Jurnal Nasional Informatika dan Teknologi Jaringan
E-ISSN : 2540-7600
P-ISSN : 2540-7597

KOMBINASI ALGORITMA CAESAR CIPHER DAN ALGORITMA RSA UNTUK PENGAMANAN FILE DOKUMEN DAN PESAN TEKS

Indra Gunawan
STIKOM Tunas Bangsa Pematangsiantar
Jl. Jend. Sudirman Blok A, No. 1, 2 dan 3. Kode Pose : 21127
indra@amiktunasbangsa.ac.id

Abstrak - Pada saat sekarang ini, kemajuan teknologi dibidang ilmu komputer dan telekomunikasi sangatlah berkembang dan maju dengan pesat. Pengamanan data merupakan hal yang sangat penting untuk menjaga isi data yang penting dari pihak-pihak yang dapat merugikan dengan cara merusak data-data penting dari pemilik data. Dengan meningkatkan keamanan data menggunakan kombinasi algoritma, dapat menjaga keamanan data lebih terjamin dari serangan-serangan yang dapat membahayakan isi dari data yang tersimpan, terutama data dalam bentuk berkas dokumen dan pesan teks. Kombinasi algoritma yang digunakan untuk pengamanan data yang digunakan yaitu algoritma caesar cipher dan algoritma RSA. Jadi dengan menggunakan kombinasi algotitma caesar cipher dan algoritma RSA, tingkat pengamanan file dokumen dan pesan teks bisa lebih terjaga keaslian datanya.

Kata kunci **: pengaman data, kombinasi algoritma, caesar cipher, rsa**

I. PENDAHULUAN

Masalah dalam pengamanan data masih merupanan suatu aspek penting didalam penjagaan penyimpanan data, terutama data yang tersimpan dalam bentuk digital. Hal ini disebabkan karena kemajuan yang sangat pesata didalam bidang ilmu komputer dengan konsep *open-system* yang sudah banyak digunakan, sehingga hal ini dapat memudahkan seseorang untuk melakukan perusakan data terutama data yang tersimpan dalam bentuk digital tanpa harus diketahui oleh pihak penyimpan data. Oleh karena itu dibutuhkan pengelolaan kemaanan data digital dengan mengkombinasi 2 (dua) buah algoritma, yaitu algoritma caesar cipher dan algoritma rsa untuk meningkatkan tingkat keamanan file dokumen dan pesan teks.

Caesar cipher merupakan salah satu algoritma tertua dan merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Kelemahan caesar cipher adalah kita biasa memproleh pesan asli dengan memanfaatkan
metode *brute force* dan presentasi frekuensi huruf yang paling sering muncul dalam suatu kalimat[1].

Algoritma caesar cipher yaitu algoritma dengan mengganti posisi huruf awal dengan alphabet atau disebut dengan algoritma ROT3. Algoritma transposisi yaitu dengan cara mengubah letak dari teks pesan yang akan disandikan dengan menggunakan bentuk tertentu[10].

Dari sekian banyak algoritma kriptografi dengan kunci-publik yang pernah dibuat, algoritma yang paling populer adalah algoritma rsa. Algoritma rsa yang dibuat oleh Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1976. Keamanan algoritma rsa terletak pada sulitnya untuk memfaktorkan bilangan prima yang relatif lebih besar. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama bilangan pemfaktoran prima yang besar besar belum ditemukan algoritma yang berhasil memecahkan, maka selama itu pula algoritma rsa akan tetap terjamin keaananannya[2].

Kriptografi muncul didasari atas berkomunikasi dan saling bertukar informasi/data secara jarak jauh.komunikasi dan pertukaran data antar wilayah dan negara ataupun benua bukan lagi menjadi suatu kendala yang berarti. Seiring dengan itu tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu

perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain.oleh karena itu munculah Cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi[9].

1. Uraian Penelitian

A. Kriptografi

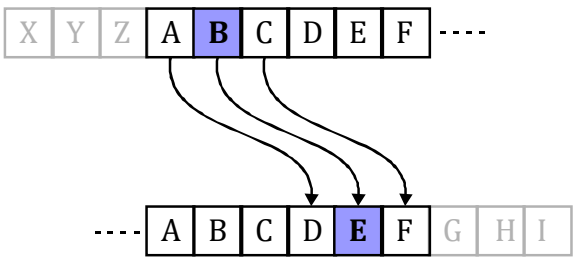
Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem Kriptografi (*Cryptosystem*) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi[3]. Menurut Katz, kriptografi adalah studi ilmiah atau teknik untuk mengamankan informasi digital, transaksi dan komputasi yang terdistribusi[4].

