KOMBINASI METODE *AFFINE CIPHER* DAN *EXCLUSIVE-OR (XOR)* DALAM PENGAMANAN PESAN

Pembimbing :

OLEH:

SUHARDI

NIP. 19880923 201903 1 010

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA
MEDAN
2021

Judul : KOMBINASI METODE *AFFINE CIPHER* DAN *EXCLUSIVE-OR (XOR)* DALAM PENGAMANAN PESAN

Nama : SUHARDI

NIP : 19880923 201903 1 010

FAKULTAS SAINS DAN TEKNOLOGI
PROGRAM ILMU KOMPUTER

SUHARDI

Kombinasi Metode *Affine Cipher* dan *Exclusive-OR (XOR)* dalam Pengamanan Pesan

x + 41 halaman, 11 Gambar, 4 tabel

ABSTRAK

Komputer sebagai sarana penyimpanan dan pengiriman data, informasi, dan dokumen yang penting dan rahasia sering dapat dengan mudah diakses oleh orang yang tidak bertanggungjawab. Beberapa kasus menyangkut keamanan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Penelitian ini bertujuan membangun prototipe keamanan data (kriptografi) yang lebih baik untuk pesan teks dengan melakukan kombinasi dua metode kriptografi. Metode yang digunakan dalam penelitian ini adalah metode Affine Cipher dan metode Exclusive-OR (XOR). Model analisa kebutuhan kriptografi pesan ini menggunakan State Transition Diagram (STD), perancangan proses menggunakan flowchart program dan algoritma serta diimplementasikan dengan Javascript. Hasil dari penelitian ini menunjukkan bahwa cipher teks hasil enkripsi dari metode Affine Cipher kemudian dienkripsikan kembali menggunakan Exclusive-OR (XOR) dan apabila ingin melakukan proses dekripsi pesan maka cipher teks terlebih dahulu dengan metode XOR kemudian didekripsi kembali menggunakan Affine Cipher. Dapat disimpulkan bahwa kombinasi dua metode kriptografi tersebut berjalan dengan baik dan tanpa mengalami kendala apapun baik dalam proses enkripsi maupun dekripsi.

Kata Kunci : *kriptografi, pesan, affine cipher, exlusive or, state transition diagram, flowchart*

SCIENCE AND TECHNOLOGY FACULTY
DEPARTMENT OF COMPUTER SCIENCE

SUHARDI
Affine Cipher And Exclusive-OR (XOR) Methods Combination in Message Security

x + 41 pages, 11 Images, 4 tables

ABSTRACT

Computers as a means of storing and sending important and confidential data, information and documents can often be easily accessed by irresponsible people. Several cases concerning computer security are now a job that requires handling and security costs that are so large. This study aims to build a better data security (cryptography) prototype for text messages by combining two cryptographic methods. The method used in this research is the Affine Cipher method and the Exclusive-OR (XOR) method. This message cryptographic needs analysis model uses State Transition Diagram (STD), the process design uses program flowcharts and algorithms and is implemented with Javascript. The results of this study indicate that the cipher text encrypted from the Affine Cipher method is then re-encrypted using Exclusive-OR (XOR) and if you want to decrypt the message, the text cipher first uses the XOR method and then decrypts it again using the Affine Cipher. It can be concluded that the combination of the two cryptographic methods worked well and without experiencing any problems in the encryption or decryption process.

Keyword : cryptography, message, affine cipher, exclusive or, state transition diagram, flowchart

SURAT REKOMENDASI

Saya yang bertanda tangan di bawah ini, menyatakan bahwa penelitian saudara :

Nama	: **Suhardi, M.Kom**
NIP	: 19880923 201903 1 010
Tempat/tanggal lahir	: Pkl. Brandan, 23 September 1988
Jenis Kelamin	: Laki-laki
Agama	: Islam
Pangkat/Gol	: Penata Muda TK.I (III/b)
Unit Kerja	: Fakultas Sains dan Teknologi UIN Sumatera Utara Medan
Judul Penelitian	: Kombinasi Metode Affine Cipher dan Exclusive-Or (XOR) dalam Pengamanan Pesan

Telah memenuhi syarat sebagai suatu karya ilmiah, setelah membaca dan memberikan masukan saran-saran terlebih dahulu.

Demikian surat rekomendasi ini diberikan untuk dapat dipergunakan seperlunya.

Medan, 02 Februari 2021
Konsultan I,

Dr. Mhd Furqan, S.Si., M.Comp.Sc.
NIP. 19800806 200604 1 003

SURAT REKOMENDASI

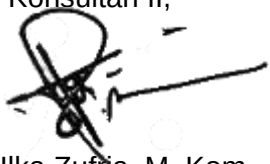
Saya yang bertanda tangan di bawah ini, menyatakan bahwa penelitian saudara :

Nama	: **Suhardi, M.Kom**
NIP	: 19880923 201903 1 010
Tempat/tanggal lahir	: Pkl. Brandan, 23 September 1988
Jenis Kelamin	: Laki-laki
Agama	: Islam
Pangkat/Gol	: Penata Muda TK.I (III/b)
Unit Kerja	: Fakultas Sains dan Teknologi UIN Sumatera Utara Medan
Judul Penelitian	: Kombinasi Metode Affine Cipher dan Exclusive-Or (XOR) dalam Pengamanan Pesan

Telah memenuhi syarat sebagai suatu karya ilmiah, setelah membaca dan memberikan masukan saran-saran terlebih dahulu.

Demikian surat rekomendasi ini diberikan untuk dapat dipergunakan seperlunya.

Medan, 02 Februari 2021
Konsultan II,



Ilka Zufria, M. Kom
NIP. 19850604 201503 1 006

KATA PENGANTAR

Puja dan puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga laporan penelitian ini dapat terselesaikan. Penelitian ini berjudul “Kombinasi Metode Affine Cipher dan Exclusive-Or (XOR) dalam Pengamanan Pesan”. Penyusunan laporan tidak terlepas dari bantuan dan dorongan dari berbagai pihak, baik moril maupun materiil. Untuk itu dengan segala hormat penulis mengucapkan terimakasih kepada rekan-rekan yang telah membantu dan terutama kepada Kedua Konsultan yang memberi koreksi dan masukan berharga.

Penulis menyadari bahwa semua yang tertuang dalam laporan ini jauh dari sempurna. Oleh karena itu penulis mengharapkan masukan berupa kritik dan saran demi kesempurnaan penelitian ini. Akhirnya penulis berharap semoga laporan penelitian ini dapat bermanfaat.

