkripsi dan dekripsi pada implementasi algoritma RSA dan Algoritma Kunci EM2B dalam mengenkripsi pesan dapat diamati melalui blog diagram berikut.



Gambar 3. Proses Enkripsi dan Dekripsi

Dalam penelitian ini digunakan Algoritma Kriptografi RSA dan Kunci EM2B untuk meningkatkan keamanan pesan yang telah dienkripsi. Hal ini diharapkan Kunci EM2B dapat menjadi algoritma kunci untuk mengenkripsi plainteks serta kemampuan algoritma RSA dalam mengenkripsi kunci akan menjadikan pesan sangat sulit untuk dipecahkan.

Untuk itu perlu dilakukan analisis pada masing-masing algoritma baik RSA maupun kunci EM2B yang digunakan dalam mengenkripsi pesan.

Algoritma RSA dapat dilihat sebagai berikut:

1. Ambil secara random dua bilangan prima p dan q yang besar dan berbeda, namun ukuran keduanya (jumlah digit dalam basis bilangan yang digunakan) harus sama.
2. Hitung modulus n dan fungsi Euler's Totient φ (n) dengan rumus : n = p q
   φ (n)=(p −1)[q −1]
   dengan :
   n = modulus (*public key*)
   p dan q = dua bilangan prima yang dimunculkan secara random.
3. Pilih suatu bilangan integer *e* sedemikian hingga I<e<φ (n) dan gcd(e,φ (n)) =1
   dengan :
   I = bilangan integer
   e = *public key* (kunci enkripsi)
   gcd = persekutuan pembagi terbesar (*greatest common divisor*)
4. Hitung nilai integer d dimana I < d <φ (n) sedemikian hingga
   d = e−1modφ (n) atau ed = I(modφ (n))
   dengan :
   d = *private key* (kunci dekripsi)
5. Membangun tabel untuk mempresentasikan tiap karakter.
6. Plainteks (teks yang akan dienkripsi) disandikan dengan angka-angka sesua dengan tabel yang terbentuk oleh proses 5 dan akan diperoleh suatu nilai *M* yang merupakan kumpulan angka-angka dari plaintext, kemudian kumpulan angka-angka tersebut diblok tiap 4 angka menjadi $m_1, m_2, \ldots, m_n$. Proses enkripsi dilakukan per blok dan masing-masing blok rumus enkripsinya adalah:
   $c_1 = m_1^e \pmod n$, $c_2 = m_2^e \pmod n$, … , dst
   sehingga menghasilkan nilai *C* dimana *C* merupakan kumpulan angka-angka dari $c_1, c_2, \ldots, c_n$.

7. Proses dekripsi dilakukan dengan menggunakan logika seperti langkah 6 dengan melakukan perhitungan terbalik, yaitu $m_1 = c_1^d \pmod n$, $m_2 = c_2^d \pmod n$, … ,dst, sehingga menghasilkan nilai M dimana M = m_1, m_2, m_3 Nilai akhir M tersebut dipresentasikan balik dengan table yang dibangun seperti pada proses 5 di atas.

Untuk meningkatkan kemanan algoritma RSA, maka ditentukan kunci pengaman berupa sandi *private key*, *public key* dan *modulo* yang di hasilkan dari dua buah bilangan prima. Kunci ini yang nanti akan terus digunakan oleh pengirim dan penerima pesan dalam mengenkripsi dan mendekripsi pesan. Apabila sandi kunci pengaman oleh pemilik sistem dirasa sudah tidak aman, maka kedua pihak segera menginformasikannya untuk segeri diubah. Tampilan kunci pengaman ini terdiri dari :

Analisa algoritma EM2B sebagai berikut:

1. Tentukan beberapa kata yang digunakan sebagai kunci utama untuk mengenkripsi pesan, Kunci diberi lambang dengan K_i dimana, $K_i = K_1, K_2, \dots, K_n$.
2. Kunci tersebut di konversi kedalam bilanga ASCII desimal.
3. Tentukan nilai modulus 26 dari masing-masing karakter kunci yang telah diubah ke dalam desimal. $K_j = K_i$ Mod 26.
4. Jumlahkan K_i dengan K_j kemudian dimodulasikan dengan 256 dan menghasilkan kunci baru ($K_{i[new])}$ yang diubah dalam karakter ASCCI desimal.

