Implementasi Multi Enkripsi Algoritma *Vigenere Cipher* dan *Cipher Block Chaining* (CBC) untuk Pengamanan Data Pegawai

Mohammad Hafitz Firmansyah, Gusti Eka Yuliastuti, Citra Nurina Prabiantissa

Institut Teknologi Adhi Tama Surabaya
e-mail: hafisfiermansyah@gmail.com

ABSTRACT

The Sugio District Office, located in Lamongan City on the Sugio-Kedungpring highway, is in charge of providing services to residents and storing a lot of data. There are various important pieces of data that no one else can know other than the person concerned, such as employee or staff data. However, the data is stored without a security system. Cryptography is a technique to secure data, including maintaining data integrity and confidentiality and increasing data security. In this study, the authors chose a cryptographic algorithm for compiling this final project, namely the Vigenere Cipher and Cipher Block Chaining (CBC) algorithms for securing data. The test results obtained an average Avalanche Effect for the Vigenere Cipher of 14.14%, the CBC of 64.53%, and the combined Vigenere Cipher and CBC of 66.31%, meaning that the combined method of the two Vigenere Cipher and CBC algorithms was better. In conclusion, the combined method of both Vigenere Cipher and CBC algorithms was better than the single method in data security, with an Avalanche Effect testing result of 66.31%.

Kata kunci: *Avalanche Effect, CBC, decryption, encryption, Vigenere Cipher*.

ABSTRAK

Kantor Kecamatan Sugio merupakan salah satu kantor kecamatan yang berada di kota Lamongan yang beralamat di jalan raya Sugio Kedungpring yang bertugas memberi pelayanan pada warga dan menyimpan banyak data terdapat berbagai data penting sehingga tidak boleh ada orang lain yang mengetahuinya selain yang bersangkutan, salah satunya seperti data pegawai atau staff. Data tersebut hanya disimpan tanpa adanya sistem keamanan. Kriptografi merupakan teknik yang digunakan untuk mengamankan data, termasuk menjaga integritas dan kerahasiaan data, serta meningkatkan keamanan data. Pada penelitian ini, penulis memilih sebuah algoritma kriptografi dalam menyusun tugas akhir ini, yaitu algoritma *Vigenere Cipher* dan *Cipher Block Chaining* (CBC) untuk implementasi dalam mengamankan data. Berdasarkan hasil pengujian, didapatkan hasil rata-rata *Avalanche Effect* untuk *Vigenere Cipher* sebesar 14,14%, CBC sebesar 64,53%, dan Gabungan *Vigenere Cipher* dan CBC sebesar 66,31% yang berarti metode gabungan dua algoritma *Vigenere Cipher* dan CBC lebih baik. Dari hasil penelitian ini menyimpulkan bahwa dengan metode gabungan dua algoritma *Vigenere Cipher* dan CBC lebih baik dari metode tunggal dalam keamanan data dengan hasil pengujian *Avalanche Effect* sebesar 66,31%.

Kata kunci: Avalanche Effect, CBC, Dekripsi, Enkripsi, Vigenere Cipher.

PENDAHULUAN

Kantor Kecamatan Sugio merupakan salah satu kantor kecamatan yang berada di kota Lamongan yang beralamat di Jl. Raya Sugio - Kedungpring yang bertugas memberi pelayanan pada warga dan menyimpan banyak data terdapat berbagai data penting sehingga tidak boleh ada orang lain yang mengetahuinya selain yang bersangkutan, salah satunya seperti data pegawai atau staff. Data tersebut hanya disimpan tanpa adanya sistem keamanan.[1].

Kriptografi merupakan teknik yang digunakan untuk mengamankan data, termasuk menjaga integritas dan kerahasiaan data, serta meningkatkan keamanan data. [2]. Algoritma *vigenere* merupakan algoritma kriptografi klasik. Algoritma *Vigenere*, juga dikenal sebagai

Vigenere Cipher adalah pengembangan dari *Caesar Cipher* yang termasuk pada jenis metode kriptografi substitusi. [3]. Algoritma Cipher Block Chaining (CBC) merupakan penerapan mekanisme umpan balik pada sebuah blok bit dimana hasil enkripsi blok sebelumnya diumpan balikkan ke dalam proses enkripsi blok current. [4].

