AFFINE-HILL-LU *CIPHER WITH* MATLAB *IMPLEMENTATION*

Joko Eliyanto
Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Ahmad Dahlan
joko1400015006@webmail.uad.ac.id

Abstract

Affine Hill LU Cipher is a Cipher Technique that incorporates Affine Cipher and Hill Cipher. Affine cipher is the cipher that uses a form $y = ax + b$ *where the integers modulo a must have an inverse in* Z_{29} *. Hill cipher is the cipher that uses a key of a square matrix and that inverse for the encryption and decryption process. The incorporation of this technique is done by replacing the integer a by a square matrix invertible in* Z_{29} A *and B is a regular square matrix. Identify matrix invertible in the* Z_{29} *is not an easy thing. Matrices L and U is a decomposition matrix of a square matrix. L is the lower triangular matrix, so that's must be invertible matrix .So we get new form of the cipher* $Y = LX + U$*. The key matrix of this cipher is K which can be decomposed into a matrix L & U, so by a single key we can produce two other key that is L and U. By this form we expected to produce a tough and difficult to hack. To identify the decomposition Matrix L and U, also to encrypt and decrypt this cipher it's so complex . To overcome this, the technique is implemented in MATLAB (Matrix Laboratory) software to calculate the matrix accurately and efficiently.*

Keyword : Affine-Hill-LU Cipher, Encryption Algorithm, Decryption Algorithm , Matrix $\boldsymbol{Z_{29}^{n\times n}}$***,LU Decomposition.***

PENDAHULUAN

Sandi Affine

Pada sandi Affine, teknik persandian menggunakan fungsi berikut :

$$\boldsymbol{e(x) = (ax + b) mod\ 29\ a, b\ \in \mathbb{Z}_{29}}$$

Proses dekripsi dan enkripsi sesuai kriptosistem berikut :

Diberikan $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{29}$ dan diberikan

$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{29} \times \mathbb{Z}_{29} : \gcd(a, 29) = 1\}$.

Untuk $K = (a, b) \in \mathcal{K}$, didefinisikan

$$e_K(x) = (ax + b) \bmod 29$$

Dan

$$d_K(y) = a^{-1}(y - b) \bmod 29$$

$$(x, y\ \in \mathbb{Z}_{29})$$

Sandi Hill

Sandi ini ditemukan pada tahun 1993 oleh Lester S.Hill. Diberikan m bilangan bulat positif, dan didefinisikan $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{29})^m$. Ide dasarnya adalah untuk mengambil kombinasi linear dari karakter huruf m pada plainteks, yang selanjutnya menghasilkan karakter huruf pada cipherteks.

Diberikan $m \geq 2$ bilangan bulat .Diberikan $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{29})^m$ dan diberikan

$\mathcal{K} = \{m \times m$ matriks $invertible$ pada $\mathbb{Z}_{29}\}$.

Untuk setiap kunci K,we definisikan

$$e_K(x) = xK$$

Dan

$$d_K(y) = yK^{-1}$$

$$(x, y\ \in \mathbb{Z}_{29})$$

 ISBN 978-979-3812-42-7

Dari kedua sandi ini , disusun sebuah sandi baru yang menggabungkan keduanya yaitu sani Affine-Hill dengan keriptosistem sebagai berikut :

Diberikan $\mathcal{P} = \mathcal{C} = Z_{29}^{n\times n}$ dan diberikan

$$\mathcal{K} = \{(A,B)|, A, B, A^{-1} \in Z_{29}^{n\times n}\}$$

dengan *m* adalah bilangan prima

dan $n \in Z$, $n \geq 2$, maka untuk setiap $K = (A,B) \in \mathcal{K}$,

didefinisikan

$$e_K(X) = (AX + B)\ mod\ 29$$

Dan

$$d_K(Y) = A^{-1}(Y - B)\ mod\ 29$$

$A, B, A^{-1} \in Z_{29}^{n\times n}$ dan A adalah matriks *multiplicative invertible* (memiliki *invers* modulo pada$Z_{29}^{n\times n}$) .

Sandi ini memiliki kelemahan yaitu untuk mencari matriks kunci yang memenuhi kriteria dalam kriptosistem tersebut. Maka sandi ini dikembangkan dengan teori Matriks Dekomposisi LU, dimana sebuah matriks persegi tunggal dapat difaktorkan menjadi dua buah matriks L dan U yang kemudian menggantikan matriks kunci A dan B.

HASIL DAN PEMBAHASAN

Kriptosistem Sandi Affine-Hill-LU

Diberikan $\mathcal{P} = \mathcal{C} = Z_{29}^{n\times n}$
dan diberikan

$\mathcal{K} = \{(K,L,U)|K, L, U, L^{-1} \in Z_{29}^{n\times n}$
$, L\ U\ matrix\ dekomposisi\ dari\ K\}$

dengan *m* adalah bilangan prima
dan $n \in Z$, $n \geq 2$, maka untuk setiap $K = K = (L,U) \in \mathcal{K}$,

didefinisikan

$$e_K(X) = (LX + U)\ mod\ 29$$

Dan

$$d_K(Y) = L^{-1}(Y - U)\ mod\ 29$$

$K, L, U, L^{-1} \in Z_{29}^{n\times n}$ dan L adalah matriks *multiplicative invertible* (memiliki invers modulo pada$Z_{29}^{n\times n}$) .