Dalam algoritma EM2B, kunci yang kita pilih tidak harsu memilik panjang karakter yang sama dengan plainteks. Plainteks boleh saja terdiri dari beberapa kalimat bahkan paragraf. Kunci akan menyesuaikan panjang karakternya dengan plainteks denga menggunakan algoritma *increament key* yang telah tersimpan di dalamnya. Analasisa kenerja dari algoritma increament key ini dapa diperhatikan dibawah ini.

1. Indeks karakter maksimal dijumlahkan dengan indeks karakter sebelumnya ($K_{i[max]} - K_{i[max-1]}$) dan menghasilkan indek karakter kunci yang baru ($K_{i[new]}$).
2. Indeks kunci baru ($K_{i[new]}$) menjadi indeks kunci maksimal, kemudia ditambahkan lagi dengan indeks kunci sebelumnya.
3. Langkah perulangan ini akan berhenti apabila indeks maksimum kunci sama dengan dengan indeks maksimum plainteks. $K_{i[max]} = P_{i[max]}$

Proses implementasi algoritma RSA dan EM2B dalam mengenkripsi pesan dapat dapat dijelaskan dengan tahap-tahap berikut ini.

1. Sebuah pesan atau plainteks dienkripsi dengan menggunakan sebuah kunci.
2. Terlebih dahulu kunci diubah kedalam EM2B kemudia menghasilkan karaker ASCII yang baru.

$$K_{i[new]} = K_i + (K_j \ mod \ 26) \ mod \ 256$$

3. Jika panjang kunci masih lebih kecil dari panjang plainteks, maka kunci di proses dengan *increament key*

$$IncK_i = K_{i[max]} + K_{i[max]-1} \ mod \ 256$$

4. Selanjutnya melakukan enkripsi dimana, setiap plainteks di tambahakan dengan kunci dan dimodulasi dengan 256 untuk menghasilkan sebuah ciphertext. $C_i = P_i + K_i \ mod \ 256$. Cipherteks dalam proses merupakan pesan yang akan dikirimkan kepada sipenerima.
5. Kemudian nilai kunci utama tersebut disatukan menjadi satu blok kemudian dipisah-pisah menjadi beberapa blok. Nilai tiap blok tidak lebih besar dari nilai n pada pembangkit kunci RSA.
6. Setelah proses blok dilakukan kemudian diekripsi dengan menggunakan RSA. $E_k = M^e \bmod n$. E_k adalah hasil enkripsi dari K_i
7. Informasi yang dikirimkan ke sipenerima adalah cipherteks ($C_{i)}$, dan asil enkripsi kunci (E_k).

Selanjutnya berikut proses untuk dekripsi pesan .

1. Tahap pertama dengan mendekripsi kunci menggunakan rumus $K_i = D_k = M^d \bmod n$.
2. Hasil dekripsi tersebut dipisahkan menjadi masing-masing dua digit bilang, dimana akan menghasilkan karakter kunci utama.
3. Kunci utama tersebut diproses kembali kedalam algoritma EM2B untuk menghasilkan kunci baru dalam bilangan ASCII desimal.
4. Digunakan kembali algritma *increament key* untuk memperoleh panjang kunci sama dengan plainteks.

5. Setelah itu cipherteks di dekripsi dengan menggunakan kunci baru tersebut, dengan menggunakan persamaan P = C - K mod 256.

IV. HASIL DAN PEMBAHASAN

Hasil yang ditawarkan pada penelitian ini berupa metode untuk meningkatkan keamanan pesan dari pihak yang tidak bertanggung jawab.Penelitian inimemberikan contoh sebuahproses enkripsi dan dekripsi.Plainteks yang digunakan adalah "HALLOWORLD" dengan kunci utama "BRO" seperti pada gambar berikut ini.