Medan, Februari 2021

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Hampir semua orang dapat dengan mudahnya melakukan perekaman dan penyebaran data secara sengaja maupun tidak sengaja, baik itu melalui komputer maupun melalui telepon genggam. Data tersebut dapat berupa pesan teks, gambar, audio, video dan lain sebagainya. Hal ini menyebabkan dibutuhkannya mekanisme pengamanan data untuk mencegah akses yang tidak diinginkan sehingga kerahasiaan data dan integritas data tetap terjamin. Mekanisme pengamanan data yang sering dilakukan yaitu dengan melakukan kontrol akses terhadap data tersebut. Namun saat sekarang ini dibutuhkan mekanisme yang lebih baik selain melakukan kontrol akses data. Salah satu caranya yaitu dengan menerapkan teknik kriptografi

Suatu sistem kriptografi (kriptosistem) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Pada dasarnya mekanisme kerja semacam ini telah dikenal sejak jaman dahulu. Bangsa Mesir kuno sekitar 4000 tahun yang lalu bahkan telah mempraktekkannya dengan cara yang sangat primitif[1]. Kriptografi pada mulanya dipahami sebagai ilmu tentang menyembunyikan pesan[2], tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi[3]

Beberapa penelitian telah banyak dilakukan dalam kriptografi. Salah satunya tentang modifikasi algoritma

---

1 Rinaldi Munir (2011) Kriptografi Keamanan

2 Rifki Sadikin (2012) Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java

3 Diffie, Whitfield, Martin E Hellman (1976) New Directions in Cryptography. IEEE Trans. Info. Theory IT-22.

kritografi Affine Cipher untuk penyandian *password* yang melakukan percobaan pada pesan teks pada *password* dengan membalikkan kata pada pesan teks *password* sebelum dilakukan proses enkripsi. Proses enkripsi dan dekripsi pesan dapat berjalan dengan baik[4]. Penelitian selanjutnya adalah tentang kombinasi kriptografi Caesar dan *Affine Cipher* untuk penyembunyian pesan yang melakukan juga melakukan percobaan pada pesan teks Proses enkripsi pesan teks asli dilakukan dengan algoritma Caesar Cipher kemudian pesan hasil enkripsi tersebut dienkripsi kembali dengan algoritma Affine Cipher sehingga menghasilkan Cipherteks. Hal serupa juga dilakukan pada proses dekripsinya. Kombinasi sandi *Caesar* dan sandi Affine dilakukan karena *Affine Cipher* memiliki kelebihan yang bisa menutupi kekurangan sandi Caesar yaitu sandi affine memiliki tiga kunci berbeda dalam melakukan enkripsi, dekripsi, dan pergeseran sehingga kode yang terbentuk lebih sulit dipecahkan[5].

Berdasarkan penelitian-penelitian tersebut maka teknik kriptografi *Affine Cipher* dapat dikombinasikan dengan Kriptografi *Exclusive-OR (XOR)* untuk meningkatkan pengamanan pesan teks. Affine Cipher merupakan metode kriptografi yang menggunakan kunci simetris, yang mana kunci yang digunakan untuk melakukan enkripsi sama dengan kunci yang digunakan untuk dekripsi[6], sedangkan algoritma XOR adalah salah satu algoritma kriptografi modern sederhana dengan meng-XOR kan plainteks (P) dengan kunci (K) menghasilkan cipherteks[7]. Peneliti berharap kombinasi kedua teknik

---

[4] Sriramoju Ajay Babu (2017) International Journal of Research In Science & Engineering 3 346-351

[5] Septi Yana Wulandari (2020) Proceeding International Conference on Science and Engineering 3: 741-744

[6] Juliadi and dkk (2013) Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat Dengan Vigenere Cipher, Buletin Ilmiah Matematika Statistik, vol. 2, no. 2, pp. 87 - 92.

[7] M. Jain (2014) Implementation Of Hybrid Cryptography Algorithm, IJCEM. India, vol. 1, pp. 126-142

kriptografi tersebut dapat berjalan dengan baik dan dapat meningkatkan keamanan pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka permasalaha umum yang akan di bahas dalam penelitian ini adalah bagaimanakah langkah – langkah mengkombinasikan teknik kriptografi *Affine Cipher* dengan Kriptografi *Exclusive-OR (XOR)* dalam proses enkripsi dan dekripsi pesan

1.3 Batasan Masalah

Untuk mendapatkan hasil penelitian dari permasalahan yang ditentukan, maka ada pembatasan masalah penelitian, yaitu sebagai berikut :

1 Pesan yang digunakan berupa pesan teks yang dapat dibaca

2 Rekayasa dan pemodelan sistem menggunakan bahasa pemrograman Javascript dan aplikasi browser.

3 Analisa kebutuhan perangkat lunak kriptografi pesan menggunakan *State Transition Diagram* (STD)

1.4. Tujuan Penelitan

Mengetahui langkah – langkah mengkombinasikan teknik kriptografi *Affine Cipher* dengan Kriptografi *Exclusive-OR* (XOR) dalam proses enkripsi dan dekripsi pesan.

1.5. Manfaat Penelitian

Dari penelitian ini diharapkan dapat digunakan sebagai salah satu rujukan dan panduan dalam memahami proses pengamanan pesan teks menggunakan kombinasi

teknik kriptografi *Affine Cipher* dengan Kriptografi *Exclusive-OR* (XOR), sehingga dapat meningkatkan keamanan pesan agar tidak mudah untuk diketahui oleh orang lain.

BAB II
TINJAUAN PUSTAKA

2.1 Kriptografi

Kata kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata kryptos yang artinya tersembunyi dan graphein yang artinya menulis. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi, dan dokumen dikonversi ke bentuk tertentu yang sulit untuk dimengerti[8]. Kriptografi bertujuan untuk menjaga kerahasiaan data, informasi, dan dokumen supaya tidak dapat diketahui oleh pihak yang tidak berhak mengetahuinya (*unauthorized person*).

Terdapat bermacam sistem sandi yang tujuan penggunaan dan tingkat kerahasiaannya berbeda sesuai dengan permintaan user, tetapi dalam prakteknya user menginginkan kemudahan-kemudahan seperti: kerahasiaan data, kecepatan, ketepatan, maupun biaya yang murah. Suatu data yang tidak disandikan disebut plaintext atau cleartext sedangkan data yang telah disandikan disebut ciphertext. Proses yang dilakukan untuk mengubah plaintext menjadi ciphertext disebut enkripsi (*encryption*) atau encipherment sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut dekripsi (*decryption*) atau *decipherment* (ISO 7498-2). Kriptografi memerlukan parameter untuk proses konversi yang dikendalikan oleh sebuah kunci atau beberapa kunci[9].

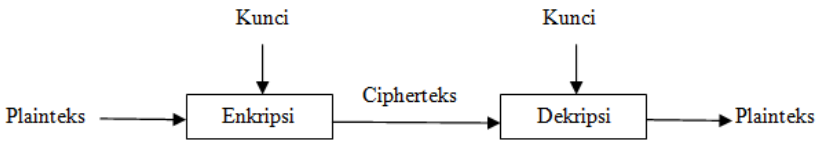
Kriptografi saat ini menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan. Pengiriman pesan sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan

---

[8] Goyal, D dan Srivastava (2012) International Journal of Information and Communication Technology Research, Volume 2 No. 4.

[9] Ibisa (2011) Keamanan Sistem Informasi.

pesan yang dikirim, dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut berdasarkan algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berhak atas data, informasi, dan dokumen tersebut.