Kriptografi bertujuan untuk memberikan layanan keamanan [5] sebagai berikut :

- Kerahasiaan (*Confidentiality*)
  Informasi dirahasiakan dari semua pihak yang tidak berwenang.
- Keutuhan Data (*Integrity*)
- Pesan tidak berubah dalam proses pengiriman hingga pesan diterima oleh si penerima.
- Autentikasi (*Message Autentication*)
  Kepastian terhadap identitas yang terlibat dan keaslian sumber data.
- Nirpenyangkalan (*Nonrepudiation*)
- Setiap entitas yang berkomunikasi tidak dapat menolak atau menyangkal atas data yang telah dikirim atau diterima.

B. Caesar Cipher

Substitusi yang pertama dalam dunia pengamanan data adalah pada zaman pemerintahan Julius Caesar, sehingga dikenallah dengan nama Caesar Cipher, yakni mengganti posisi huruf awal dari alphabet [6], caesar cipher dikenal juga dengan nama *Shift Cipher*.



Gbr. 1 Pergeseran pada caesar cipher

Dari gambar 1 ditunjukkan telah terjadi pergeseran 3 (tiga) buah karakter, yaitu A berubah menjadi D, B berubah menjadi E dan C berubah menjadi F dan seterusnya. Caesar cipher dapat dipecahkan dengan menggunakan *brute force*, yaitu suatu bentuk serangan yang mencoba kemungkinan-kemungkinan untuk menemukan kunci, dapat dinyatakan dengan fungsi kongruen sebagai berikut:

$$C=E(P) =(p+k) \bmod 26 \ldots (1)$$

Dimana mod 26 adalah jumlah alphabet. Persamaan 1 digunakan untuk proses enkripsi.

$$P=D(C) =(c-k) \bmod 26, \text{ (jika c-k adalah negatif, maka tambahkan 26)} \ldots (2)$$

Dimana, jika hasil dari c-k adalah nilai negatif, mod 26 tidak berlaku, melainkan hasil nilai negatif langsung dijumlahkan dengan 26. Persamaan 2 digunakan untuk proses dekripsi.

C. Algoritma RSA

RSA merupakan salah satu dari *Public Key Cryptosystem* yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar[7].

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi dan salah satu penemuan besar pertaman 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 mutakhir[8].

Algoritma pembentukan kunci :

- Tentukan p dan q bernilai dua bilangan prima besar, acak dan dirahasiakan, $p \neq q$, p dan q memiliki ukuran yang sama.
- Hitung n = p x q, dan hitung $\phi(n) = (p - 1) \times (q - 1)$, bilangan integer n disebut (RSA) modulus.
-Tentukan e bilangan prima acak yang memiliki syarat :

$1 < e < 1(n)$, GCD(e, i(n)) = 1, disebut e relatif prima terhadap i(n), bilangan integer n disebut (RSA) *enciphering component*, sehingga menghasilkan $D_d(E_e(m)) = E_e(D_d(c)) \equiv m^d \bmod n$

D. Kombinasi Caesar Cipher dan Algoritma RSA

Kombinasi caesar cipher dan algoritma RSA bertujuan untuk mengatasi kelemahan dari caesar cipher. Karena caesar cipher bekerja hanya dengan melakukan pergeseran karakter, sehingga memungkinkan untuk dipecahkan dengang menggunakan *brute force*. Metode *brute force* yang paling sering digunakan adalah dengan menggunakan statistika frekuensi kemunculan huruf yang paling sering muncul. Contoh : Mereka mendapatkan pesan KATA. Karena huruf yang paling sering muncul adalah huruf A, maka dilakukan pergeseran dari huruf A ke huruf P yang hanya memiliki frekuensi kemunculan 2 kali, lalu gantilah huruf A dengan huruf P, lalu geser mundur pesan sisanya. Kombinasi caesar cipher dengan algoritma RSA bekerja dengan cara mengenkripsikan pesan terlebih dahulu dengan caesar cipher, selanjutnya hasil pesan (cipherteks) di enkripsi kembali menggunakan algoritma rsa, sehingga pola kemunculan statistika dari pesan tidak dapat di deteksi.