Plainteks	H	A	L	L	O	W	O	R	L	D
ASCII	72	65	76	76	79	87	79	82	76	68

Kunci EM2B & Inc Kunci										
Kunci	B	R	O							
ASCII	66	82	79							
Ki MOD 26	14	4	1							
Ki+Ki MOD 26	80	86	80	166	246	157	148	50	198	248
Inc Kunci	P	V	P	ª	÷	Ø	ö	2	ã	°

Enkripsi dengan EM2B										
P + K Mod 256	152	151	156	242	69	244	227	132	18	60
Cipherteks	ÿ	ù	£	_	E	¶	Ò	ä	DC2	<

Gambar 4. Proses Enkripsi Kunci EM2B

Plainteks diubah ke dalam desimal. Kemudia kunci diproses ke dengan EM2B menjadi karakter (P, V, P) dan panjang kunci bertambah dengan menggunakan increament key. Kunci yang dihasilkan berupa karakter ASCII. Kunci baru: (PVPª÷Øö2ã°)

Tahapan berikutnya adalah dengan mengenkripsi plaintek dengan kunci baru yang telah dihasilkan sebelumnya. Cipherteks yang dihasilkan antara lain: (ÿù£_E¶ÒäDC2<)

Selanjutnya proses pembuatan kunci RSA dengan mengikuti langkah-langkah di bawah ini:
- Tentukan nilai p dan q; p & q bilangan prima
- Tentukan p x q untuk menghasilkan nilai n
- Tentukan nilai phi(n) = (p-1)*(q-1)
- Tentukan nilai e sebagai kunci enkripsi, e relative prima 1 < e <phi(n)
- Hitung nilai d sebagai kunci dekripsi.

Pembuatan Kunci					
p	q	n	$\varphi(n)$	e	d
7	17	119	96	13	37

Gambar 5. Pembuatan Kunci Dalam penentuan kunci

Penentuan Nilai (e)						
φ(n)	96	48	24	12	37	3,36
Prima	2	2	2	2	11	11
Hasil	48	24	12	6	3,36	STOP

Gambar 6. Pehitungan Nilai e

Perhitungan Nilai (d)										
Indeks	1	2	3	4	5	6	7	8	9	10
a =	1	0	1	-2	3	-5				
b =	0	1	-7	15	-22	37				
d =	96	13	5	3	2	1				
k =	-	7	2	1	1	2				

Gambar 7. Perhitungan Nilai d

Dari proses ini kita menemukan nilai kunci untuk mengenkripsi pesan pada RSA adalah e = 13 dan kunci dekripsi adalah d = 37.

.

Manipulasi Panjang Kunci EM2B									
Panjang K	unci Utam	668279							
		M1	M2	M3	M3	M4	M5	M6	
6	668279	66	82	79					

Enkripsi kunci *EM2B dengan RSA*							
P^e Mod n	87	5	58	61	93	67	4
Cipherteks	W	ENC	:	=	]	C	EOT

Gambar 8. Enkripsi Kunci dengan RSA

Cipherteks diatas merupakan sebuah informasi atau pesan yang diperoleh dari gabungan beberapa algoritma serta implementasinya dalam mengankan informasi.

Untuk mendekripsi pesan diperoleh hasil pengujian sebagai beriku.

Cipherteks	W	ENQ	:	=	]	C	EOT
ASCII	87	5	58	61	93	67	4

Dekripsi kunci *EM2B dengan RSA*							
Mi-n	M1	M2	M3	M3	M4	M5	M6
C^d mod 119	66	82	79	40	09	67	4
Gabung Ci	6682794009674						
Panjang Key	68279						
K.EM2B	66	82	79				
Kunci	B	R	O				

Gambar 9. Proses Dekripsi Kunci dengan menggunakan algoritma RSA

Kunci EM2B & Inc Kunci										
Kunci	B	R	O							
ASCII	66	82	79							
ASCII INC	66	82	79	161	240	146	131	22	153	175
Inc Kunci	B	R	O	í	-	Æ	â	SYN	Ö	»

Gambar 10. Dekripsi Algoritma Kunci EM2B

Dekripsi menggunakan Kunci EM2B										
Cipherteks	ÿ	ù	£	_	E	¶	Ò	ä	DC2	<
P - K Mod 256	152	151	156	242	69	244	227	132	18	60
Plainteks	H	A	L	L	O	W	O	R	L	D
ASCII	72	65	76	76	79	87	79	82	76	68

Gambar 11. Dekripsi Cipherteks dengan Algoritma EM2B.