Gambar 2.1 Skema Enkripsi dan Dekripsi

2.2 Tujuan Kriptografi

Kriptografi merupakan suatu metode yang dapat digunakan dalam rangka pengamanan pesan. Oleh karena itu, kriptografi mempunyai tujuan sebagai berikut:

a. Kerahasiaan Data (*confidentiality*)
   Ancaman atau serangan terhadap kerahasiaan data ini biasanya dilakukan dengan menerobos hak akses, penyadapan data dan penipuan. Di dalam kriptografi layanan ini di realisasikan dengan menyandikan pesan menjadi cipherteks. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data asli (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang akan dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai pada si penerima ciphertext tersebut diubah lagi ke bentuk asli (plaintext).
b. Nirpeyangkalan (*non-repudiation*)
   Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu

pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Aspek ini sangat berguna dalam melakukan sebuah transaksi. Sebagai contoh, seseorang yang akan melakukan transaksi jual beli online dan dalam tahap pertama si pembeli mengirimkan sebuah email dalam orderan maka si pembeli tidak dapat menyangkal bahwa dia telah mengirim *email*.

c. Integritas Data (*data integrity*)
   Layanan yang menjamin bahwa data masih dalam keadaan asli atau belum pernah diubah selama dalam pengiriman. Layanan ini di realisasikan dengan menggunakan tanda tangan digital (*digital signature*). Data yang dikirim dengan tanda tangan digital menyiratkan bahwa data itu asli. Aspek ini menjamin bahwa data tidak dapat diubah tanpa izin dari yang berhak.
d. Autentikasi Data (*authentication*)
   Layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication atau entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Data yang didapat oleh suatu pihak oleh pihak lain harus di lakukan identifikasi agar memastikan keaslian data tersebut. Identifikasi terhadap data tersebut dapat berupa tanggal pembuatan data, isi informasi, waktu kirim dan hal-hal lainnya yang berhubungan dengan data tersebut[10].

[10] Rinaldi (2006) Kriptografi

2.3 Algoritma Kriptografi

Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Kunci yang digunakan dalam algoritma kriptografi dapat dibedakan atas algoritma simetri dan algoritma asimetri. Pengembangan kedua algoritma tersebut diperlukan *cipher* dan kunci[11].

2.4 *Cipher* dan Kunci

Algoritma kriptografi disebut sebagai cipher yang dapat diartikan sebagai aturan untuk melakukan enkripsi dan dekripsi. Pengertian *cipher* dapat juga dinyatakan sebagai fungsi matematika yang digunakan untuk melakukan enkripsi dan dekripsi. Konsep matematis dari algoritma kriptografi adalah hubungan antara dua buah himpunan yang terdiri elemen plainteks dan elemen cipherteks. Enkripsi dan dekripsi merupakan fungsi yang akan memetakan elemen dari kedua himpunan tersebut[12]. Jika P adalah plainteks dan C adalah cipeherteks, maka fungsi enkripsi E yang memetakan P ke cipher C adalah sebagai berikut:

$$E(P) = C \quad \text{.....} \quad (2.1)$$

Sedangkan fungsi dekripsi D yang memetakan cipher C ke plainteks P dapat ditulis sebagai berikut:

---

[11] Andy Nugroho (2012) Implemantasi Algoritma Caesar Cipher ROT13 dan BASE64 untuk Enkripsi dan Dekripsi Pesan SMS pada Handphone Berbasis Android, [Skripsi], Sekolah Tinggi Manajemen Informatika dan Komputer Amikom, Yogyakarta.

[12] Pressman, R.S (1997) *Software Engineering a Practitioner's Approach*, 4th edition,McGraw-Hill International Editions, New York.

$$D(C) = P \text{ .....} \quad (2.2)$$

Proses enkripsi menjadi dekripsi dimana akan dilakukan dalam rangka mengembalikan pesan ke pesan asal maka persamaan tersebut di atas akan menjadi persamaan sebagai berikut:

$$D(E(P)) = P \text{ .....} \quad (2.3)$$

Kriptografi modern dapat mengatasi keamanan algoritma dengan menggunakan kunci yang tidak dirahasiakan tetapi kunci tersebut harus dijaga kerahasiaannya. Kunci (*key*) adalah Parameter yang digunakan untuk melakukan transformasi enkripsi dan dekripsi[13] dan secara matematis dapat ditulis sebagai berikut:

$$E_K(P) = C \text{ dan } D_K(C) = P \text{ .....} \quad (2.4)$$

Persamaan (2.4) dapat memenuhi jika persamaan tersebut dapat diformulasikan sebagai berikut:

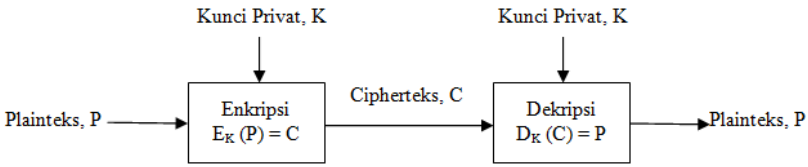
$$D_K(E_K(P)) = P \text{ .....} \quad (2.5)$$

2.5 Algoritma Simetris

Algoritma kriptografi simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada

[13] Rahayu, T. P, Yakub, dan Limiady, I (2012) Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA) Yogyakarta.

algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu *byte* data[14].

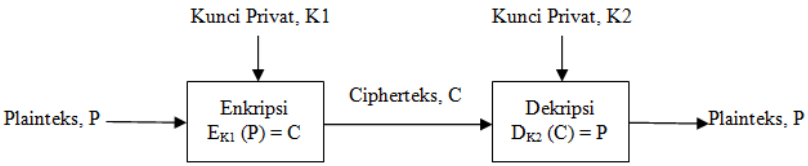


Gambar 2.2 Skema Algoritma Simetris

Sedangkan pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok). Contoh algoritma kunci simetris yang terkenal adalah DES (Data Encryption Standard).

2.6 Algoritma Asimetris

Algoritma kriptografi asimetrik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (*public key algorithm*) karena kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*).Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA dan ECC



Gambar 2.3 Skema Algoritma Asimetri

[14] Ariyus, D (2008) Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.

2.7 Aspek – Aspek Keamanan pada Kriptografi

Kriptografi pada dasarnya adalah menjaga kerahasiaan plaintext atau kunci dari penyadapan. Penyadap berusaha mendapatkan data yang digunakan untuk kegiatan pencurian data atau biasa disebut kriptanalisis (*cryptanalysis*). Kriptanalisis bertujuan untuk memecahkan cipherteks menjadi plainteks semula tanpa memiliki akses ke kunci yang digunakan hingga berhasil menemukan kelemahan dari sistem kriptografi yang pada akhirnya mengarah untuk menemukan kunci dan mengungkap plainteks. Aspek-aspek yang diamankan pada sistem kriptografi agar sistem dapat berjalan sempurna, ada delapan aspek yang perlu diperhatikan[15] antara lain :

a. *Authentifikasi* : agar penerima informasi dapat memastikan pesan tersebut datang dari orang yang dimintai informasi, dengan kata lain informasi tersebut benar-benar datang dari orang yang dikehendaki.
b. *Integrity* : keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang lain yang tidak berhak dalam perjalanan informasi tersebut.
c. *Nonrepudiation* : menyatakan pesan yang dikirim dari orang yang asli, artinya si pengirim pesan tidak dapat mengelak bahwa dialah yang mengirimkan informasi tersebut.
d. *Authority* : informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
e. *Confidentiality* : merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
f. *Privacy* : merupakan data-data yang sifatnya rahasia dan tidak boleh diketahui oleh pihak lain.

