


ANALISIS KOMBINASI METODE CAESAR CIPHER, VERNAM CIPHER, DAN HILL CIPHER DALAM PROSES KRIPTOGRAFI

Muhammad Rhifky Wayahdi

Related papers

[Download a PDF Pack](#) of the best related papers 



[Penerapan Metode Dynamic Cell Spreading \(DCS\) Untuk Menyembunyikan Teks Tersandi Pad...](#)
Taronisokhi Zebua

[Algoritma Kriptografi & Contohnya](#)

Mahardika Yuzlizar Fachruddin

[UNIVERSITAS INDONESIA APLIKASI ALGORITMA RIVEST CODE 6 DALAM PENGAMANAN CITRA DIGITAL...](#)

Anastasya Pattipawae

ANALISIS KOMBINASI METODE CAESAR CIPHER, VERNAM CIPHER, DAN HILL CIPHER DALAM PROSES KRIPTOGRAFI

Khairani Puspita¹⁾, M. Rhifky Wayahdi²⁾

¹⁾ Dosen Sistem Informasi Universitas Potensi Utama

²⁾ Mahasiswa Sistem Informasi Universitas Potensi Utama

^{1),2)} Jl. K.L. Yos Sudarso Km 6,5 No. 3A Tanjung Mulia-Medan

Email: khairan.adwa@gmail.com¹⁾, rhifky.wayahdi@yahoo.com²⁾

Abstrak

Kriptografi berasal dari kata “Crypto” yang berarti rahasia dan “graphy” yang berarti tulisan. Jadi, kriptografi adalah tulisan yang tersembunyi. Banyak metode yang dapat digunakan dalam proses kriptografi seperti Caesar Cipher, Vernam Cipher, Hill Cipher, dan lain sebagainya. Pada penelitian ini penulis akan mengkombinasikan metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dalam proses kriptografi (enkripsi dan dekripsi).

Dari hasil penelitian yang penulis lakukan, penulis dapat menyimpulkan bahwa metode Caesar Cipher, Vernam Cipher, dan Hill Cipher adalah jenis kriptografi klasik yang cukup kuat jika dilihat dari segi keamanannya dengan sedikit modifikasi. Ketiga metode ini dapat dikombinasikan menjadi satu dalam proses kriptografi (enkripsi dan dekripsi) dengan tingkat keamanan yang sangat baik dan sulit untuk dipecahkan.

Kombinasi metode Caesar Cipher, Vernam Cipher, dan Hill Cipher ini hanya membutuhkan sebuah kunci (key) dalam proses enkripsi maupun dekripsi yang akan memudahkan kita untuk mengingatnya.

Kata kunci: Kriptografi, Caesar Cipher, Vernam Cipher, Hill Cipher.

1. Pendahuluan

Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuno. Kriptografi sendiri berasal dari kata “Crypto” yang berarti rahasia dan “graphy” yang berarti tulisan. Jadi, dapat dikatakan kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang yang tidak mengetahui bagaimana tulisan tersebut disembunyikan tidak akan mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut [1].

Ada beberapa algoritma atau metode yang dapat digunakan dalam proses kriptografi seperti metode Caesar Cipher, Vernam Cipher, Hill Cipher, dan lain sebagainya. Dalam kriptografi, Caesar Cipher juga dikenal sebagai pergeseran cipher yang merupakan salah satu teknik enkripsi yang paling sederhana dan dasar dikenal. Metode ini adalah jenis menggantikan angka di

mana setiap huruf dalam *plaintext* diganti dengan huruf dengan posisi tetap dipisahkan oleh nilai numerik yang digunakan sebagai “kunci” [2].

Metode Vernam Cipher telah memainkan peran penting dalam kriptografi karena merupakan sistem kerahasiaan yang sempurna. Metode ini memungksikan boolean eksklusif (Ex-OR dan Ex-Nor) [3] “vernham cipher”. Sedangkan metode Hill Cipher adalah cipher simetris klasik berdasarkan transformasi matriks. Metode ini memiliki beberapa keuntungan termasuk ketahanan terhadap analisis frekuensi dan implicity karena metode ini menggunakan perkalian matriks dan inversi untuk enkripsi dan dekripsi [4].

