Jurnal Mahajana Informasi. Vol. 5, No. 1, Juni 2020
e-ISSN : 2527-8290

PENYANDIAN TEKS DENGAN KOMBINASI VERNAM CIPHER DAN CAESAR CIPHER 220

Legito
Program Studi Teknik Informatika Sekolah Tinggi Teknologi Sinar Husni Helvetia
Jalan Veteran Gg.Utama, pasar V, Helvetia
legito@sttsinarhusni.ac.id

Abstrak

Pertukaran informasi yang digunakan orang-orang adalah sebuah bentuk kalimat ataupun teks (*text*), yang dapat di baca oleh orang-orang yang menerima informasi. Untuk itu diperlukan sebuah sistem untuk mengamankan isi pesan teks. Pada sistem ini isi pesan teks dapat disandikan, sehingga tidak dapat terbaca oleh pencuri informasi, dua metode yaitu metode *vernam cipher* dan metode *caesar cipher* agar keamanan datanya lebih terjaga.kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* yang berasal dari hasil *XOR* antara bit *plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode *ASCII* dan kemudian dikenakan operasi *XOR* terhadap kunci yang sudah diubah ke dalam kode *ASCII.* (Sholeh dan Hamokwarong, 2011). Dalam kriptografi, sandi *Caesar*, atau sandi geser, kode *Caesar* atau Geseran *Caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada *Caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama.
Kata Kunci : Kombinasi vernam cipher , caesar cipher 220

1. PENDAHULUAN

Pertukaran informasi yang digunakan orang-orang adalah sebuah bentuk kalimat ataupun teks (*text*), yang dapat di baca oleh orang-orang yang menerima informasi. Namun hal ini dapat membahayakan pemberi informasi, apabila pengirim informasi tidak menginginkan informasi yang dia kirim diketahui oleh pencuri informasi ataupun pihak ketiga.Untuk itu diperlukan sebuah sistem untuk mengamankan isi pesan teks. Pada sistem ini isi pesan teks dapat disandikan, sehingga tidak dapat terbaca oleh pencuri informasi.

Namun di dalam penerapannya dibutuhkan metode untuk menyelesaikan masalah di dalam keamanan data. Untuk itu penulis merekomendasikan dua metode yaitu metode *vernam cipher* dan metode *caesar cipher* agar keamanan datanya lebih terjaga. Metode *vernam cipher* atau biasa dikenal dengan sebutan *one time pad* (OTP) merupakan algoritma berjenis *symmetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* yang berasal dari hasil XOR antara bit *plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode ASCII dan kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII.

2. TINJAUAN TEORI

2.1. Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi. (Sadikin, 2012).

2.2. *Caesar Cipher*

Dalam kriptografi, sandi *Caesar*, atau sandi geser, kode *Caesar* atau Geseran *Caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan

oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada *Caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf (yaitu 3). (Seftyanto, dkk, 2012).

2.3. *Vernam Cipher*

Algoritma *vernam cipher* atau biasa dikenal dengan sebutan *one time pad* (*OTP*) merupakan algoritma berjenis *symmetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* yang berasal dari hasil *XOR* antara bit *plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode *ASCII* dan kemudian dikenakan operasi *XOR* terhadap kunci yang sudah diubah ke dalam kode *ASCII*. (Sholeh dan Hamokwarong, 2011).

2.4. *Visual Basic* 2010

Visual Basic 2010 merupakan salah satu bagian dari produk pemrograman terbaru yang dikeluarkan oleh *Microsoft*, yaitu *Microsoft Visual Studio 2010*. *Visual Studio* merupakan produk pemrograman andalan dari *mocrosoft corporation*, dimana di dalamnya berisi beberapa jenis *IDE* pemrograman seperti *Visual Basic*, *Visual C++*, *Visual Web Developer*, *Visual C#,* dan *Visual F#*.