[15] Saroha, V, Mor, S dan Dagar, A (2012) Enhancing Security of Caeser Cipher by Double Columnar Transposition Method, International Journal of Advanced Research Computer Science and Software Engineering, Volume 2, Issue 10.

g. *Availability* : Sistem yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
h. *Access Control* : Aspek ini berhubungan dengan cara pengaturan siapa-siapa saja yang berhak mengakses sistem, mengetahui sistem keamanannya.

2.*8 Affine Cipher*

Affine cipher adalah perluasan dari *Caesar cipher*, yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran[16]. Secara matematis enkripsi plainteks P menghasilkan cipherteks C dapat dinyatakan dengan fungsi kongruen sebagai berikut:

$$E(P) = (ax + b) \bmod m \quad \text{.....} \quad (2.6)$$

Dimana :

m = ukuran alfabet
a = bilangan bulat yang harus relatif prima dengan m (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan).
b = jumlah pergeseran (*caesar cipher* adalah khusus dari *affine cipher* dengan m = 1).
x = plainteks yang dikonversi menjadi bilangan bulat dari 0 sampai m – 1 sesuai dengan urutan dalam alfabet.
E(P) = cipherteks yang dikonversi menjadi bilangan bulat dari 0 sampai m – 1 sesuai dengan urutan dalam alfabet.

Sedangkan fungsi dekripsinya dapat dituliskan dengan menggunakan persaman sebagai berikut :

[16] Singh, A, Nandal, A dan Malik, S (2012) International Journal of Advanced Research Computer Science and Software Engineering, Volume 2, Issue 12.

$$D(x) = a^{-1}(x-b) \bmod m \quad \text{.....} \quad (2.7)$$

Dimana a^{-1} adalah invers perkalian a modulus m yang dapat memenuhi persamaan sebagai berikut :

$$1 = aa^{-1} \bmod m \quad \text{.....} \quad (2.8)$$

Invers perkalian a hanya ada jika a dan m adalah *coprime*. Jika tidak maka proses algoritma akan terhenti. Fungsi dekripsi merupakan kebalikan dari fungsi enkripsi yang dapat dituliskan sebagai berikut:

$$\begin{aligned} D(E(P)) &= a^{-1}(E(P)-b) \bmod m \\ &= a^{-1}(((ax+b) \bmod m)-b) \bmod m \\ &= a^{-1}(ax+b-b) \bmod m \\ &= a^{-1}ax \bmod m \\ D(E(x)) &= x \bmod m \quad \text{.....} \quad (2.9) \end{aligned}$$

Contoh konkrit dari kegiatan dimana satu mengenkripsikan dan satu mendekripsikan dimana alfabet akan menjadi huruf A sampai Z dan akan memiliki nilai sesuai dengan Tabel 1 berikut ini

Table 2.1 Konversi Karakter ke Nilai Desimal

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2.9 Operasi Logika *Exclusive OR* (XOR)

Operator biner yang banyak digunakan dalam cipher yang yang beroperasi dalam mode bit adalah operasi logika XOR[17]. Notasi matematis operator XOR yaitu "⊕" . Operator

[17] Suhardi (2016) Jurnal Teknik dan Inovasi (Teknovasi), Vol 3 No. 2.

XOR dioperasikan pada dua bit dengan aturan sebagai berikut:

Tabel 2.2 Aturan Operasi XOR

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Contoh: 11100 ⊕ 10111 = 01010
hasilnya diperoleh sebagai berikut:

$$\begin{array}{cccccccccc} 1 & & 1 & & 1 & & 0 & & 0 & \\ 1 & & 0 & & 1 & & 1 & & 1 & \oplus \\ \hline 1 \oplus 1 & & 1 \oplus 0 & & 1 \oplus 1 & & 0 \oplus 1 & & 1 \oplus 0 & \\ 0 & & 1 & & 0 & & 1 & & 1 & \end{array}$$

2.10 Kriptografi Metode *Exclusive OR* (XOR)

Kriptografi metode *XOR* adalah teknik kriptografi (penyandian) yang menggunakan prinsip operasi logika XOR dalam proses enkripsi dan deskripsinya[18]. Algoritma enkripsinya dengan meng-*XOR*-kan plainteks (P) dengan kunci (K) menghasilkan cipherteks (C):

$$C = P \oplus K \quad \text{.....(2.10)}$$

Algoritma dekripsinya yaitu dengan meng-*XOR*-kan ciphertext (C) dengan kunci (K) menghasilkan plainteks (P):

$$P = C \oplus K \quad \text{.....(2.11)}$$

[18] Suhardi (2016) Jurnal Teknik dan Inovasi (Teknovasi), Vol 3 No. 2.

Sebagai contoh enkripsi yaitu kata “ILKOMPUINSU” akan dikonversi menggunakan Tabel 2.1 untuk nilai numerik dari setiap huruf. Berdasarkan formula dari enkripsi yang telah dijelaskan sebelumnya pada tinjauan pustaka maka dimisalkan a adalah 5, b adalah 20, dan m adalah 26 karena ada 26 karakter dalam alfabet yang digunakan. Nilai a yang terbatas karena *coprime* dengan 26. Nilai a yang mungkin adalah 1, 3, 5, 7, 11, 15, 17, 19, 21, 23, dan 25. Nilai untuk b bisa sembarangan sepanjang a tidak sama dengan 1 karena terjadi pergeseran cipher. Dengan demikian, fungsi enkripsi untuk contoh di atas adalah menjadi y = E(P) = (5x + 20) (mod 26). Tabel 2.3 tersebut menunjukkan hasil enkripsi pesan.

Tabel 2.3 Enkripsi Pesan

Plainteks	I	L	K	O	M	P	U	I	N	S	U
x	8	11	10	14	12	15	20	8	13	18	20
5x+20	60	75	70	90	80	95	120	60	85	110	120
(5x+20)(mod 26)	8	23	18	12	2	17	16	8	7	6	16
Cipherteks	I	X	S	M	C	R	Q	I	H	G	Q

Contoh dekripsi dimana cipherteks yang akan didekripsikan adalah cipherteks dari contoh enkripsi. Fungsi dekripsi secara matematis dapat dituliskan sebagai berikut:
D(y) = 21 (y – 20) mod 26. Nilai 21 adalah hasil dari a^{-1}, b adalah 20, dan m adalah 26.

Hasil proses dekripsi terhadap cipherteks seperti terlihat pada Tabel 2.4 Plainteks dekripsi adalah KRIPTOGRAFI.

Tabel 2.4 Dekripsi Pesan

Cipherteks	I	X	S	M	C	R	Q	I	H	G	Q
X	8	23	18	12	2	17	16	8	7	6	16
21(x-20)	-252	63	-42	-168	-378	-63	-84	-252	-273	-294	-84
(21(x-20)mod 26)	8	11	10	14	12	15	20	8	13	18	20
Plainteks	I	L	K	O	M	P	U	I	N	S	U

BAB III
METODE PENELITIAN

Penelitian kriptografi pesan menggunakan kombinasi metode *Affine Ciphers* dan *Exclusive-OR* (XOR) diharapkan bahwa pesan yang bersifat pribadi bagi pengguna dapat disampaikan kepada pengguna lain dengan aman dan pengguna yang tidak bertanggungjawab tidak dapat melihat pesan tersebut.