Dey, Somdip (2013) dalam penelitiannya memodifikasi metode Caesar Cipher dengan memperkenalkan fungsi polinom acak dan modular pengurangan yang membuat metode ini semakin kuat terhadap differential pembacaan sandi [2].

Ryabko, Boris (2013) dalam penelitiannya mengatakan bahwa metode Vernam Cipher (*or one-time pad*) telah memainkan peran penting dalam kriptografi karena merupakan sistem kerahasiaan yang sempurna [3].

Farmandar, Mina and Alexander G. Chefranov (2012) dalam penelitiannya mengungkapkan bahwa metode Hill Cipher dalam pembacaan sandi relatif mudah atau rentan terhadap serangan pengenalan *plaintext-ciphertext* karena linearitas [5].

Dari penelitian yang dilakukan oleh Dey, Somdip (2013), Ryabko, Boris (2013), dan Farmandar, Mina and Alexander G. Chefranov (2012) menunjukkan bahwa metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dapat diterapkan dalam penyandian dan dapat dimodifikasi untuk meningkatkan keamanannya. Setiap metode memiliki kelebihan dan kekurangan masing-masing. Hal ini yang mendasari penulis untuk menganalisa lebih dalam mengenai metode Caesar Cipher, Vernam Cipher, dan Hill Cipher.

Tujuan penelitian ini dilakukan adalah untuk menganalisis metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dalam proses kriptografi. Penulis ingin mengkombinasikan ketiga metode tersebut dalam proses enkripsi dan dekripsi untuk meningkatkan keamanan data atau pesan.

2. Metode Caesar Cipher

Metode *Caesar Cipher* berasal Julius Caesar, yang merupakan kaisar Roma, ia menggunakan cipher substitusi untuk mengirim pesan ke panglima perangnya. *Caesar Cipher* dikenal dengan beberapa nama seperti: *Shift Cipher*, *Caesar's Code*, atau *Caesar Cipher Shift* [1].

Metode *Caesar Cipher* mungkin adalah metodologi enkripsi pertama. Metode enkripsi ini berjenis cipher substitusi, di mana setiap huruf pada *plaintext*-nya digantikan dengan huruf lain. Misalnya dengan pergeseran 3 langkah, A akan digantikan oleh D, B akan menjadi E, dan seterusnya [2].

Proses enkripsi dalam metode ini adalah sebagai berikut:

Misalkan:

Plaintext = AYO

Key = 3

Kemudian ubah *plaintext* dan *key* menjadi data biner.

AYO = 01000001 01011001 01001111

3 = 00110011

Kemudian lakukan proses enkripsi dengan melakukan pergeseran pada bilangan biner tersebut sebanyak 3 langkah (sesuai *key*) ke arah kanan, kemudian ubah bilangan biner tersebut menjadi karakter.

Biner = 01000001 01011001 01001111

Hasil = 00101000 00101011 11101001

Karakter = (+ é

Jadi, *ciphertext* dari kata AYO adalah (+é.

Sedangkan untuk proses dekripsi sama dengan pada proses enkripsi yaitu dengan melakukan proses pergeseran pada bilangan biner dari suatu karakter tertentu sebanyak 3 langkah (sesuai *key*) ke arah kiri, dan ubah menjadi karakter kembali untuk mengetahui kata apa yang disembunyi.

Ciphertext = (+ é

Biner = 00101000 00101011 11101001

Hasil = 01000001 01011001 01001111

Plaintext = A Y O

Jadi, *plaintext* dari kata (+é adalah AYO.

3. Metode Vernam Cipher

Metode *Vernam Cipher* merupakan sistem kerahasiaan yang sempurna di mana metode ini adalah stream cipher simetris di mana *plaintext* dikombinasikan dengan *key stream* (*pseudorandom*) yang sama panjang untuk menghasilkan *ciphertext* yang memungsi boolean eksklusif (Ex-OR dan Ex-Nor) [3].

Proses enkripsi dalam metode ini adalah sebagai berikut:

Misalkan:

Plaintext = TES

Key = 3

Kemudian ubah *plaintext* dan *key* menjadi data biner.

TES = 01010100 01000101 01010011

3 = 00110011

Kemudian lakukan proses enkripsi dengan menggunakan logika Ex-OR.