Pada penelitian ini, akan digunakan algoritma Vigenere Cipher dan CBC untuk implementasi dalam mengamankan data teks, karena algoritma vigenere cipher hanya dapat mengenkripsi karakter huruf sedangkan data pegawai memiliki karakter lain seperti nomor dan simbol, jadi untuk mengatasi kelemahan vigenere penulis mengambil metode kedua yaitu CBC untuk mengenkripsi karakter yang tidak bisa di enkripsi vigenere cipher.

TINJAUAN PUSTAKA

Kriptografi

Kriptografi berasal dari kata "*Crypto*" yang memiliki arti "rahasia" dan *"graphy*" yang memiliki arti "tulisan". Kriptografi pada komputasi definisikan ilmu dan seni menjaga keamanan informasi atau data. Ahli kriptografi disebut kriptografer[5]. Kriptografi juga memiliki arti yaitu ilmu teknik matematis yang berkaitan dengan *data security*, seperti integritas, keamanan, serta outentikasi data. Kata "seni" di atas mengacu pada metode bagaimana data dirahasiakan. Didalam "*cryptography*" sendiri, kata "*graphy*" sendiri mengacu pada seni[6].

Terdapat 4 komponen utama dari kriptografi antara lain:

a. *Plaintext*, berarti pesan dapat dibaca.
b. *Ciphertext*, berarti pesan tersandi yang sulit dibaca.
c. *Key*, berarti sebuah kunci proses kriptografi.
d. Algoritma, berarti metode untuk enkripsi dan dekripsi[7].

4 tujuan yaitu dari kriptografi ialah:

a. Kerahasiaan (*confidentiality*), merupakan fasilitas bertujuan untuk melindungi kerahasiaan pesan sehingga orang yang tidak berwenang tidak akan bisa memahami kandungan dari pesan tersebut.
b. Integritas data (*data integrity*), merupakan fasilitas yang bertujuan untuk memastikan bahwa data tidak dimanipulasi atau diubah membantu menjamin bahwa isi pesan tetap asli dan terjaga kerahasiaannya saat pesan dikirimkan.
c. Otentikasi (*authentication*), merupakan fasilitas untuk melakukan verifikasi keaslian dan kebenaran tentang sumber pesan yangrmelakukan komunikasi.
   Nir penyangkalan (*non-repudiation*), merupakan fasilitas untuk mencegah penyangkalan terjadi saat proses pengiriman informasi[1].

Vigenere Cipher

Vigenere Cipher dalam kriptografi merupakan teknik pengkodean. Enkripsi pada metode ini dilakukan menggunakan tabel diagram yang huruf alfabetnya disusun secara diagonal. Selanjutnya, kita akan menuliskan *plaintext* di bagian atas, dan kunci di sebelah kiri. Kemudian dicari perpotongan huruf tersebut dan menghasilkan *chipertext* yang di inginkan, begitu seterusnya sampai *plaintext* terakhir. Jika jumlah kunci tidak cukup untuk mencakup semua huruf pada *plaintext*, maka kita harus mulai dari awal lagi dengan huruf pertama dari kunci.[8].

Persamaan matematika dari enkripsi pada algoritma *Vigenere cipher* ini adalah seperti berikut :

$$Ciq = Ek(Mi) = (Mi + Ki) \bmod 26 \quad (1)$$

Persamaan matematika untuk dekripsi adalah :

$$Mi = Dk(Ci) = (Ci - Ki) \bmod 26 \quad (2)$$

Keterangan :
C : cipherteks, M : Plainteks, K : Kunci.