3.1 Teknik Pengumpulan Data

Pengumpulan data dilakukan terutama melakukan kajian pustaka yang berupa jurnal, buku, dan informasi lainnya dari internet yang berhubungan dengan topik yang akan dibahas. Teknik pengumpulan data tersebut dilakukan dalam rangka membangun latar belakang dan tinjauan pustaka terutama yang berkaitan dengan kriptografi

3.2 Metode Pembangunan Perangkat Lunak

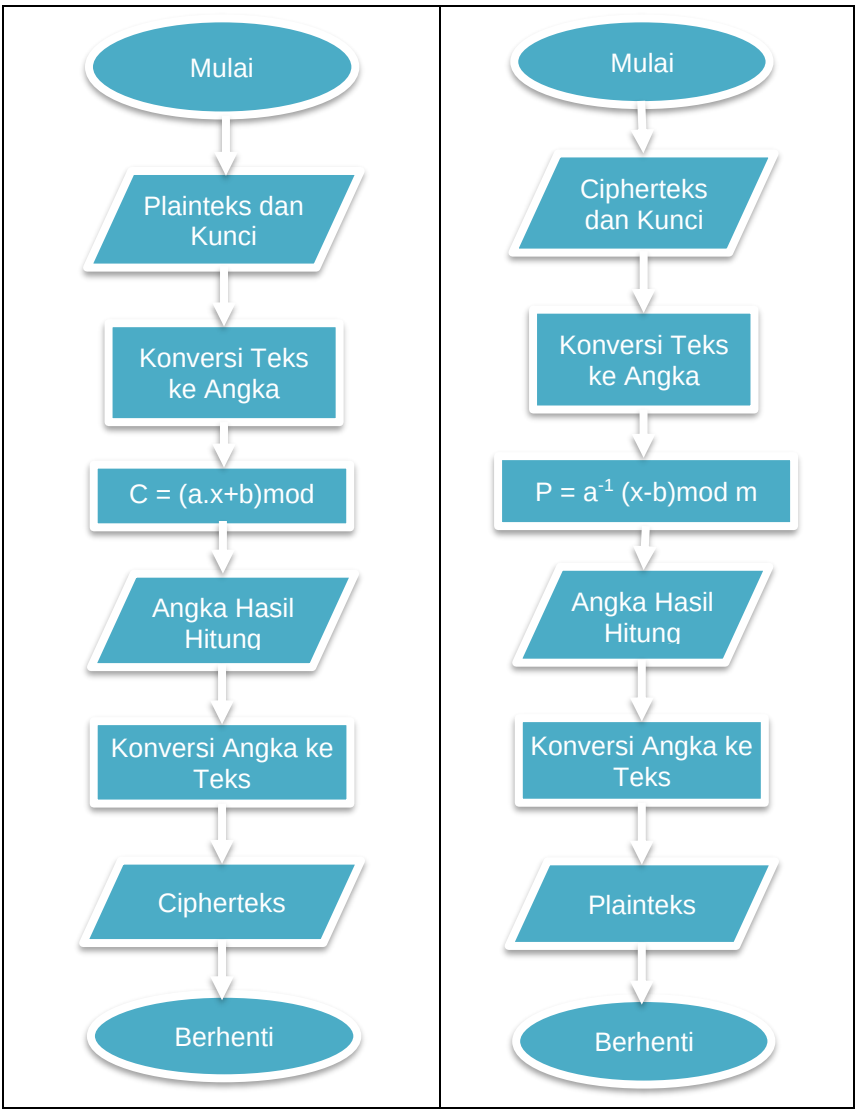
Dari teknik pengumpulan yang telah dijelaskan di atas maka dibangun suatu perangkat lunak menggunakan prinsip kriptografi menggunakan metode affine cipher. Tahapan-tahapan dalam membangun perangkat lunak kriptografi pesan menggunakan metode affine cipher dilakukan sebagai berikut:

a. Rekayasa dan pemodelan sistem dimana elemen sistem yang dibutuhkan pada perangkat lunak kriptografi pesan adalah seperangkat komputer yang dapat mendukung Adobe Dreamweaver CS 3, Javascript, browser Mozilla Firefox serta sistem operasi Windows 10 dan user yang bisa mengoperasikan komputer.

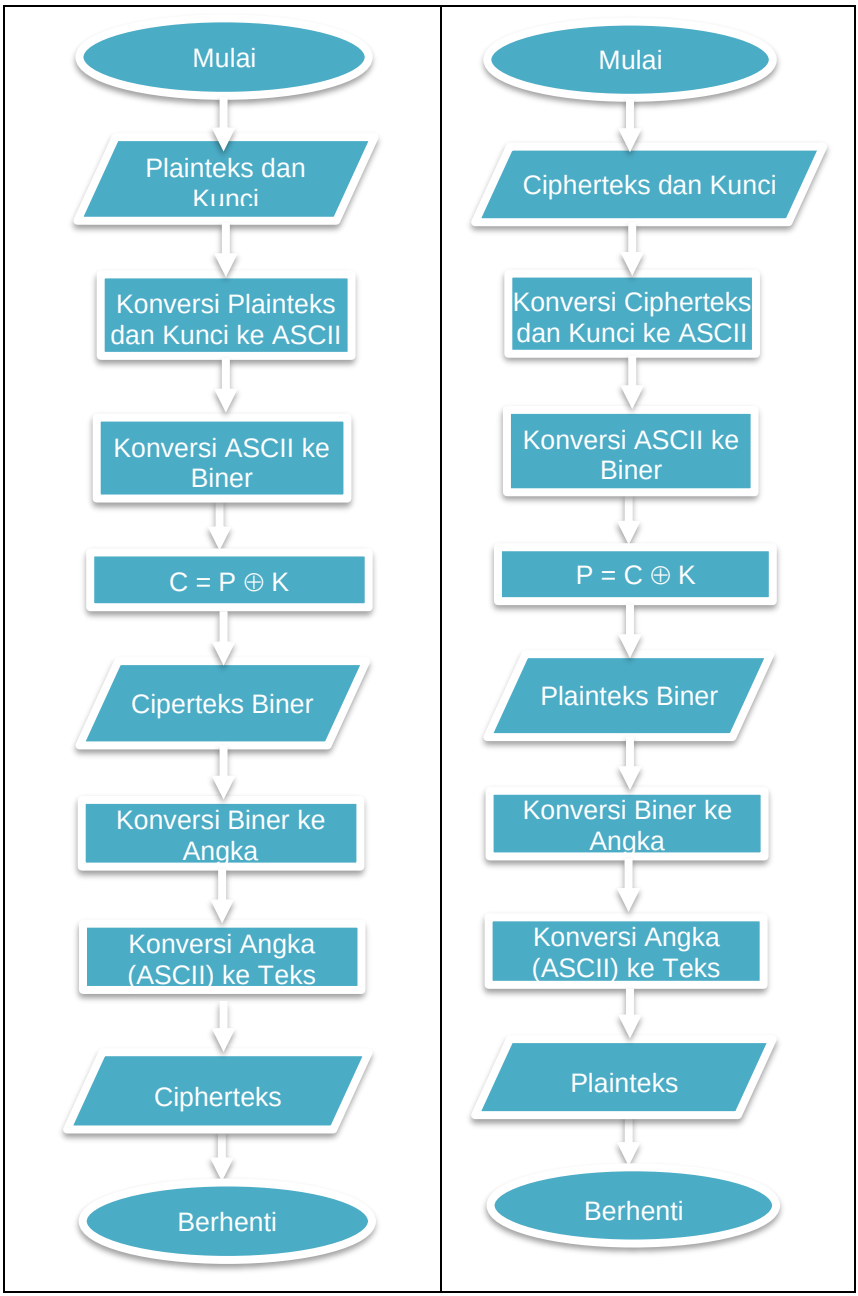
b. Analisa kebutuhan perangkat lunak kriptografi pesan berupa *State Transition Diagram* (STD, kebutuhan modul enkripsi yaitu menyiapkan plainteks dalam hal ini pesan yang selanjutnya disandikan ke bentuk lain agar tidak dapat dipahami oleh pihak lain (cipherteks). Kebutuhan modul dekripsi yaitu mentransformasikan kembali cipherteks ke plainteks semula.
c. Desain, menggunakan *flowchart* program dan perancangan antarmuka.
d. Implementasi, menggunakan Javascript.
e. Pengujian, teknik pengujian yang digunakan dengan metode *whitebox* dan *blackbox*