01010100	01000101	01010011
00110011 ⊕	00110011 ⊕	00110011 ⊕
01100111	01110110	01100000

Setelah didapatkan hasil dari proses enkripsi dengan logika Ex-OR, maka nilai-nilai biner tersebut dikonversikan kembali ke dalam bentuk karakter.

Biner = 01100111 01110110 01100000

Karakter = g v `

Jadi, *ciphertext* dari kata TES adalah gv`.

Sedangkan untuk proses dekripsi sama dengan pada proses enkripsi yaitu dengan melakukan proses Ex-OR pada *ciphertext* dan *key*.

01100111	01110110	01100000
00110011 ⊕	00110011 ⊕	00110011 ⊕
01010100	01000101	01010011

Setelah didapatkan hasil dari proses dekripsi dengan logika Ex-OR, maka nilai-nilai biner tersebut dikonversikan kembali ke dalam bentuk karakter.

Biner = 01010100 01000101 01010011

Karakter = T E S

Jadi, *plaintext* dari kata gv` adalah TES.

4. Metode Hill Cipher

Metode *Hill Cipher* adalah cipher simetris klasik yang memecah *plaintext* menjadi blok-blok ukuran *m* dan kemudian mengalikan setiap blok oleh sebuah kunci matriks *m x m* untuk menghasilkan *ciphertext* [4].

Proses enkripsi dalam metode ini adalah sebagai berikut:

Misalkan:

Plaintext = MAJU

Key (k) = $\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$

Kemudian ubah *plaintext* dari kata MAJU menjadi bilangan desimal.

MAJU = 77 65 74 85

Selanjutnya membagi deretan bilangan desimal tersebut menjadi blok matriks yang sesuai dengan jumlah kolom matriks kunci (*key* = 2x2).

MA = $\begin{bmatrix} 77 \\ 65 \end{bmatrix}$ JU = $\begin{bmatrix} 74 \\ 85 \end{bmatrix}$

Melakukan perhitungan pada matriks kunci (*key*) dengan blok matriks *plaintext*.

$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 77 \\ 65 \end{bmatrix} = \begin{bmatrix} (3 * 77) + (2 * 65) \\ (4 * 77) + (5 * 65) \end{bmatrix} = \begin{bmatrix} 361 \\ 633 \end{bmatrix} \text{mod } 255 = \begin{bmatrix} 106 \\ 123 \end{bmatrix}$

$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 74 \\ 85 \end{bmatrix} = \begin{bmatrix} (3 * 74) + (2 * 85) \\ (4 * 74) + (5 * 85) \end{bmatrix} = \begin{bmatrix} 392 \\ 721 \end{bmatrix} \text{mod } 255 = \begin{bmatrix} 137 \\ 211 \end{bmatrix}$

Kemudian ubah bilangan desimal hasil perhitungan matriks di atas menjadi karakter.

Desimal = 106 123 137 211

Karakter = j { % Ó

Jadi, *ciphertext* dari kata MAJU adalah j{ % Ó.

Untuk melakukan proses dekripsi yaitu dengan melakukan perkalian pada invers matriks kunci dengan blok matriks *ciphertext*.

$$k = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \quad \det k = (3 \cdot 5) - (2 \cdot 4) = 7$$

invers modulo:

$$7^{-1} \bmod 255$$

$$7x = 1 \bmod 255$$

$$7x = 1 + 255k$$

$$x = (1 + 255k) / 7$$

Cari k=n sehingga hasil x adalah bilangan bulat.

$$k=0; \quad x = (1 + 255 \cdot 0) / 7 = 1/7 \text{ (bukan bilangan bulat)}$$

$$k=1; \quad x = (1 + 255 \cdot 1) / 7 = 36.6 \text{ (bukan bilangan bulat)}$$

$$k=2; \quad x = (1 + 255 \cdot 2) / 7 = 73 \text{ (bilangan bulat)}$$

Sehingga invers dari $7 \bmod 255$ ekuivalen dengan 73 $\bmod 255$ yaitu **73**.