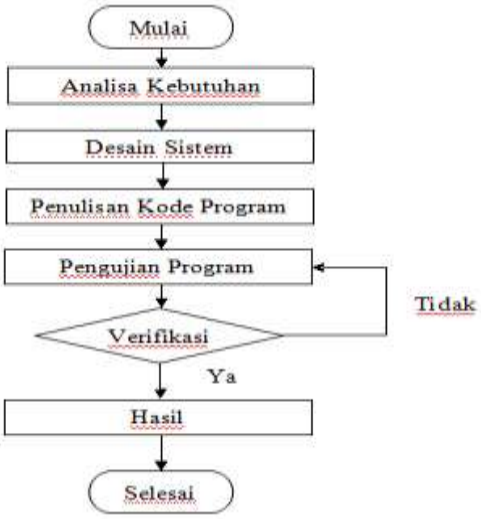
Semua *IDE* pemrograman tersebut sudah mendukung penuh implementasi *.Net Framework* terbaru, yaitu *.Net Framework 4.0* yang merupakan pengembangan dari *.Net Framework 3.5*. Adapun database standar yang disertakan adalah *Microfot SQL Server 2008 express*.

Visual Basic 2010 merupakan versi perbaikan dan pengembangan dari versi pendahulunya yaitu *visual basic 2008*. Beberapa pengembangan yang terdapat di dalamnya antara lain dukungan terhadap *library* terbaru dari *Microsoft*, yaitu *.Net Framework 4.0,* dukungan terhadap pengembangan aplikasi menggunakan *Microsoft SilverLight*, dukungan terhaddap aplikasi berbasis *cloud computing*, serta perluasan dukungan terhadap *database-database*, baik *standalone* maupun *database server.* (Wahana Komputer, 2011).

3. METODE PENELITIAN

3.1 Kerangka Penelitian

Tahapan dalam menyelesaikan penelitian ini, peneliti menggunakan kerangka penelitian dalam bentuk *flowchart* sebagai berikut :



Gambar 1. Flow Chart Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data tentang kriptografi. Pada tahapan ini juga ditentukan *software* dan *hardware* yang akan digunakan untuk mengimplementasikan dan menguji hasil penelitian. Berdasarkan data-data yang ada ini kemudian dilakukan tahap selanjutnya, yaitu desain sistem.

Berikut adalah *software* yang digunakan untuk pembuatan sistem :

a. Sistem operasi *windows* 7
b. *Visual Basic* 2010

Berikut adalah *hardware* yang digunakan untuk penerapan sistem :

a. *Laptop/ Computer*
b. *Hardisk*

2. Desain Sistem

Pada tahap ini dilakukan desain perangkat lunak secara teori menggunakan pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram* dan desain perangkat lunak secara praktek menggunakan *Viusal Basic* 2010.

3. Penulisan Kode Program

Kode program merupakan terjemahan *design* dalam bahasa yang bisa dikenali komputer. Pada tahap ini desain sistem diimplementasikan ke dalam kode program. Pemrograman dimulai dengan bahasa pemrograman *Visual Basic* 2010.

4. Pengujian Program

Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik.

5. Hasil

Pada tahap ini program sudah berjalan dengan baik dan sudah sesuai dengan rancangan yang dibuat.

4. ANALISIS dan HASIL

4.1. Uraian Umum Tentang Sistem

Berikut ini adalah uraian umum tentang Kombinasi Metode *Vernam Cipher* Dan *Caesar Cipher* 220 Dalam Penyandian Text :

4.1.1. Metode *Vernam Cipher*

Algoritma *vernam cipher* atau biasa dikenal dengan sebutan *one time pad* (OTP) merupakan algoritma berjenis *symmetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* yang berasal dari hasil XOR antara *bit plaintext* dan *bit key*. Pada metode ini plain text diubah kedalam kode ASCII dan kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASC2.