Cipher Block Chaining (CBC)

***Cipher Block Chaining* (CBC)**

CBC merupakan algoritma kriptografi modern, CBC menggunakan larik khusus yang disebut IV seukuran dengan ukuran blok (n bit). CBC direkomendasikan digunakan dengan sistem sandi yang memiliki ukuran blok lebih dari 64 bit. Pada proses CBC akan dilakukan pembagian tiap block plaintext maupun ciphertext. Operasi dapat dilakukan untuk mewujudkan layanan otentikasi. Sebelumnya CBC memiliki ketentuan dimana CBC memiliki C_0 dan nilai C_0 dapat kita tentukan sendiri. C_0 berfungsi sebagai nilai awal pada blok yang pertama di dalam proses XOR enkripsi dan dekripsi nantinya.

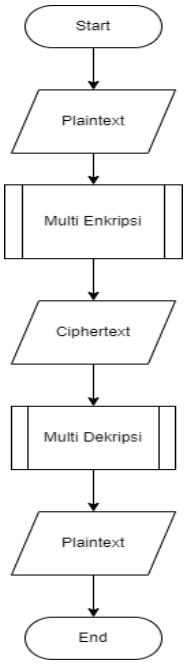
Avalanche Effect

Avalanche Effect adalah teknik untuk mengukur keefektifan algoritma kriptografi pengenkripsian data. Asusmsi suatu algoritma lebih baik jika memiliki nilai perhitungan yang tinggi[9]. Pengujian Avalanche Effect dianggap baik apabila terjadi perubahan bit yang menunjukkan antara 45-60% adalah hasil yang dianggap baik dalam pengujian.

METODE

Gambaran Umum

Pada alur sistem dibawah ini merupakan alur sistem enkripsi dan dekripsi Vigenere Cipher dan CBC:



Gambar 1. Gambaran Umum Sistem

Pada alur sistem yang dibuat menggunakan metode Vigenere Cipher dan CBC, Pada tahap awal akan masuk pada menu untuk menginputkan data, setelah itu sistem akan melakukan proses enkripsi menggunakan kombinasi algoritma *vigenere* dan CBC. Setelah data terenkripsi, data tersebut dapat dikembalikan ke bentuk aslinya dengan melakukan pendekripsian data melalui proses dekripsi kombinasi *vigenere* dan CBC.

HASIL DAN PEMBAHASAN

Pengujian *Avalanche Effect*

Dari hasil enkripsi data pegawai akan dilakukan pengujian yaitu avalanche effect yang akan dilakukan 3 tahap pengujian yaitu dengan melakukan pengujian pada metode vigenere tunggal, CBC tunggal dan metode gabungan vigenere cipher dan CBC dan akan dilakukan perbandingan keamanan dari 3 pengujian tersebut, seperti berikut :

Tabel 1. Pengujian Avalanche Vigenere Cipher

No	Ciphertext	Avalanche Effect
1	19730507 200906 1 001 VUBQR FOXKOZSUVC Bohmzccjcz/Komqc	16.29%
2	19731206 199803 2 005 DORCY ZUTLOQUTQ,G.Kiy,UA Vyqmhsaavu/Komqc	16.60%
3	19731120 201001 1 002 TUSJOFA YCXSXO Curqdshm/Aiycu	14.95%
4	19710404 201212 1 002 KOVIFVC Lusjoclooovoto/Haeavu	14.46%
5	19710514 200906 1 005 EOTROJ QGVHG Komqc/Komqc	12.50%
	Rata-rata Avalanche Effect	14.14%

Pada tabel 1 hanya diambil contoh 5 data dari data ke 26 - 30. Berdasarkan pengujian pada tabel 1, *Vigenere Cipher* mendapatkan hasil *avalanche effect* sebesar 14,14%.