Invers modulo determinan digunakan untuk mencari invers matriks.

$$k = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ maka } k^{-1} = \text{determinan} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Sehingga,

$$k^{-1} = 73 \begin{bmatrix} 5 & -2 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 365 & -146 \\ -292 & 219 \end{bmatrix} \bmod 255$$

$$= \begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix}$$

Untuk modulo bilangan negatif dapat dikerjakan dengan:

$$\begin{aligned} -n \bmod x &= x - (n \bmod x) \\ &= 255 - (146 \bmod 255) = 109 \\ &= 255 - (292 \bmod 255) = 218 \end{aligned}$$

Setelah matriks k di-invers, selanjutnya mengalikan matriks k dengan *ciphertext*.

$$\begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix} \begin{bmatrix} 106 \\ 123 \end{bmatrix} = \begin{bmatrix} 25067 \\ 50045 \end{bmatrix} \bmod 255 = \begin{bmatrix} 77 \\ 65 \end{bmatrix}$$

$$\begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix} \begin{bmatrix} 137 \\ 211 \end{bmatrix} = \begin{bmatrix} 38069 \\ 76075 \end{bmatrix} \bmod 255 = \begin{bmatrix} 74 \\ 85 \end{bmatrix}$$

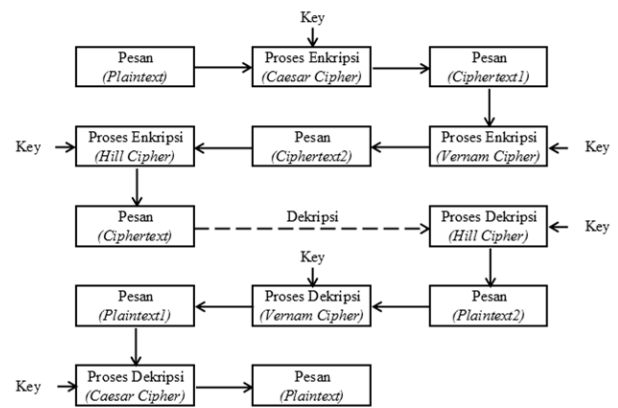
Setelah didapatkan hasil dari proses perhitungan, maka nilai-nilai desimal tersebut dikonversikan kembali ke dalam bentuk karakter.

$$\begin{array}{lclcl} \text{Desimal} & = & 77 & 65 & 74 & 85 \\ \text{Karakter} & = & M & A & J & U \end{array}$$

Jadi, *plaintext* dari kata j{ % Ó adalah MAJU.

5. Metode Penelitian

Tujuan penelitian ini yaitu untuk menganalisis metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* dalam proses kriptografi dan mengkombinasikan ketiga metode tersebut dalam proses enkripsi dan dekripsi untuk meningkatkan keamanan data. Untuk mencapai tujuan tersebut, ada beberapa proses atau tahapan dalam mengkombinasikan metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* dalam mengenkripsi ataupun mendekripsikan teks atau pesan. Gambar 1 menunjukkan proses kriptografi dengan kombinasi metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher*.



Gambar 1. Proses Kriptografi Kombinasi

Pada Gambar 1 dapat dilihat proses kriptografi dengan kombinasi 3 metode yaitu *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher*. Proses pertama pesan asli (*plaintext*) dienkripsi dengan metode *Caesar Cipher* dan menghasilkan pesan sandi (*ciphertext1*), setelah itu dienkripsi kembali dengan metode *Vernam Cipher* dan menghasilkan *ciphertext2*, kemudian dienkripsi kembali dengan metode *Hill Cipher* dan menghasilkan *ciphertext* akhir.

Sedangkan untuk proses dekripsi adalah kebalikan daripada proses enkripsi yaitu *ciphertext* pertama kali didekripsi dengan metode *Hill Cipher*, kemudian hasilnya didekripsi kembali dengan metode *Vernam Cipher*, dan terakhir dengan metode *Caesar Cipher* yang akan mengembalikan pesan asli (*plaintext*) yang telah dienkripsi.

6. Hasil dan Analisa

Proses kriptografi dengan kombinasi metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* dilakukan dengan membuat pesan yang akan dienkripsi dan membuat sebuah kunci (*key*) sebagai proses penyandian. Pertama pesan akan dienkripsi dengan menggunakan metode *Caesar Cipher*, kemudian selanjutnya akan dienkripsi kembali dengan metode *Vernam Cipher*, dan yang terakhir dengan metode *Hill Cipher* dengan sekali proses dan sebuah kunci (*key*).