2. Implementasi

A. Perhitungan Kombinasi caesar cipher dan algoritma rsa

Dari dasar teoritis yang sudah dibahas, untuk mengenkripsi suatu data menggunakan kombinasi caesar cipher dan algoritma rsa dibutuhkan beberapa sampel bilangan untuk menampung karakter, misalkan (c, k dan p). Satu buah bilangan digunakan sebagai kunci pergeseran objek (k), dan dua sisanya digunakan untuk enkripsi.

Contoh : terdapat pesan plainteks STIKOM dengan kunci k=20, dengan memetakan alphabet A=0 hingga Z=25.

Langkah 1 : lakukan pemetaan antara proses enkripsi dengan plaintek, lalu hasilnya di modulus kan dengan 26, maka hasil yang akan diperoleh MNCEIG (caesar cipher).

Langkah 2 : cipherteks yang sudah diperoleh (MNCEIG) dienkripsi kembali dengan menentukan faktor bilangan prima yang lebih besar. Berbeda dengan caesar cipher yang hanya menggunakan karakter alphabetis, algoritma rsa menggunakan semua jenis karakter yang ada. Jadi untuk mengenkripsi karakter M saja sudah bisa menghasilkan enkripsi dengan nilai karakter yang lebih panjang, hasil dari enkripsi karakter M adalah
XKe4/FWxibRz/bYLNzP40XVCsWYXrOEJbSzcGKut8mij88XnqdvJJ5Yv+ll7en+gf1QTO16sjAdwj/bcTTSmSXQTg3ZCzwhd/+tXpcd8FhWGaslzM1JENfhLCFchT75gCxC9vcs1ND5rK23nr/nI2ZWE9s74lS5Oc/b/F/S69jE=, sehingga jika semua karakter MNCEIG di enkripsi akan menghasilkan
WKGrE+923RxzF/1ijbjh1g7nLvMfjHk4jlfNrHppkyNSuGYCA/w4+eAiX/uV5bAbgsUIKGpkiwiqeiv/zyrEP+K01HKzLMEpGBdCYye8x2b48wfrh0Lsym/G2tQIbi9yPyTEsCebT/Zv3GVN5lQOK0qssVh7qz2nudTGcI41lWs=.

Proses pengembalian pesan (dekripsi) adalah sebagai berikut
Langkah 1 : lakukan dekripsi dari algoritma rsa,
sehingga akan mengkasilkan pesan terenkripsi untuk diolah di caesar cipher. Pesan yang masih terenkripsi dengan algoritma rsa adalah
XKe4/FWxibRz/bYLNzP40XVCsWYXrOEJbSzcGKut8mij88XnqdvJJ5Yv+ll7en+gf1QTO16sjAdwj/bcTTSmSXQTg3ZCzwhd/+tXpcd8FhWGaslzM1JENfhLCFchT75gCxC9vcs1ND5rK23nr/nI2ZWE9s74lS5Oc/b/F/S69jE=, akan di dekripsi kembali dengan memanggil kunci publik dengan menentukan bilangan n (prima) terbesar, setelah diproses akan menghasilkan karakter M, sehingga jika semua karakter
WKGrE+923RxzF/1ijbjh1g7nLvMfjHk4jlfNrHppkyNSuGYCA/w4+eAiX/uV5bAbgsUIKGpkiwiqeiv/zyrEP+K01HKzLMEpGBdCYye8x2b48wfrh0Lsym/G2tQIbi9yPyTEsCebT/Zv3GVN5lQOK0qssVh7qz2nudTGcI41lWs= didekripsi, akan menghasilkan MNCEIG.

Langkah 2 : hasil dari dekripsi dengan algoritma rsa akan di dekripsi kembali menggunakan caesar cipher, dengan menggunakan pemetaan dekripsi ke cipher. Pemetaan alphabet masih tetap sama, yaitu A=0 hingga Z=25 dengan kunci yang sama yaitu *k*=20. Sehingga jika huruf M dengan urutan alphabet = 12, maka (12-20) mod 26, karena 12-20 menghasilkan bilangan negatif (-8) maka modulus bisa diabaikan dan bilangan (-8) bisa langsung dijumlahkan dengan 26, maka hasilnya adalah 18, dan dengan urutan alphabetis 18 adalah huruf S. Jadi cipherteks MNCEIG setelah didekripsi kembali akan menghasilkan STIKOM.