3.3 Proses Kombinasi Metode *Affine Cipher* dan XOR

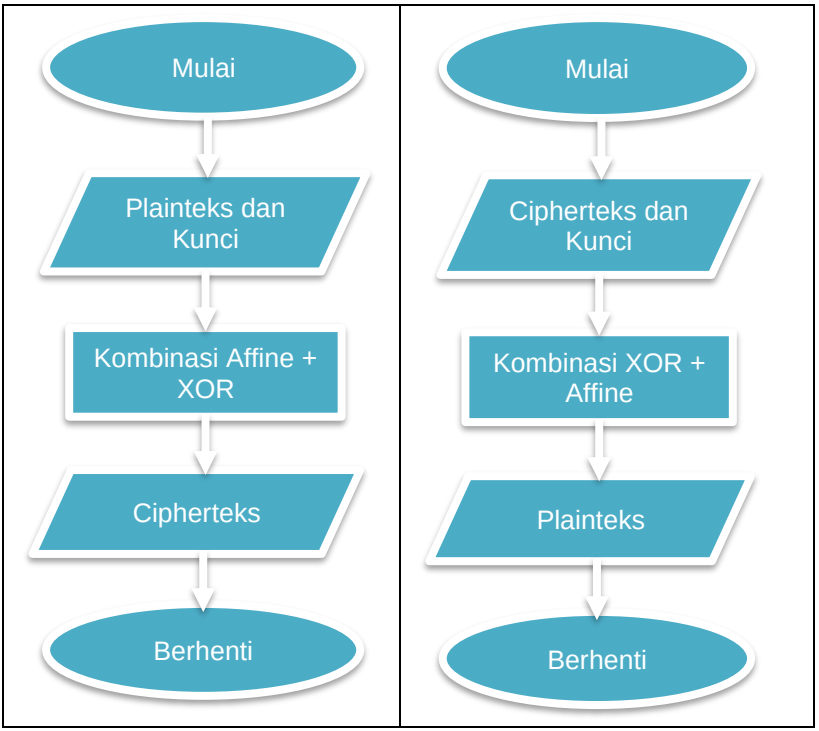
Proses kombinasi metode Affine Cipher dan XOR pada penelitian ini dimulai dengan proses enkripsi pesan menggunakan metode Affine Cipher terlebih dahulu sehingga dihasilkan Cipherteks. Cipherteks hasil enkripsi tersebut kemudian dienkripsikan kembali menggunakan metode XOR dengan mengubah Cipherteks dan kunci berupa teks menjadi ASCII dan kemudian diubah ke biner. Nilai biner Cipherteks akan di XOR-kan dengan nilai biner kunci sehingga dihasilkan Cipherteks kedua. Proses dekripsi akan dilakukan sebaliknya.



Gambar 3.1 *Flowchart* Enkripsi dan Dekripsi *Affine Cipher*



Gambar 3.2 *Flowchart* Enkripsi dan Dekripsi XOR



Gambar 3.3 *Flowchart* Kombinasi *Affine Cipher* dan XOR

BAB IV
HASIL DAN PEMBAHASAN

Telah dilakukan percobaan dan pengamatan untuk melihat proses kombinasi metode *Affine Cipher* dan *Exclusive-OR* (XOR) dengan melakukan rekayasa dan pemodelan sistem menggunakan bahasa pemrograman Javascript dan aplikasi *browser* maka proses yang dilakukan pada pemodelan sistem tersebut yaitu melakukan subsistem enkripsi dan subsistem dekripsi

4.1 Subsistem Enkripsi

Proses yang dilakukan pada sistem ini yaitu melakukan subsistem enkripsi

a. Kebutuhan input merupakan kebutuhan berupa masukan dari pengguna. Kebutuhan input pada subsistem enkripsi ini adalah pengguna memasukkan dua buah kunci dan plainteks (pesan).
b. Kebutuhan proses merupakan pemrosesan dari input yang diberikan oleh pengguna sampai menghasilkan *output* yang ditujukan untuk pengguna. Kebutuhan proses pada subsistem ini adalah melakukan enkripsi pesan yang diberikan pengguna.
c. Kebutuhan *output* merupakan hasil keluaran dari *input* yang diberikan oleh pengguna. Kebutuhan *output* pada subsistem ini adalah pesan yang terenkripsi (tidak terbaca).

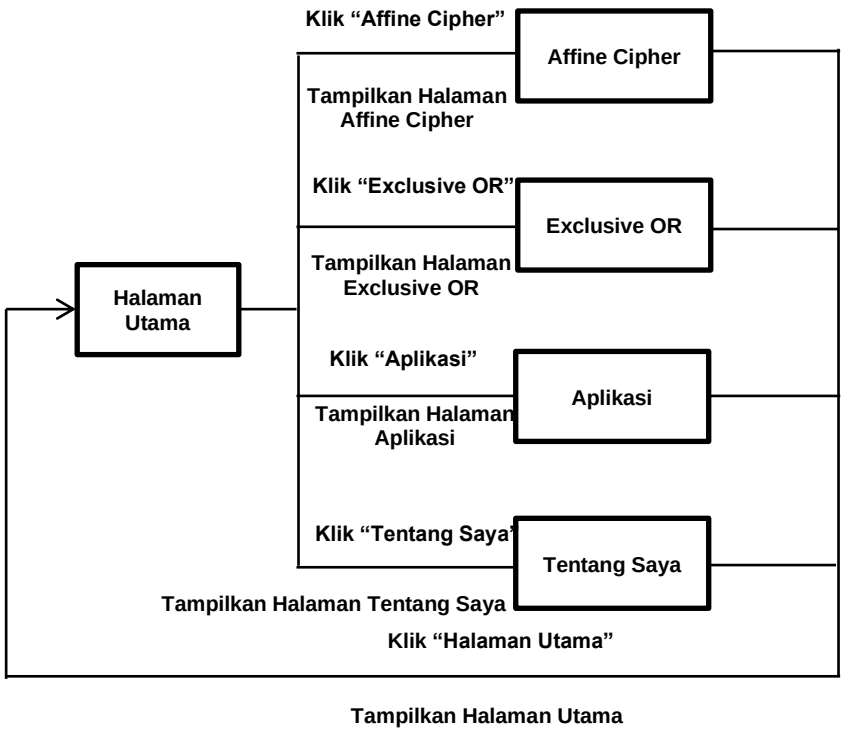
4.2 Subsistem Dekripsi

a. Kebutuhan input pada subsistem dekripsi ini adalah pengguna memasukkan dua buah kunci yang sama