Contoh pesan yang akan dienkripsi adalah kata "VISUAL" dengan kunci (*key*) = 5. Tahap pertama yaitu mengenkripsi pesan dengan menggunakan metode *Caesar Cipher*. Adapun prosesnya adalah sebagai berikut:

$$\text{Plaintext} = \text{VISUAL}$$

$$\text{Key} = 5$$

Kemudian ubah *plaintext* dan *key* menjadi data biner, dapat dilihat pada Tabel 1.

Tabel 1. Konversi Plaintext ke Bilangan Biner

Plaintext	Biner
V	01010110
I	01001001
S	01010011

U	01010101
A	01000001
L	01001100

Kemudian lakukan proses enkripsi dengan melakukan pergeseran pada bilangan biner tersebut sebanyak 5 langkah (sesuai *key*) ke arah kanan, dapat dilihat pada Tabel 2.

Tabel 2. Proses Enkripsi Caesar Cipher

Biner	Ciphertext1
01010110	10110010
01001001	01001010
01010011	10011010
01010101	10101010
01000001	00001010
01001100	01100010

Pada Tabel 2 didapatkan hasil enkripsi dengan metode *Caesar Cipher* yang masih dalam bentuk bilangan biner dengan kunci = 5. Selanjutnya dilakukan proses enkripsi kembali dengan menggunakan metode *Vernam Cipher* masih dengan kunci yang sama yaitu 5. Sebelumnya kunci diubah menjadi bilangan biner terlebih dahulu, 5 = 00110101.

Selanjutnya dilakukan proses enkripsi metode *Vernam Cipher* dengan fungsi logika Ex-OR.

10110010	01001010	10011010
00110101	⊕	00110101
<u>10000111</u>	<u>01111111</u>	<u>10101111</u>
10101010	00001010	01100010
00110101	⊕	00110101
<u>10011111</u>	<u>00111111</u>	<u>01010111</u>

Setelah didapatkan hasil enkripsi dengan fungsi logika Ex-OR, selanjutnya bilangan biner tersebut diubah menjadi bilangan desimal untuk memudahkan proses enkripsi yang selanjutnya, dapat dilihat pada Tabel 3.

Tabel 3. Proses Konversi Bilangan Biner ke Desimal

Hasil	Ciphertext2
10000111	135
01111111	127
10101111	175
10011111	159
00111111	63
01010111	87

Pada Tabel 3 dapat dilihat hasil *ciphertext* dengan metode *Vernam Cipher*, di mana *ciphertext* berupa bilangan desimal yang akan diproses enkripsi kembali dengan metode *Hill Cipher*. Dalam metode *Hill Cipher*, *key* yang digunakan adalah berbentuk matriks di mana matriks yang digunakan adalah 2x2 dengan menggunakan kunci (*key*) yang sama pada proses enkripsi dengan metode sebelumnya yaitu 5.

Agar kunci (*key*) yang ada bisa digunakan untuk proses enkripsi dengan metode *Hill Cipher*, kunci akan dibentuk matriks 2x2 dengan melakukan proses perhitungan sederhana.

$$key = 5 \quad k = \begin{bmatrix} key & key - 1 \\ key + 1 & key + 2 \end{bmatrix} \quad k = \begin{bmatrix} 5 & 5 - 1 \\ 5 + 1 & 5 + 2 \end{bmatrix}$$

Jadi, *key* yang digunakan untuk proses enkripsi dengan metode *Hill Cipher* ini adalah:

$$k = \begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix}$$

Selanjutnya membagi deretan bilangan desimal pada *ciphertext2* menjadi blok matriks yang sesuai dengan jumlah kolom matriks kunci (*key* = 2x2).

$$\begin{bmatrix} 135 \\ 127 \end{bmatrix} \quad \begin{bmatrix} 175 \\ 159 \end{bmatrix} \quad \begin{bmatrix} 63 \\ 87 \end{bmatrix}$$

Kemudian melakukan perhitungan pada matriks kunci (*key*) dengan blok matriks *ciphertext2*.

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 135 \\ 127 \end{bmatrix} = \begin{bmatrix} 1183 \\ 1699 \end{bmatrix} \text{mod } 255 = \begin{bmatrix} 163 \\ 169 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 175 \\ 159 \end{bmatrix} = \begin{bmatrix} 1511 \\ 2163 \end{bmatrix} \text{mod } 255 = \begin{bmatrix} 236 \\ 123 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 63 \\ 87 \end{bmatrix} = \begin{bmatrix} 663 \\ 987 \end{bmatrix} \text{mod } 255 = \begin{bmatrix} 153 \\ 222 \end{bmatrix}$$

Kemudian pada proses terakhir, ubah bilangan desimal hasil perhitungan matriks di atas menjadi karakter, dapat dilihat pada Tabel 4.