B. Pseudocode Caesar Cipher dan Algoritma RSA

Pseudocode yang digunakan untuk melakukan enkripsi dan dekripsi dengan caesar cipher adalah:

Proses Enkripsi Caesar Cipher

```
For i:=1 to lenght (s) do
Begin
C:=ord(upcase(s[i]))+indice;
If c>90 then c:=c-26;
S[i]:=chr(c);
End;
```

Proses Dekripsi Caesar Cipher

```
For i:=1 to lenght (s) do
Begin
    C:=ord(upcase(s[i]))-indice;
    If c<65 then c:=c+26;
    S[i]:=chr(c);
    End;
```

Skema RSA sendiri mengadopsi dari skema block cipher, dimana sebelum dilakukan enkripsi, plainteks yang ada dibagi – bagi menjadi blok – blok dengan panjang yang sama, dimana plainteks dan cipherteksnya berupa integer(bilangan bulat) antara 1 hingga n, dimana n berukuran biasanya sebesar 1024 bit, dan panjang bloknya sendiri berukuran lebih kecil atau sama dengan log(n) +1 dengan basis 2. Fungsi enkripsi dan dekripsinya dijabarkan dalam fungsi berikut :

$C = M^e \bmod n$ . . .(fungsi enkripsi)
$M = C^d \bmod n$ . . .(fungsi dekripsi)

C = Cipherteks
M = Message / Plainteks
e = kunci publik
d= kunci privat
n = modulo pembagi

Kedua pihak harus mengetahui nilai e dan nilai n ini, dan salah satu pihak harus memilki d untuk melakukan dekripsi terhadap hasil enkripsi dengan menggunakan public key e. Penggunaan algoritma ini harus memenuhi kriteria berikut :

1. Memungkinkan untuk mencari nilai e, d, n sedemikian rupa sehingga Med mod n = M untuk semua M < n.
2. Relatif mudah untuk menghitung nilai Me mod n dan Cd mod n untuk semua nilai M < n.
3. Tidak memungkinkan mencari nilai d jika diberikan nilai n dan e.

Syarat nilai e dan d ini, gcd(d,e)=1
sebelum memulai penggunaan RSA ini, terlebih dahulu kita harus memiliki bahan – bahan dasar sebagai berikut :

1. p, q = 2 bilangan prima yang dirahasiakan
2. n, dari hasil p.q
3. e, dengan ketentuan gcd (Φ(n), e) =1
4. d, $e^{-1} \pmod{\Phi(n)}$

contoh :

1. Pilih 2 bilangan prima, misalnya p = 17 dan q = 11.
2. Hitung n = pq = 17 × 11 = 187.
3. Hitung Φ(n) = (p – 1)(q – 1) = 16 × 10 = 160.
4. Pilih nilai e sedemikian sehingga relatif prima terhadap Φ(n) = 160 dan kurang dari Φ(n); kita pilih e = 7.
5. Hitung d sedemikian sehingga de ≡ 1 (mod 160) dan d < 160.Nilai yang didapatkan d = 23,karena 23 × 7 = 161 = (1 × 160) + 1; d dapat dihitung dengan Extended Euclidean Algorithm.

Nah, nilai e dan d inilah yang kita sebut sebagai Public Key(e) dan Private Key(d). Pasangan Kunci Publiknya ={7,187} dan Kunci Privatnya = {23, 187}

