# IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER PADA MEDIA TEKS DENGAN KOMBINASI TRANSPOSISI KOLOM

**Daurat Sinaga[1], Chaerul Umam[2]**
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]dauratsinaga@dsn.dinus.ac.id,[2]chaerul@dsn.dinus.ac.id

**ABSTRAK**

Popularitas implementasi kriptografi pada media teks masih terus ada sampai saat ini, hal ini dibuktikan dengan berbagai penelitian mengenai penyelesaian kasus tertentu khususnya pada berbagai media teks. Salah satu media yang digunakan adalah media teks dan pada penelitian ini, digunakan media teks sebagai implementasi kriptografi menggunakan algoritma vigenere cipher dengan kombinasi algoritma transposisi kolom. Dalam penelitian ini membuktikan bahwa pesan asli (plaintext) dapat di proses enkripsi dengan baik menggunakan kombinasi algoritma tersebut serta dapat dikembalikan seperti semua (didekripsi secara sempurna. Selain itu, penelitian ini juga membuktikan apabila salah satu karakter dari text tersebut diubah, maka akan mengubah semua karakter pada pesan yang terenkripsi (cipherteks). Untuk menentukan tingkat keamanan data pesan dengan menggunakan avalanche effect dengan 5 (lima) buah percobaan mendapatkan nilai tertinggi 45,416. Salah satu komponen dalam avalanche effect adalah bit flipping atau dapat disebut juga perubahan bit dalam suatu proses enkripsi. Dalam bit flipping ini digunakan untuk menentukan perubahan bit sebelum dan sesudah proses enkripsi berjalan sehingga mempengaruhi dapat meningkatkan proses keamanan dalam proses kriptografi tersebut.

**Kata Kunci**:kriptografi, plaintext, vigenere cipher, transposisi kolom, avalanche effect, bit flipping.

## 1. PENDAHULUAN

Cipher adalah sesuatu yang digunakan untuk mengubah data aktual ke dalam format yang tidak dapat dikenali oleh siapa pun kecuali pengirim dan penerima. Salah satu pertimbangan penting untuk mengukur kekuatan setiap algoritma kriptografi adalah *avalanche effect*-nya[5]. Algoritma yang baik memiliki Efek *avalanche* yang tinggi. Teknik enkripsi modern baik menggunakan kunci simetrik tunggal atau dua kunci. Algoritma ini disebut sebagai *symmetric key cryptography* jika hanya satu kunci yang digunakan dan disebut sebagai kriptografi kunci publik jika dua kunci digunakan.

Beberapa contoh kunci kriptografi *Symmetric*[4] yang terkenal adalah *Data Encryption Standard* (DES)[6], *Advanced Encryption Standard* (AES), Blowfish, dll. Algoritma ini menggunakan kunci tunggal untuk mengenkripsi data. Kriptografi kunci publik, di sisi lain menggunakan dua kunci dan karenanya lebih aman dan memberikan tanda tangan digital juga. *Algoritma public key* yang paling umum digunakan adalah algoritma *Rivest-Shamir-Adleman* (RSA)[9]. Kerugian utama dari kriptografi kunci Publik [10] adalah bahwa hal itu memerlukan komunikasi yang berlebihan dan sumber daya pemrosesan.

Dalam tulisan ini, kami telah mengambil keuntungan dari kriptografi klasik pada model operasi substitusi dan permutasi. Seperti penelitian yang telah dilakukan oleh Hannan [2] yang telah mengevaluasi kombinasi *polyalfabeth* dan transposisi cipher pada media teks pendek sejumlah 12 karakter saja sehingga perlu perluasan plainteks dengan tujuan keamanan data. Pada penelitian tersebut belum digunakan metode evaluasi yang terstandar maka pada makalah ini akan digunakan *avalanche effect* untuk melihat jumlah bit yang berubah pada pesan dengan karakter panjang. Untuk memahami konsep *Avalanche Effect*[7] dan tujuan perbandingan, dalam makalah ini telah diambil beberapa algoritma seperti Vigenere Cipher, Caesar Cipher, *Data Encryption Standard* (DES) dan Blowfish.

Pada bagian berikutnya, akan di bahas tentang algoritma yang disebutkan di atas termasuk algoritma yang diusulkan. Selanjutnya pada bagian pembahsan, akan dilakukan pembandingan hasil dari efek *avalanche* dari semua metode.