Tabel 4. Proses Konversi Bilangan Desimal ke Karakter

Desimal	Ciphertext
163	£
169	©
236	ì
123	{
153	™
222	Þ

Pada Tabel 4 dapat dilihat hasil *ciphertext* akhir dari kombinasi metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher*, *ciphertext* berupa karakter bilangan ASCII. Jadi, *ciphertext* dari kata VISUAL adalah £©ì{™Þ.

Selanjutnya melakukan proses dekripsi untuk mengetahui apakah kombinasi metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* berhasil atau tidak dalam pengamanan pesan. Untuk melakukan proses dekripsi yang pertama adalah dimulai dengan metode *Hill Cipher* yaitu dengan melakukan perkalian pada invers matriks kunci dengan blok matriks *ciphertext*.

$$k = \begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \quad \det k = (5 \cdot 7) - (4 \cdot 6) = 11$$

invers modulo:

$$11^{-1} \text{ mod } 255$$

$$11x = 1 \text{ mod } 255$$

$$11x = 1 + 255k$$

$$x = (1 + 255k) / 11$$

Cari k=n sehingga hasil x adalah bilangan bulat.

k=0; $x=(1+255*0)/11 = 1/11$ (bukan bilangan bulat)
k=1; $x=(1+255*1)/11 = 23.2$ (bukan bilangan bulat)
k=2; $x=(1+255*2)/11 = 46.4$ (bukan bilangan bulat)
k=3; $x=(1+255*3)/11 = 69.6$ (bukan bilangan bulat)
k=4; $x=(1+255*4)/11 = 92.8$ (bukan bilangan bulat)
k=5; $x=(1+255*5)/11 = 116$ (bilangan bulat)
Sehingga invers dari 11 mod 255 ekuivalen dengan 116 mod 255 yaitu **116**.

Invers modulo determinan digunakan untuk mencari invers matriks.

$$k = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ maka } k^{-1} = \text{determinan} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Sehingga,

$$k^{-1} = 116 \begin{bmatrix} 7 & -4 \\ -6 & 5 \end{bmatrix} = \begin{bmatrix} 812 & -464 \\ -696 & 580 \end{bmatrix} \text{ mod } 255$$

$$= \begin{bmatrix} 47 & 46 \\ 69 & 70 \end{bmatrix}$$

Untuk modulo bilangan negatif dapat dikerjakan dengan:
-n mod x

$$\text{maka, } -n \text{ mod } x = x - (n \text{ mod } x)$$

$$= 255 - (464 \text{ mod } 255) = 46$$

$$= 255 - (696 \text{ mod } 255) = 69$$

Setelah matriks k di-invers, selanjutnya mengalikan matriks k dengan *ciphertext*.

$$\begin{bmatrix} 47 & 46 \\ 69 & 70 \end{bmatrix} \begin{bmatrix} 163 \\ 169 \end{bmatrix} = \begin{bmatrix} 15435 \\ 23077 \end{bmatrix} \text{ mod } 255 = \begin{bmatrix} 135 \\ 127 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 46 \\ 69 & 70 \end{bmatrix} \begin{bmatrix} 236 \\ 123 \end{bmatrix} = \begin{bmatrix} 16750 \\ 24894 \end{bmatrix} \text{ mod } 255 = \begin{bmatrix} 175 \\ 159 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 46 \\ 69 & 70 \end{bmatrix} \begin{bmatrix} 153 \\ 222 \end{bmatrix} = \begin{bmatrix} 17403 \\ 26097 \end{bmatrix} \text{ mod } 255 = \begin{bmatrix} 63 \\ 87 \end{bmatrix}$$

Setelah didapatkan hasil dari proses perhitungan, maka nilai-nilai desimal tersebut dikonversikan ke dalam bilangan biner untuk diproses selanjutnya, hasil konversi dapat dilihat pada Tabel 5.