ketika plainteks (pesan) dienkripsi dan pesan yang sudah terenkripsi.

b. Kebutuhan proses pada subsistem ini adalah melakukan dekripsi pesan yang dimasukkan pengguna.
c. Kebutuhan output pada subsistem ini adalah pesan yang telah terdekripsi (terbaca) untuk mengetahui kebenaran dari proses dekripsi tersebut.

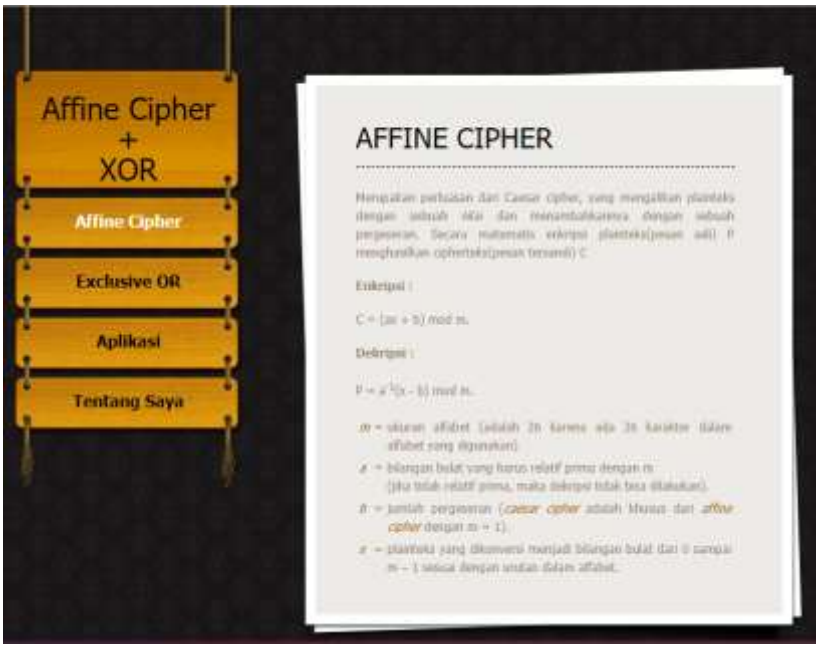
Model analisa kebutuhan menggunakan State Transition Diagram (STD) Kriptografi Password ditunjukkan pada Gambar 4.1.



Gambar 4.1 STD Kriptografi Pesan

4.3 Hasil Eksekusi Program

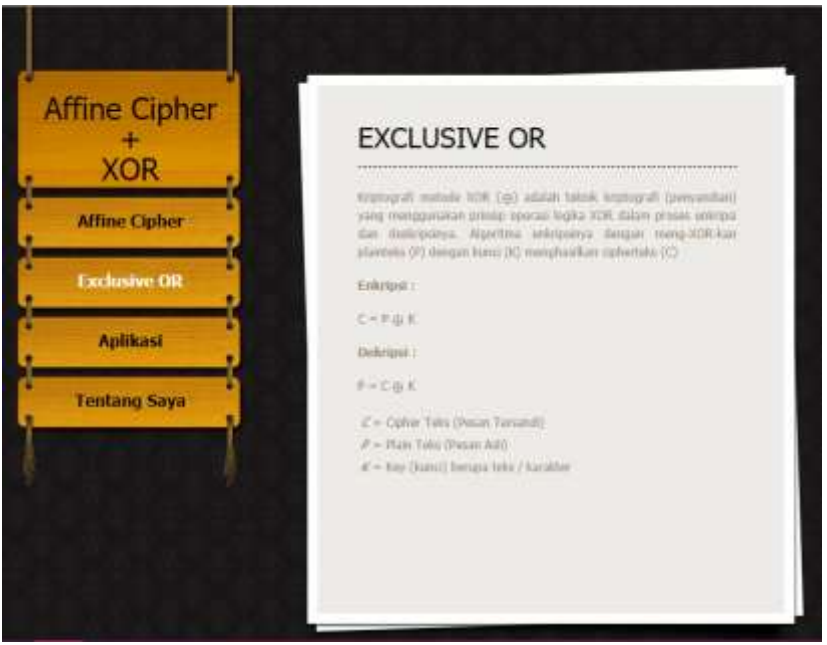
Jika perangkat lunak kriptografi ini dijalankan maka akan tampil halaman utama yang juga sebagai halaman *Affine Cipher* yang berisi tentang pengenalan *Affine Cipher* seperti pada gambar 4.2.



Gambar 4.2 Halaman Utama

4.3.1 Halaman *Exclusive OR*

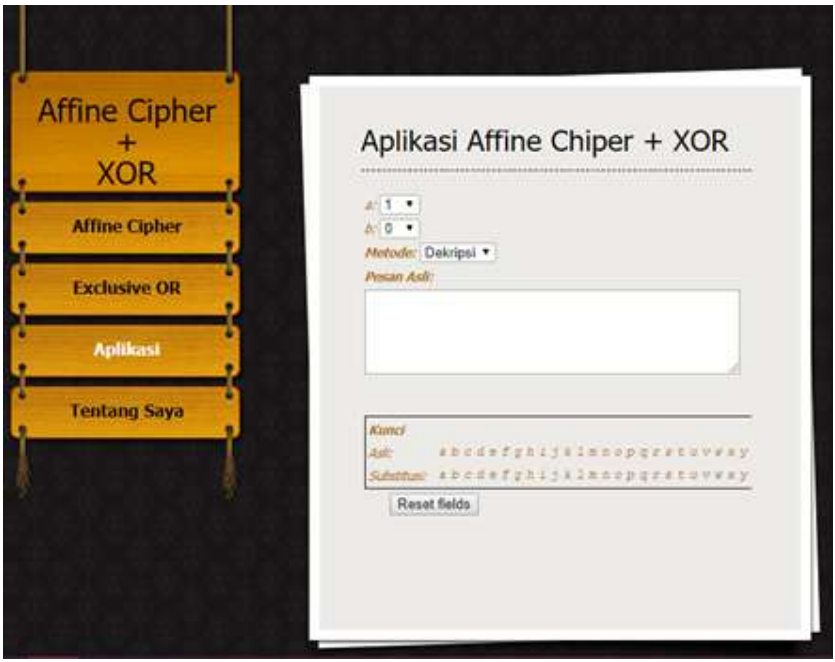
Pada halaman ini berisi tentang pengenalan metode kriptografi XOR yang akan dilihat pada gambar 4.3



Gambar 4.3 Halaman *Exclusive OR*

4.3.2 Halaman Aplikasi

Pada halaman Aplikasi pengguna diminta untuk memasukkan pesan yang ingin dienkripsi atau didekripsi. Kemudian pengguna diminta memasukan nilai a dan b sebagai nilai kunci enkripsi atau dekripsi. Kemudian pengguna diminta memilih metode antara enkripsi atau dekripsi. Setelah itu akan muncul pesan tersandi dan kunci pergeseran secara otomatis. Apabila pengguna ingin menginputkan pesan kembali maka pengguna dapat menekan tombol reset field. Tampilan halaman Aplikasi ditampilan pada gambar 4.4.