Tabel 2. Pengujian Avalanche CBC

No	Ciphertext	Avalanche Effect
1	5a 4e 7a 1a dc 5b 5e 5a 7c 14 c0 69 28 b8 95 e3 2d 92 cd 73 c b0 6b f2 ff ff 37 7a d6 81 d 10 38 4a 82 11 34 ac 3b 3a 36 3c 26 16 6c ba 25 9c 17 4c de e7 99	67.19%
2	5a 4e 7a 1a de 51 4a 70 28 ba 8f e5 33 8e f3 2f b2 ad b3 8f fd a0 63 d6 8f 1 ca 8d 11 36 6c d2 9f 35 7e e6 1d 14 fc d7 f9 9d eb c5 99 b0 23 18 72 84 43 c0 e3 93 61 14 6 6e 9a 6f 88	68.33%
3	5a 4e 7a 1a de 57 42 6c 10 cc 71 8 f8 19 d8 79 18 f8 19 da 59 bc 73 f4 e5 c1 97 29 9a 1b 14 34 62 c4 93 ae 17 7e a6 25 0 54 ee b 38 12 62 9e 6b	66.71%
4	5a 4e 7a 1e d4 49 7a 14 e0 2d b2 8f f3 d f6 25 a0 89 fb 1f d2 9e 1f 16 26 60 c0 9b 90 6b 84 45 c0 df d3 fd bd 31 22 26 18 76 3a 54 f2 bb 15 7e ba	66.11%
5	5a 4e 7a 1e d4 4b 7c 18 f8 1d d2 4d 60 28 b4 a1 a9 9b df 57 4c a2 67 da a9 59 9e f5 cd 91 37 4e 8a 9e 5f f8 ab 1 d4 87 6d 9c 63 90	67.24%
	Rata-rata Avalanche Effect	64.53%

Pada tabel 2 hanya diabil contoh 5 data dari data ke 26 - 30. Berdasarkan pengujian pada tabel 2, metode gabungan *Vigenere Cipher* dan CBC mendapatkan hasil *avalanche effect* sebesar 64,53%.

Tabel 3. Pengujian Avalanche Vigenere Cipher dan CBC

No	Ciphertext	Avalanche Effect
1	5a 4e 7a 1a dc 5b 5e 5a 7c 14 c0 69 28 b8 95 e3 2d 92 cd 73 c 94 b 1a 1e 10 e8 d5 bd 43 98 27 72 ca b7 4b 98 bc 2f 6 5e c0 cf d1 ff b1 1f e8 cf c9 c1 e9 9d	67.48%
2	5a 4e 7a 1a de 51 4a 70 28 ba 8f e5 33 8e f3 2f b2 ad b3 8f fd b0 77 c2 8b 2d 92 19 10 0 10 36 46 ae 7d d0 71 e4 1d 24 12 5e 6c fa ff 94 53 cc cb cf f1 a9 19 56 ce 4b 88 47 dc d3 e9	68.90%
3	5a 4e 7a 1a de 57 42 6c 10 cc 71 8 f8 19 d8 79 18 f8 19 da 59 90 3 28 4c 8e 19 38 b8 4b 98 9 3c 40 96 be 1f 52 ce dd d5 f3 b5 bd 71 b8 b 58 d2	67.82%
4	5a 4e 7a 1e d4 49 7a 14 e0 2d b2 8f f3 d f6 25 a0 89 fb 1f d2 ae 4b b2 7f fa d1 ad a0 23 28 c 4e d2 f5 bd 2d c 7c ae 3d 2c 8e 5 40 c2 cf fb 95	64.23%
5	5a 4e 7a 1e d4 4b 7c 18 f8 1d d2 4d 60 28 b4 a1 a9 9b df 57 4c b2 73 c6 a1 55 b6 a5 61 c4 ad 43 80 ae b 44 e2 8b c1 9d 6d 88 7b b8	67.53%
	Rata -rata Avalanche Effect	66,31%

Pada tabel 3 hanya diabil contoh 5 data dari data ke 26 - 30. Berdasarkan pengujian pada tabel 3, metode gabungan *Vigenere Cipher* dan CBC mendapatkan hasil *avalanche effect* sebesar 66,31%.