## 2. METODE PENELITIAN

### 2.1 Vigenere Cipher

Vigenere cipher adalah salah satu jenis kriptografi simteris dan dikategorikan pula sebagai *polyalfabet* cipher. Vigenere cipher mulai diperkenalkan pada tahun 1586 oleh Blaise de Vigenere. Sandi vigenere atau vigenere cipher mempunyai karakteristik yang mudah digunakan dan cocok untuk plainteks yang panjang [1]. Penggunaan plainteks yang panjang dinilai lebih aman karena kunci akan berputar sebanyak plainteks. Vigenere cipher menggunakan pola pergeseran. Pada bentuk aslinya, dapat digunakan tabel *tabula recta* atau dapat pula menggunakan perhitungan XOR sesuai pada persamaan (1) untuk proses enkripsi dan persamaan (2) untuk proses dekripsi.

$$C = (P + K)\ mod\ 26 \quad (1)$$

$$P = (C - K) mod\ 26 \quad (2)$$

Pada persamaan (1) dan persamaan (2) diketahui bahwa P adalah plainteks, C adalah cipherteks, K adalah kunci. Kunci enkripsi dan dekripsi harus sama, sehingga vigenere cipher disebut sebagai kriptografi kunci simetris.

2.2 Transposisi Kolom

Transposisi kolom merupakan salah satu jenis transposisi cipher. Adapun bentuk lain dari transposisi cipher yaitu *route*, ganda, *myzkowsky*, dan *rail fence*. Transposisi kolom fleksibel [8] dan dapat digabung dengan jenis kriptografi simetris lain misalnya playfair cipher, hill cipher, Caesar cipher, shift cipher, *beaufort* cipher, *autokey* cipher dan vigenere cipher serta berbagai macam cipher polialfabet lain. Transposisi kolom dapat digunakan dengan aman apabila kunci yang digunakan cukup panjang[3]. Dalam makalah ini telah digunakan kunci dengan panjang beragam untuk mengetahui performa dari kombinasi algoritma yang telah diteliti, seperti terlihat pada *pseudocode* di bawah ini.

```
idx=1;
for k=1:kolom
    for b=1:baris
        epesan(idx)=pesan2d(b,idxk(k));
        idx=idx+1;
    end
end
```

## 3. HASIL DAN PEMBAHASAN

Dalam makalah ini teks panjang yang digunakan akan diubah satu karakter untuk melihat hasil perubahan karakter yang di enkripsi dengan kombinasi vigenere cipher dan transposisi kolom. Akan terlihat perubahan bit dari plainteks asli dan plainteks dengan perubahan satu buah karakter di bagian akhir. Hasil eksperimen dievaluasi dengan *avelanche effect. Avalanche* effect yaitu salah satu model perhitungan untuk melihat perubahan bit yang terjadi pada sebuah media [5][11] melalui persamaan (3).

$$Avalanche\ Effect = \left(\frac{jumlah\ bit\ flip}{total\ bit}\right) x\ 100\% = \quad (3)$$

Dari persamaan (3), jumlah bit flip merupakan jumlah bit yang berubah selama proses enkripsi berlangsung. Hasil perhitungan *avalanche effect* dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan hasil perubahan bit

| No. | Pesan | cipher | Bit berubah | Avalenche effect |
|---|---|---|---|---|
| 1 | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**O** | Ss9ECy r > i\ 'P SE9-Zpw Z1N, 6!= t k$. 4 = d^ D Y@+ | 217 | 45.20833333 3333336 |
| | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**E** | " w2X&6y 9]:9 Wl ^; " -yH>m !Z n1b<`aFD e4Jw8us aj hShl | | |
| 2 | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**O** | [CJ7;0WQl6 GZua^ 2?ly vPk_dG Z4O n=MY= _^9G 1sl7C%V!# | 203 | 42.29167 |
| | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**E** | 6=XG$MocFJhN>6^S<5'$;K(.# ?$Xc][;qO 4jw!x#U/Go` | | |
| 3 | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**O** | U!N\ M6 )a* @)6 U1Y0gP8;Lx#wm CTc_rb\t>H&-t Et' u cUCd | 211 | 43.95833 |
| | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**E** | m)j+Wzl0YK7 r^ 8 &N6 p?> rbyzs;ja_< klTeFKw[`\$a ;Oql | | |
| 4 | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**O** | 2 Tte` ? K Ol$C )(q;$@o+%Q Y>Ty 5l/ZOZ0Za X,_ w#ed+ % | 209 | 43.54167 |
| | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**E** | R :*in _<) [ \hc gqC t/D,z 7=D*w Uyp4ay^i -( QIQ *x< mQ | | |
| 5 | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**O** | x[ sW"kV% 0 OH p8;T? (w61 D.Mi. =(^ I Dhak !7&Q L\Rs d VV | 218 | 45.41667 |

| | | | | |
|---|---|---|---|---|
| | UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OK**E** | "! Kk j/ )' % 2nk b=tlVF$ x 4 P`W-Sv M0%18lX;0L # | | |

Berdasarkan Tabel 1 pada nomor pesan ke satu yaitu UNIVERSITAS DIAN NUSWANTORO SEMARANG MEMANG JEMPOL DAN OKO dan cipher yaitu Ss9ECy r > i\ 'P SE9-Zpw Z1N, 6!= t k$. 4 = d^ D Y@+ telah terjadi perubahan bit sebanyak 217 buah seperti terlihat pada Gambar 1.