Gambar 4.4 Halaman Aplikasi

4.3.3 Halaman Tentang Saya

Pada halaman Tentang Saya merupakan profil singkat pembuat aplikasi yang merancang aplikasi affine cipher. Tampilannya akan ditampilkan pada gambar 4.5.

Gambar 4.5 Halaman Tentang Saya

BAB V
SIMPULAN DAN SARAN

5.1 Kesimpulan

1. Kombinasi metode kriptografi *Affine Cipher* dan *Exclusive-OR (XOR)* berjalan dengan baik dan tanpa mengalami kendala apapun baik dalam proses enkripsi maupun dekripsi.
2. Tingkat keamanan pada pesan teks jauh lebih baik dari sebelumnya dikarenakan proses enkripsi pesan terjadi dua kali dengan metode kriptografi yang berbeda
3. Kombinasi metode kriptografi dapat diimplementasikan ke dalam *Javascript*

5.2 Saran

Adapun saran dari penelitian ini sebagai acuan perkembangan riset selanjutnya adalah :

1. Untuk pengembangan selanjutnya diharapkan dapat melakukan penggabungan metode *Affine Cipher* dengan berbagai macam metode yang lain dalam proses enkripsi dan deskripsi datanya. Sehingga diperoleh pengamanan data yang lebih baik.
2. Perlu dilakukan rekayasa dan pemodelan sistem menggunakan bahasa pemrograman lainnya yang lebih baik.
3. Perlu dilakukan pengujian dan perbandingan terhadap waktu yang dibutuhkan untuk proses enkripsi dan dekripsi data sebelum dan setelah dilakukannya kombinasi algoritma kriptografi.

DAFTAR PUSTAKA

S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

Abraham, O. dan Shefiu, G.O. 2012. *An Improved Caesar Cipher (ICC) Algorithm*, International Journal of Engineering Science & Advanced Technology, Volume 2, Issue-5.: 1199-1202

Ariwibowo, E. 2008. *Aplikasi Pengamanan Dokumen Office dengan Algoritma Kriptografi Kunci Asimetri Elgamal*, Jurnal Informatika, Vol 2 No. 2.

Dey, S. 2012. SD-AREE : *A New Modified Caesar Cipher Cryptographic MethodAlong with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted*, Department of Computer

Science St. Xavier's College [Autonomous] Kolkata, West Bengal, India.

Goyal, D dan Srivastava, V. 2012. *RDA Algoritm: Symmeric Key Algoritm, International Journal of Information and Communication Technology Research*, Volume 2 No. 4.

Hadi, A. 2011. *Rancang Bangun Sistem Pengamanan Dokumen pada Sistem Informasi Akademik Menggunakan Digital Signature dengan Algoritma Kurva Eliptik,* [Tesis], Program Pascasarjana Universitas Diponegoro, Semarang.

Herryawan, I. P. 2010. *Aplikasi Keamanan Data Menggunakan Metode Kriptografi Gost*, Jurnal TSI, Vol. 1 No. 2.

Ibisa. 2011. *Keamanan Sistem Informasi*, Penerbit Andi, Yogyakarta.

ISO 7498-2 : *Security Architecture of OSI Reference Model*.

Kristanto, A. 2003. *Keamanan Data pada Jaringan Komputer*, Edisi Pertama, Penerbit Gava Media, Yogyakarta.

Munir, R. 2006. *Kriptografi*, Cetakan Pertama, Penerbit Informatika, Bandung.

Nugroho, A. 2012. *Implemantasi Algoritma Caesar Cipher ROT13 dan BASE64 untuk Enkripsi dan Dekripsi Pesan SMS pada Handphone Berbasis Android*, [Skripsi], Sekolah Tinggi Manajemen Informatika dan Komputer Amikom, Yogyakarta.

Pressman, R.S. 1997. *Software Engineering a Practitioner's Approach*, 4th edition,McGraw-Hill International Editions, New York.

Rahajoeningroem, T dan Aria, M. 2009. *Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa*, Majalah Ilmiah UNIKOM, Vol8 No. 1.

Rahayu, T. P, Yakub, dan Limiady, I. 2012. *Aplikasi Enkripsi Pesan Teks (SMS) pada Perangkat Handphone dengan Algoritma Caesar Cipher*, Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA) Yogyakarta.

Saroha, V, Mor, S dan Dagar, A. 2012. *Enhancing Security of Caeser Cipher by Double Columnar Transposition Method, International Journal of Advanced Research Computer Science and Software Engineering*, Volume 2, Issue 10.

Septiarini, A dan Hamdani. 2011. *Sistem Kriptografi untuk Text Message Menggunakan Metode Affine*, Jurnal Informatika Mulawarman, Vol 6 No. 1.

Singh, A, Nandal, A dan Malik, S. 2012. *Impementation of Caesar Cipher with Rail Fence for Enhancing Data*

Security, International Journal of Advanced Research Computer Science and Software Engineering, Volume 2, Issue 12.

Suhardi. 2016. *Implementasi Algoritma Affine Cipher Pada Record Tabel Database,* Prosiding Seminar Nasional Inovasi dan Teknologi Informasi (SNITI-3).

Suhardi. 2016. *Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-Or (XOR),* Jurnal Teknik dan Inovasi (Teknovasi), Vol3 No. 2.

Suhardi, Saib, S dan Erna, B. N. 2017. *Use Of One Time Pad Algorithm For Bit Plane Security Improvement,* International Conference on Information and Communication Technology (IconICT).

Srikantaswamy, S. G dan Phaneendra, H. D. 2012. *Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption*, International Journal on Cryptography and Information Security (IJCIS), Vol 2 No. 4.

Wahana Komputer, 2004. *Tutorial Membuat Program dengan Visual Basic*, Edisi Pertama, Penerbit Salemba Infotek.

Wardiana, W dan Heryana, A. 2008. *Penerapan Algoritma Kriptografi Kunci Publik sebagai Pengamanan Sistem Distribusi Perangkat Lunak Lipirism*, Prosiding Seminar Nasional Teknoin, Bidang Teknik Informatika, Yogyakarta.

Wirdasari, D. 2008. *Prinsip Kerja Kriptografi dalam Mengamankan Informasi*, Jurnal Saintikom, Vol. 5 No. 2.