Tabel 5. Proses Konversi Bilangan Desimal ke Biner

<i>Plaintext2</i>	<i>Biner</i>
135	10000111
127	01111111
175	10101111
159	10011111
63	00111111
87	01010111

Selanjutnya dilakukan proses dekripsi kembali metode *Vernam Cipher* dengan fungsi logika Ex-OR masih dengan kunci yang sama yaitu 5. Sebelumnya kunci diubah menjadi bilangan biner terlebih dahulu, 5 = 00110101.

$$\begin{array}{r} 10000111 \\ 00110101 \\ \hline 10110010 \end{array} \oplus \begin{array}{r} 01111111 \\ 00110101 \\ \hline 01001010 \end{array} \oplus \begin{array}{r} 10101111 \\ 00110101 \\ \hline 10011010 \end{array}$$

$$\begin{array}{r} 10011111 \\ 00110101 \\ \hline 10101010 \end{array} \oplus \begin{array}{r} 00111111 \\ 00110101 \\ \hline 00001010 \end{array} \oplus \begin{array}{r} 01010111 \\ 00110101 \\ \hline 01100010 \end{array}$$

Setelah didapatkan hasil dari proses dekripsi dengan logika Ex-OR, maka nilai-nilai biner tersebut didekripsi lagi untuk yang terakhir kalinya dengan metode *Caesar Cipher* dengan kunci (*key*) yang sama yaitu 5. Dekripsi metode ini dengan melakukan proses pergeseran pada bilangan biner dari suatu karakter tertentu sebanyak 5 langkah (sesuai *key*) ke arah kiri, kemudian ubah hasil pergeseran bilangan biner tersebut dengan karakter, dapat dilihat pada Tabel 6.

Tabel 6. Proses Dekripsi Metode Caesar Cipher.

<i>Plaintext1</i>	<i>Hasil</i>	<i>Plaintext</i>
10110010	01010110	V
01001010	01001001	I
10011010	01010011	S
10101010	01010101	U
00001010	01000001	A
01100010	01001100	L

Pada Tabel 5 dapat dilihat proses dekripsi dengan metode *Caesar Cipher* yang merupakan proses dekripsi akhir dari kriptografi metode kombinasi ini. *Plaintext* yang didapatkan yaitu kata VISUAL yang sesuai dengan pesan yang dienkripsi dengan kombinasi dari ketiga metode ini. Hal ini menunjukkan bahwa metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* dapat dikombinasikan dalam proses kriptografi (enkripsi dan dekripsi).

7. Kesimpulan

Dari hasil penelitian dapat diambil beberapa kesimpulan antara lain:

1. Metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* adalah jenis kriptografi klasik, tetapi cukup kuat jika dilihat dari segi keamanannya dengan sedikit modifikasi.
2. Metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* dapat dikombinasikan menjadi satu dalam proses kriptografi (enkripsi dan dekripsi) dengan tingkat keamanan yang sangat baik dan sulit untuk dipecahkan.
3. Kombinasi metode *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* ini hanya membutuhkan sebuah kunci (*key*) dalam proses enkripsi maupun dekripsi yang akan memudahkan kita untuk mengingatnya.

Daftar Pustaka

- [1] Andrian, Yudhi, *Kombinasi Kriptografi Caesar Cipher dan Steganografi Citra Digital Metode LSB*, 2014.
- [2] Dey, Somdip, *SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted*, 2013.
- [3] Ryabko, Boris, *The Vernam Cipher is Robust to Small Deviations from Randomness*. 9 Mar 2013.
- [4] Magambar, Kondwani, et al., *Variable-length Hill Cipher with MDS Key Matrix*, 2012.
- [5] Farmambar, Mina and Alexander G. Chefranov, *Investigation of Hill Cipher Modification Based on Permutation and Iteration*,

International Journal of Computer Science and Information
Security (IJSIS), Vol. 10, No. 9, September 2012.

Biodata Penulis

Khairani Puspita, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Sistem Informasi Universitas Potensi Utama Medan, lulus tahun 2010. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Komputer UPI YPTK Padang, lulus tahun 2014. Saat ini menjadi Dosen di Universitas Potensi Utama Medan.

Email: khairan.adwa@gmail.com.

M. Rhifky Wayahdi, mahasiswa Jurusan Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama Medan.

Email: muhammadrhifkywayahdi@gmail.com dan rhifky.wayahdi@yahoo.com.