| | | |
|---|---|---|
| 00101101 | 01110011 | 00110011 |
| 00001101 | 00111000 | 01010001 |
| 01110011 | 00110111 | 01011111 |
| 01100101 | 00001101 | 00111111 |
| 00011111 | 00110110 | 00100000 |
| 01100001 | 01110111 | 01100001 |
| 01010010 | 00110001 | 01011001 |
| 00000001 | 00000101 | 00000100 |
| 01101010 | 00110110 | 00100001 |
| 00001010 | 00001011 | 00010100 |
| 00101110 | 01110111 | 00111011 |
| 00000100 | 01101110 | 01101000 |
| 00100011 | 00100110 | 00010100 |
| 00001010 | 01010000 | 01001100 |
| 00100111 | 01110111 | 00101110 |
| 00101000 | 00101001 | 01010010 |
| 01010110 | 00000000 | 00100101 |
| 01001001 | 00110101 | 00000110 |
| 01110111 | 00000011 | 01011011 |
| 01010100 | 01011111 | 00010000 |

Gambar 1. Perubahan bit dari proses enkripsi pesan

Berdasarkan percobaan yang telah dilakukan nilai *avalanche* yang diperoleh cukup tinggi dan terjadi perubahan bit yang besar meskipun yang dirubah hanya satu buah karakter saja. Hal ini menandakan bahwa kombinasi vigenere cipher dan transposisi kolom yang digunakan sangat aman. Adanya perubahan bit yang besar dari satu buah karakter yang diganti menyimpulkan bahwa apabila teks di kamuflase oleh pihak lain maka akan menyebabkan teks berubah dan orang lain akan mengetahui telah terjadi perubahan teks.

## 5. KESIMPULAN

Teks sering kali di *copy paste* oleh pihak yang tidak berwenang sehingga perlu pengamanan. Dalam makalah ini vigenere cipher dan transposisi kolom telah dilakukan dengan tujuan mengamankan media, dalam makalah ini berupa teks. Perubahan karakter yang signifikan ditandai dengan nilai *avalanche e*ffect yang dihasilkan. Pada penelitian ini nilai *avalanche effect* tertinggi yaitu 45.41667 dan total bit yang berubah sebanyak 218 bit. Adapun perubahan bit pada *avalanche effect* terbesar seperti diilustrasikan pada Gambar 1. Untuk pengembangan selanjutnya, kombinasi yang sudah aman ini dapat diterapkan pada media gambar digital maupun video.

## DAFTAR PUSTAKA


[1] Ardy, R. D., Indriani, O. R., Sari, C. A., Ignatius, D. R., & Setiadi, M. (2017). Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5). In *International Conference on Smart Cities, Automation & Intelligent Computing Systems* (pp. 1–6).

[2] Hannan, S. A., Mir, A., & Mir, A. (2017). Analysis of Polyalphabetic Transposition Cipher Techniques used for Encryption and Decryption, *6*(2), 41–46.

[3] Heydari, M., Shabgahi, G. L., & Heydari, M. M. (2013). Cryptanalysis of transposition ciphers with long key lengths using an improved genetic algorithm. *World Applied Sciences Journal*, *21*(8), 1194–1199. https://doi.org/10.5829/idosi.wasj.2013.21.8.22

[4] Joseph, D. P., & Krishna, M. (2015). Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Research in Computer Science*, *6*(3), 51–56.

[5] Kumar, A., & Tiwari, N. (2012). Effective Implementation and Avalanche Effect of AES. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, *1*(3), 31–35. https://doi.org/10.5121/ijsptm.2012.1303

[6] Kusuma, E. J., Indriani, O. R., Sari, C. A., Setiadi, D. R. I. M., & Rachmawanto, E. H. (2017). An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption. In *International Conference on Innovative and Creative Information Technology (ICITech)* (pp. 1–5).

[7] Patidar, G., Agrawal, N., & Tarmakar, S. (2013). A block based Encryption Model to improve Avalanche Effect for data Security. *International Journal of Scientific and Research Publications*, *3*(1), 1–4.

[8] Pramanik, M. B. (2014). Implementation of Cryptography Technique using Columnar Transposition, 19–23.

[9] Setiadi, D. R. I. M., Handoyo, A. E., Rachmawanto, E. H., Sari, C. A., & Susanto, A. (2018). Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *Jurnal Teknologi Dan Sistem Komputer*, *6*(1), 37. https://doi.org/10.14710/jtsiskom.6.1.2018.37-43

[10] Singh, S., Iqbal, M. S., & Jaiswal, A. (2015). Survey on Techniques Developed using Digital Signature : Public key Cryptography. *International Journal of Computer Applications*, *117*(16), 1–4.

[11] Witoolkollachit, P. (2016). The avalanche effect of various hash functions between encrypted raw images versus non-encrypted images : A comparison study. *Journal of the Thai Medical Informatics Association*, *1*, 69–82.