KESIMPULAN

Dari hasil analisis dan penellitian yang telah diuraikan pada bab sebelumnya tentang Implementasi Multi Enkripsi Algoritma *Vigenere Cipher* dan *Cipher Block Chaining* (CBC) Ulntuk Keamanan Data Pegawai, maka kesimpulan yang didapatkan sebagai berikut :

1. Berdasarkan penelitian ini, didapatkan hasil rata-rata *Avalanche Effect* untuk metode Vigenere Cipher tunggal sebesar 14,14%, metode CBC tunggal sebesar 64,53% sedangkan untuk metode gabungan *Vigenere Cipher* dan CBC mendapatkan hasil rata-rata sebesar 66,31% yang berarti metode gabungan dua algoritma *Viglnere Cipher* dan CBC lebih efektif dalam pengamanan data karena memiliki hasil paling besar dibandingkan dengan metode tunggal *Vigenere Cipher* dan metode tunggal CBC.
2. Dengan metode gabungan dua algoritma dapat meningkatkan keamanan data, dengan gabungan dua algoritma juga dapat mengatasi kekurangan algoritma yang pertama seperti pada penelitian ini dimana algoritma *Vigenere Cipher* disini hanya dapat mengenkripsi karakter huruf sedangkan data memiliki banyak karakter seperti nomor dan simbol. Maka algoritma CBC disini dapat mengenkripsi karakter yang tidak dapat di enkripsi *Vigenere Cipher* sehingga hasil enkripsi memiliki keamanan lebih tinggi.
3. Penggunaan kunci pada penelitian ini juga menggunakan kunci dari masing-masing algoritma yaitul kunci *Vigenere Cipher* dan kunci CBC, selain itu dibutuhkan inputan IV (*Inisialitation Vector*) untuk menjalankan algoritma CBC sehingga dari implementasi kedua algoritma ini lebih rumit untuk di pecahkan oleh kriptoanalis.

DAFTAR PUSTAKA

[1] Imelda Asih Rohani Simbolon, Indra Gunawan, Ika Okta Kirana, Rafiqa Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst. Inform. JoSYC*, vol. 1 No 2, pp. 54–60, Feb. 2020.

[2] Sheila Maulida Intan and Fadilah Salsabila, "Implementasi Kriptografi AES pada File Word," *ResearchGate*, Dec. 2019.

[3] Dewi Purnamasari and Nindita Erwanti, "ENKRIPSI CITRA FOVEA AVASCULAR ZONE (FAZ) MENGGUNAKAN KRIPTOGRAFI VIGENERE CIPHER," *J. Pseudocode*, vol. 9 Nomor 2, pp. 114–121, Sep. 2022, doi: https://doi.org/10.33369/pseudocode.9.2.114-121.

[4] Devi Andriani, "Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining," *J. Tek. Inform. Unika St Thomas JTIUST*, vol. 2 No.2, pp. 14–23, Desember 2017.

[5] Danang H. Sulaksono, , Citra N. Prabiantissa, Gusti E. Yuliastuti, and Ainur R. Taqwa, "Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android," *Semin. Nas. Sains Dan Teknol. Terap.*, vol. 9, no. 1, pp. 570–576, Oct. 2021.

[6] Angga Aditya Permana and Desi Nurnaningsih, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," *J. Tek. Inform.*, vol. 11 NO. 2, pp. 177–186, Oktober 2018, doi: http://dx.doi.org/10.15408/jti.v11i2.7811.

[7] Muhammad Dedi Irawan, "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP," *J. Teknol. Inf.*, vol. 1 No 1, pp. 11–21, Jul. 2017, doi: https://doi.org/10.36294/jurti.v1i1.21.

[8] Angga Aditya Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *J. AL-AZHAR Indones. SERI SAINS DAN Teknol.*, vol. 4 No 3, pp. 110–115, Mar. 2018, doi: http://dx.doi.org/10.36722/sst.v4i3.280.

[9] Ainur Rilo Taqwa and Danang Haryo Sulaksono, "IMPLEMENTASI KRIPTOGRAFI DENGAN METODE ELLIPTIC CURVE CRYPTOGRAPHY (ECC) UNTUK APLIKASI CHATTING BERBASIS ANDROID," *J. Ris. Inov. Bid. Inform. Dan Pendidik. Inform. KERNEL*, vol. 1 No 1, pp. 42–48, Jun. 2020, doi: https://doi.org/10.31284/j.kernel.2020.v1i1.929.