4.1.1.1. Enkrip Metode *Vernam Cipher*

Berikut ini adalah enkrip dari metode *Vernam Cipher*, enkrip metode *Vernam Cipher* menggunakan xor *ascii plaintext* dengan *ascii* kunci dan dimoduluskan dengan nilai 256 sebagai berikut :

$C_i = (P_i \text{ xor } K_i) \bmod 256$

Keterangan :

C_i = *Ciphertext* hasil enkrip
P_i = *Plaintext* yang akan dienkrip
K_i = Kunci untuk proses enkrip
Mod = Sisa Bagi/Modulus

Contoh Proses Enkripsi :
Plaintext : Sinar Husni
Kunci : STT
Solusi :
Ascii Plaintext :
S = 83
i = 105
n = 110
a = 97
r = 114
= 32
H = 72
u = 117
s = 115
n = 110
i = 105
Key :
S = 83
T = 84
T = 84

C1 = (S xor k1) mod 256
= (83 xor 83) mod 256
= 0 mod 256
= 0
C2 = (i xor k2) mod 256
= (105 xor 84) mod 256
= 61 mod 256
= 61
C3 = (n xor k3) mod 256
= (110 xor 84) mod 256
= 58 mod 256
= 58
C4 = (a xor k1) mod 256
= (97 xor 83) mod 256
= 50 mod 256
= 50
C5 = (r xor k2) mod 256
= (114 xor 84) mod 256
= 38 mod 256
= 38
C6 = (xor k3) mod 256
= (32 xor 84) mod 256
= 116 mod 256
= 209
C7 = (H xor k1) mod 256
= (72 xor 83) mod 256
= 27 mod 256
= 27
C8 = (u xor k2) mod 256
= (117 xor 84) mod 256
= 33 mod 256
= 33
C9 = (s xor k3) mod 256
= (115 xor 84) mod 256

= 39 mod 256
= 39
C10 = (n xor k1) mod 256
= (110 xor 83) mod 256
= 61 mod 256
= 61
C11 = (i xor k2) mod 256
= (105 xor 84) mod 256
= 61 mod 256
= 61
Ascii Chipertext : 0, 61, 58, 50, 38, 116, 27, 33, 39, 61, 61

4.1.1.2. Dekrip Metode *Vernam Cipher*

Berikut ini adalah dekrip dari metode *Vernam Cipher*, dekrip metode *Vernam Cipher* menggunakan xor *ascii ciphertext* dengan *ascii* kunci dan dimoduluskan dengan nilai 256 sebagai berikut :

$P_i = (C_i \text{ xor } K_i) \bmod 256$

Keterangan :
C_i = *Ciphertext* yang akan didekrip
P_i = *Plaintext* hasil dekrip
K_i = Kunci untuk proses dekrip
Mod = Sisa Bagi/Modulus

Contoh Proses Dekripsi :
P1 = (C1 xor k1) mod 256
= (0 xor 83) mod 256
= 83 mod 256
= 83
P2 = (i xor k2) mod 256
= (61 xor 84) mod 256
= 105 mod 256
= 105
C3 = (n xor k3) mod 256
= (58 xor 84) mod 256
= 110 mod 256
= 110
C4 = (a xor k1) mod 256
= (50 xor 83) mod 256
= 97 mod 256
= 97
C5 = (r xor k2) mod 256
= (38 xor 84) mod 256
= 114 mod 256
= 114
C6 = (xor k3) mod 256
= (116 xor 84) mod 256
= 32 mod 256
= 32
C7 = (H xor k1) mod 256
= (27 xor 83) mod 256
= 72 mod 256
= 72
C8 = (u xor k2) mod 256
= (33 xor 84) mod 256
= 117 mod 256
= 117
C9 = (s xor k3) mod 256
= (39 xor 84) mod 256
= 115 mod 256
= 115
C10 = (n xor k1) mod 256
= (61 xor 83) mod 256
= 110 mod 256
= 110
C11 = (i xor k2) mod 256
= (61 xor 84) mod 256
= 105 mod 256
= 105
Plaintext : Sinar Husni

4.1.2. Metode *Caesar Cipher*

Dalam kriptografi, sandi *Caesar*, atau sandi geser, kode *Caesar* atau Geseran *Caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada *Caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf.