Proses Enkripsi

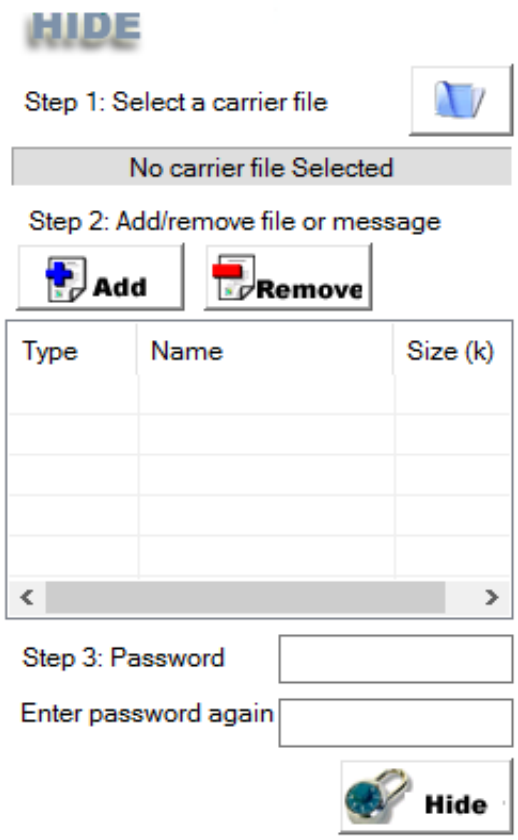
Misalnya kita punya M 88. Untuk proses enkripsi, kita akan menghitung $C = 88^7 \bmod 187$.
$= 88^7 \bmod 187$.
=894,432 mod 187
=11
Nah, kita mendapatkan nilai C =11.

Proses Dekripsi

Selanjutnya, nilai C ini dikirimkan kepada penerima untuk didekripsi dengan kunci privat miliknya.
$M = C^d \bmod n$
$= 11^{23} \bmod 187$
=79,720,245 mod187
= 88

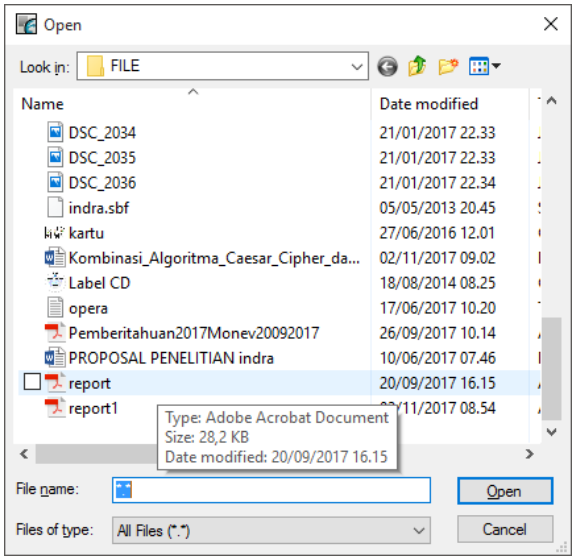
3. Hasil

Pada proses ini akan dihasilkan bagaimana langkah-langkah untuk pengamanan berkas dokumen dan pesan. Berkas dokumen yang akan diamankan terlebih dahulu akan dipilih dan selanjutnya disisipkan sebuah pesan teks kedalam berkas dokumen terpilih, selanjutnya berkas dokumen yang sudah berisikan pesan rahasia akan diberikan pengaman berupa kunci keamanan sebelum berkas dokumen yang sudah berisikan pesan teks dikirimkan kepada penerima.



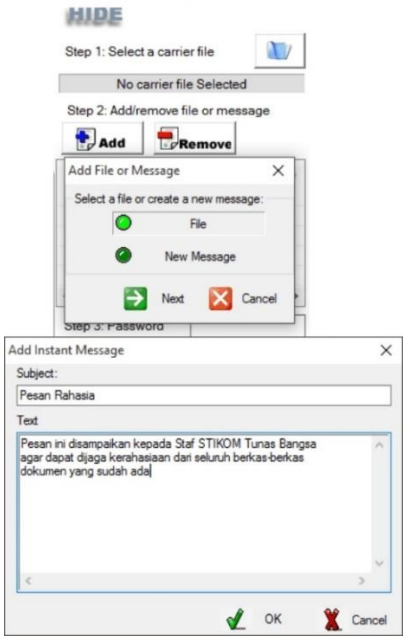
Gbr. 2 Tampilan awal aplikasi

Pada tahap awal, sipengirim akan memilih sebuah berkas dokumen yang akan disisipkan oleh pesan teks. Berkas dokumen yang dipilih dapat bertipe pdf, doc, docx, jpg, mpg.