V. KESIMPULAN

Berdasarkan hasil dari pembahasan di atas, maka dapat disimpulkan bahwa: Aplikasi pengamanan data menggunakan algoritma *RSA* mempunyai dua teknik pembacaan yaitu teknik enkripsi (mengubah *file* asli menjadi *file* yang tidak dapat dibaca) dan teknik dekripsi (mengubah *file* yang tidak dapat dibaca menjadi *file* asli). Aplikasi pengamanan mempunyai kalimat sandi / *passphare* yang harus diingat dan bersifat sensitif, maksudnya huruf besar dan kecil dibedakan,agar*passphare* sulit ditebak oleh siapapun.

DAFTAR PUSTAKA

[1] Zaeniah, Bambang Eka Purnama, "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm", *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, 2015*

[5] C. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278-0661, 2012.

[3] Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri, "An Introduction to Information Security", National Institute of Standards and Technology Special Publication 800-12 Revision 1, 2017.

[4] William Stallings, "Cryptography and Network Security: Principles& Practices", Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010.

[5] Aized Amin Soofi, Irfan Riaz, Umair Rasheed, "An Enhanced Vigenere Cipher For Data Security", International Journal Of Scientific & Technology Research Volume 5, Issue 03, March 2016, ISSN:22778616

[6] Sundram Prabhadevi, 2rahul De, 2pratik Shah, "Cost Effective Poly Vernam Cipher With Cache Optimization", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, 2013.

[7] M. Rouse. (2007, Plain text. Available: http://searchsecurity.techtarget.com/definition/plaintext.

[8] T. Gunasundari and K. Elangovan, "A ComparativeSurvey on Symmetric Key Encryption Algorithms,"International Journal of Computer Science and Mobile Applications, ISSN, pp. 2321-8363, 2014.

[9] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," International Journal on Computer Science and Engineering (IJCSE), vol. 4, pp. 877-882, 2012.

[10] V. Beal. (2009, Encryption. Available: http://www.webopedia.com/TERM/E/encryption.html

[11] Fresly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana. *Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*.Samarinda. 2015.

[12] Arya Reza Nugraha dan Ary Mazharuddin S, *Penyembunyian Pesan Rahasia yang Terenkripsi Menggunakan Algoritma RSA pada Media Kompresi*. Surabaya,2013.

[13] K Hashizume et al., "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[14] Muhammad Arief, Fitriyani, Nurul Ikhsan, "*Kriptografi Rsa Pada Aplikasi File Transfer Client- Server Based",* Jurnal Ilmiah Teknolog informasi Terapan Volume I, No 3, 10 Agustus 2015, ISSN : *2407 – 3911*

[15] Ahmad Rosyadi, Jurusan Teknik Elektro, Universitas Diponegoro Semarang, "Implementasi Algoritma Kriptografi AES Untuk Enkripsi dan Dekripsi Email", Transient, vol. 1, no. 3, September 2012, ISSN: 2302-9927,64

[16] Katz, J. and Y. Lindell. 2015. *Introduction to Modern Cryptography*. 2nd ed. CRC Press. Boca Raton.

[17] Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice*. 5th ed. Pearson Education Inc. New York.

[18] Andi Riski Alvianto dan Darmaji.*Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android*. Surabaya. 2015.

[19] Megah Mulya. *Perbandingan Kecepatan Algoritma Kriptografi Asimetri*. Palembang. 2013.

[20] Zainal Arifin. *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*.Samarinda. 2009.