4.1.2.1. Enkrip Metode *Caesar Cipher*

Berikut ini adalah enkrip dari metode *Caesar Cipher*, enkrip metode *Caesar Cipher* menggunakan penambahan 220 pada *ascii plaintext* sebagai berikut :

$C_i = P_i + 220$

Keterangan :
C_i = *Ciphertext* hasil enkrip
P_i = *Plaintext* yang akan dienkrip

Contoh Proses Enkripsi :
Plaintext : Sinar_Husni
Kunci : 3
Solusi :
Ascii Plaintext :
S = 83
i = 105
n = 110
a = 97
r = 114
_ = 133
H = 72
u = 117

s = 115
n = 110
i = 105
Key :
Kunci = 3
C1 = (S + 3)
= (83 + 3)
= 86
C2 = (i + 3)
= (105 + 3)
= 108
C3 = (n + 3)
= (110 + 3)
= 113
C4 = (a + 3)
= (97 + 3)
= 100
C5 = (r + 3)
= (114 + 3)
= 117
C6 = (_ + 3)
= (133 + 3)
= 136
C7 = (H + 3) mod 256
= (72 + 3)
= 75
C8 = (u + 3)
= (117 + 3)
= 120
C9 = (s + 3)
= (115 + 3)
= 118
C10 = (n + 3)
= (110 + 3)
= 113
C11 = (i + 3)
= (105 + 3)
= 108
Ascii Chipertext : 86, 108, 113, 100, 117, 136, 75, 120, 118, 113, 108

4.1.2.2. Dekrip Metode *Caesar Cipher*

Berikut ini adalah dekrip dari metode *Caesar Cipher*, dekrip metode *Caesar Cipher* menggunakan pengurangan 220 pada *ascii ciphertext* sebagai berikut :

$P_i = C_i - 220$

Keterangan :
P_i = *Plaintext* hasil dekrip
C_i = *Ciphertext* yang akan didekrip

Contoh Proses Dekripsi :
Kunci = 3
P1 = (C1 - 3)
= (86 - 3)
= 83
P2 = (C2 - 3)
= (108 - 3)
= 105
P3 = (C3 - 3)
= (113 - 3)
= 110
P4 = (C4 - 3)
= (100 - 3)
= 97
P5 = (C5 - 3)
= (117 - 3)
= 114
P6 = (C6 - 3)
= (136 - 3)
= 133
P7 = (C7 - 3) mod 256
= (75 - 3)
= 72
P8 = (C8 - 3)
= (120 - 3)
= 117
P9 = (C9 - 3)
= (118 - 3)
= 115
P10 = (C10 - 3)
= (113 - 3)
= 110
P11 = (C11 - 3)
= (108 - 3)
= 105
Plaintext : Sinar_Husni

4.1.4. Kombinasi Metode *Vernam Cipher* Dan *Caesar Cipher*

Kombinasi metode *Vernam Cipher* dan *Caesar Cipher* adalah ide dari penulis untuk mengembangkan metode kriptografi yang lama sehingga keamanannya lebih kuat.

4.1.4.1. Enkrip Kombinasi Metode *Vernam Cipher* Dan *Caesar Cipher*

Berikut ini adalah enkrip dari kombinasi metode *Vernam Cipher* dan *Caesar Cipher*, enkrip kombinasi metode *Vernam Cipher* dan *Caesar Cipher* menggunakan penggabungan dari metode *Vernam Cipher* dan *Caesar Cipher* sebagai berikut :

$C_{iVernam} = (P_i \text{ xor } K_i) \bmod 256$
$C_{iCaesar\ Cipher} = \text{mid}(C_{iVernam}, i, 1) + 220$

Contoh Proses Enkripsi :
Plaintext : S
Kunci : S

Solusi :
Ascii Plaintext :
S = 83
Key Vernam Cipher :
S = 83
Key Caesar Cipher :
Kunci = 220
C1 = (S xor k1) + 220 mod 256
= (83 xor 83) + 220 mod 256
= 0 + 220 mod 256
= 220 = Ü