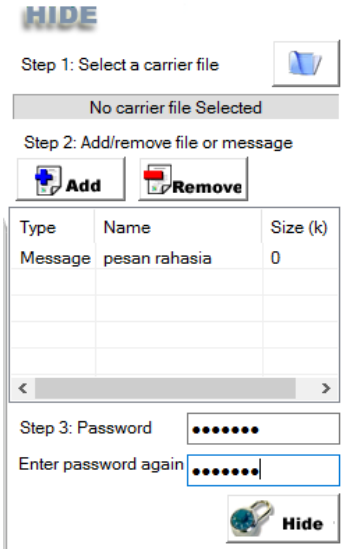
Gbr. 3 Pemilihan berkas dokumen yang akan disisipkan pesan teks

Selanjutnya menyisipkan pesan teks kedalam berkas dokumen yang sudah terpilih. Dalam hal ini, pesan teks tersebut akan di enkripsi terlebih dahulu menggunakan algoritma RSA lalu disisipkan kedalam berkas dokumen.



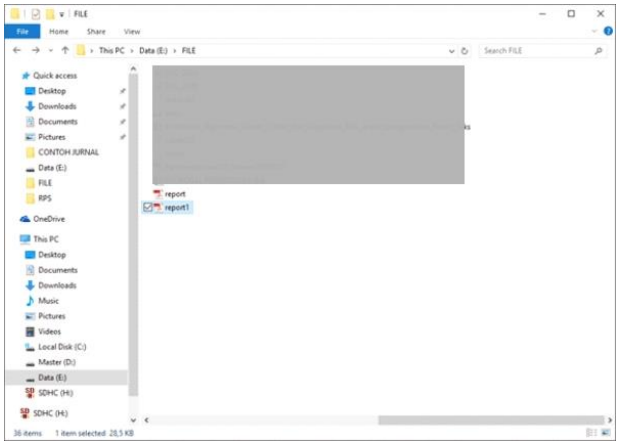
Gbr. 4 Proses Penyisipan dan Pendeskripsian Pesan Teks

Selanjutnya memberikan kata kunci kedalam penyandian pesan teks dan berkas dokumen untuk menjaga keamanan dari berkas dokumen dan pesan teks.



Gbr. 5 Proses Pemberian Kata Kunci

Hasil berkas dokumen yang sudah diberikan keamanan akan terlihat didalam gambar berikut



Gbr. 6 Hasil Berkas Dokumen yang sudah dienkripsi

4. Kesimpulan

Kombinasi caesar cipher dan algoritma rsa dapat membantu meningkatkan data, jika dibandingkan dengan hanya menggunakan satu metode saja. Menggunakan perhitungan dengan struktur alphabetis dan dipadukan dengan menggunakan memfaktoran bilangan prima dapat meningkatkan sistem keamanan data, sehingga data yang tersimpan akan semakin terjaga.

Daftar Pustaka

[1] Rachmawati, Dian & Candra, Ade. 2015. Implementasi Kombinasi *Caesar Cipher* dan *Affine Cipher* untuk keamanan data teks. Jurnal Edukasi dan Penelitian Informatika (JEPIN), Vol. 1, No. 2.

[2] Alvianto, A. R. & Darmaji. 2015. Pengamanan pengiriman pesan via SMS dengan Algoritma RSA berbasis Android. Jurnal Sains dan Seni ITS, Vol. 4, No. 1.

[3] Mollin, R. A. 2007. *An Introduction to Cryptography*. 2nd Edition. Chapman & Hall/CRC : Boca Raton, Florida.

[4] Katz, J. & Lindell, Y. 2007. Introduction to Modern Cryptography. Chapman & Hall/CRC : United States.

[5] Paar, C. & Pelzl, J. 2010. *Understanding Cryptography*. Springer-Verlag: Berlin.

[6] Ariyus, D. 2008. Pengantar Ilmu Kriptografi: Teori, analisis dan implementasi. Andi: Yogyakarta.

[7] Mollin, R. A. 2007. *An Introduction to Cryptography*. 2nd Edition. By Tailor & Francis Group, London, New York.

[8] Zainal Arifin. 2009. Studi Kasus : Penggunaan Algoritma RSA sebagai algoritma kriptografi yang aman. Samarinda.

[9] Delliana, Br. Tarigan. 2014. Implementasi Algoritma Kriptografi Hill Cipher Dalam Penyandian Data Gambar. Jurnal Pelita Informatika Budi Darma, Vol : VII, No. 2.

[10] Basuki, A. Paranita, U., Hidayat, R., 2016. Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere dan Blok Cipher Berbasis Mobile. Seminar Nasional Teknologi Informasi dan Multimedia. STMIK AMIKOM Yogyakarta.