4.1.4.2. Dekrip Kombinasi Metode *Vernam Cipher* Dan *Caesar Cipher*

Berikut ini adalah dekrip dari kombinasi metode *Vernam Cipher* dan *Caesar Cipher*, dekrip kombinasi metode *Vernam Cipher* dan *Caesar Cipher* menggunakan penggabungan dari metode *Vernam Ciper* dan *Caesar Cipher* sebagai berikut :

$P_{iCaesar\ Cipher}$ = mid(C_i, i, 1) - 220
$P_{iVernam}$ = ($P_{iCaesarCipher}$ xor K_i) mod 256

Contoh Proses Enkripsi :
Plaintext : Ü
Kunci : S
Solusi :
Ascii Plaintext :
Ü = 220
Key Vernam Cipher :
S = 83
Key Caesar Cipher :
Kunci = 220
P1 = (Ü -220) xor k1 mod 256
= (220 – 220) xor 83 mod 256
= 83 mod 256
= 83 = S

5. KESIMPULAN dan SARAN

5.1. Kesimpulan

Berdasarkan pembahasan yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Dengan menggunakan pemrograman *Visual Basic* 2010 dan menerapkan metode *Vernam Cipher* dan *Caesar Cipher* ke dalam system yang di buat maka dapat menghasilkan aplikasi penyandian isi pesan teks.
2. Dengan merubah pesan asli ataupun karakter asli menjadi kode *Ascii* kemudian menerapkan rumus dari metode *Vernam Cipher* dan *Caesar Cipher* maka dapat menyandikan isi pesan teks.
3. Dengan menambahkan nilai *Ascii* sebanyak 220 pada hasil perhitungan metode *Vernam Cipher* maka dapat menghasilkan kombinasi dari metode *Vernam Cipher* dan metode *Caesar Cipher*.

5.2. Saran

Untuk pengembangan lebih lanjut pada Aplikasi Kombinasi Metode *Vernam Cipher* Dan *Caesar Cipher* 220 Dalam Penyandian *Text* ini, maka terdapat beberapa saran sebagai berikut :

1. Diharapkan dapat mengkombinasikan metode kriptografi lain agar menghasilkan algoritma keamanan yang lebih kuat.
2. Aplikasi Kombinasi Metode *Vernam Cipher* Dan *Caesar Cipher* 220 Dalam Penyandian *Text* dapat diterapkan untuk keamanan data selain pesan teks *SMS*.
3. Diharapkan dapat mengembangkan dan menciptakan metode kriptografi yang baru.

DAFTAR PUSTAKA

1. Abdul Kadir, 2014, ***Pengenalan Sistem Informasi,*** Penerbit Andi, Yogyakarta.
2. Ernita Sitohang, 2013, "**Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook Dengan Algoritma Des"**, STMIK Budi Darma Medan, Jurnal Pelita Informatika, Vol. 5, No. 3.
3. Hanifah Azhar, 2012, "**Perbandingan Algoritma Fungsi Hash MD5 dengan SHA-1"**, Institut Teknologi Bandung, Jurnal Kriptografi, Vol. 1, No. 1.
4. Rifki Sadikin, 2012, ***Kriptografi Untuk Keamanan Jaringan***, Penerbit Andi, Yogyakarta.
5. Seftyanto, dkk, 2012, "**Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi**", Sekolah Tinggi Sandi Negara, Jurnal Prosiding, Vol. 1, No. 1.
6. Sholeh Dan Hamokwarong, 2011**, Jurnal : Aplikasi Kriptografi Dengan Metode *Vernam Cipher* Dan Metode Permutasi Biner.** Fakultas Teknologi

Industri Institut Sains & Teknologi AKPRIND, Yogyakarta. , Jurnal Momentum, Vol. 7, No. 2.

7. Taupik K, dkk, 2013, "**Pembuatan Aplikasi Anbiyapedia Ensiklopedi Muslim Anak Berbasis Web**", UIN, Jurnal Edisi Juli 2013, Vol. 7, No. 1.