Didefinisikan

$$L^{-1} = \big(inv\ mod(\det(L)) * Adjoint(L)\big)(mod\ 29)$$

Karakteristik Matriks Kunci K

Didefiniskan Matriks $K \in Z_{29}^{n\times n}$ maka

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{bmatrix}$$

kemudian dicari matriks dekomposisi L U dengan bentuk seperti berikut:

$$L = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{n1} & l_{n2} & \cdots & 1 \end{bmatrix}$$

$$U = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix}$$

(Epperson, 20013:430-435). Sesuai teorema yang berbunyi :

Jika A adalah matriks segitiga $n \times n$ (segitiga atas , segitiga bawah , atau diagonal) maka det(A) adalah hasil kali entri-entri diagonal utama matriks tersebut ; yaitu det(A) = $a_{11}a_{22}\cdots a_{nn}$.(Rorres , 2004: 98-99)

Maka determinan matriks L = 1, karena semua elemen diagonalnya=1, maka dipastikan L *invertible.*

Algoritma Enkripsi Affine-Hill-LU

Cipher

1. *Input* :
   a. Plainteks
   b. Matriks Kunci K

2. *Output* :
   Cipherteks

 ISBN 978-979-3812-42-7

3. Langkah-langkah :
   a. Masukkan plainteks
   b. Masukkan Matriks kunci K
   c. Penghitungan dan pengujian dekomposisi L U dari K, apakah L $L, U \in Z_{29}^{n \times n}$
   d. Menguji apakah setiap L dan U anggota $\mathbb{Z}_{29}$.
   e. Mengubah plainteks menjadi huruf kapital.
   f. Mengubah plainteks menjadi angka anggota $\mathbb{Z}_{29}$.
   g. Mengecek kunci L,U adalah matriks bujur sangkar.
   h. Jika modulo jumlah elemen matriks plainteks dengan jumlah elemen matriks L tidak sama dengan 0 , maka plainteks ditambah angka 0 sebanyak selisih dari elemen kunci dan hasil modulo tsb, dan sebaliknya .
   i. Mengubah bentuk matriks *vector* plainteks menjadi matriks. dengan ukuran kolom sama dengan jumlah elemen kunci.
   j. Mengubah bentuk matriks plainteks menjadi matriks dengan ukuran $n \times m$, m =kolom tergantung jumlah huruf.
   k. Mendeskripsikan matriks kunci U baru dengan jumlah kolom sama dengan plainteks.
   l. Mengenkripsi masing masing matriks plainteks dengan formula berikut :
   $$e_K(X) = (LX + U) mod\ 29$$
   m. Mengubah bentuk matriks *cipher* menjadi *vector cipher*.
   n. Mengubah *vector cipher* menjadi huruf.

Algoritma Dekripsi Affine-Hill-LU *Cipher*

1. *Input* :
   a. Cipherteks
   b. Matriks Kunci K
2. *Output* :
   Plainteks
3. Langkah-langkah :
   a. Masukkan cipherteks
   b. Matriks kunci K
   c. Penghitungan dan pengujian dekomposisi L U dari K, apakah L $L, U \in Z_{29}^{n \times n}$
   d. Menguji apakah setiap L dan U anggota $\mathbb{Z}_{29}$.
   e. Mengubah cipherteks menjadi huruf kapital .
   f. Mengubah cipherteks menjadi angka anggota $\mathbb{Z}_{29}$
   g. Mengecek kunci L,U adalah matriks bujur sangkar.
   h. Jika modulo jumlah elemen matriks cipherteks dengan jumlah elemen matriks L tidak sama dengan 0 , maka cipherteks ditambah angka 0 sebanyak selisih dari elemen kunci dan hasil modulo tsb, dan sebaliknya
   i. Mengubah bentuk matriks *vector* cipherteks menjadi matriks dengan ukuran kolom sama dengan jumlah elemen kunci.
   j. Mengubah bentuk matriks cipherteks menjadi matriks dengan ukuran $n \times m$, m =kolom tergantung jumlah huruf.
   k. Mendeskripsikan matriks kunci U baru dengan jumlah kolom sama dengan cipherteks
   l. Mendenkripsi masing masing matriks cipherteks dengan formula berikut :
   $$d_K(Y) = L^{-1}(Y - U) mod\ 29$$
   m. Mengubah bentuk matriks plainteks menjadi *vector* plainteks.
   n. Mengubah *vector* plainteks menjadi huruf.

M-File Affine-Hill-LU

Enkripsi_AHLU

```
%Affine_Hill_Encrypt_Break_Plain
text
P=input('Masukkan Matriks
Plaintetxt= ','s');%input
matriks yang akan dipecah
%Menghilangkan Spasi
P=upper(P);%membuat kalimat
menjadi huruf kapital
P=real(P);%membuat karakter pada
kalimat menjadi angka ASCII
cP=P-65;%membuat representasi
huruf a=0 , b=1 dst sampai z=25
indeks_spasi=find(cP<0);%mencari
spasi(nilai indeks spasi)/ spasi
slalu kurang dari 0
cP([indeks_spasi])=[];%menghilan
gkan elemen spasi
```

 ISBN 978-979-3812-42-7

```
K=input('Masukkan kunci K(HARUS
MATRIKS BUJUR SANGKAR)=
');%matrik yang akan menjadi
panutan pemecahan
n=size(K);
n=n(1,1);
[L,A]=LU_factor(K,n);
U=A;
if ceil(L)~=L
    Error('Dekomposisi L bukan
anggota Z29!');
else
    L=L;
end
if ceil(U)~=U
    Error('Dekomposisi U bukan
anggota Z29!');
else
    U=U;
end
ukuran_kunci=size(L);%ukuran
matriks kunci
if ukuran_kunci(1,1)==
ukuran_kunci(1,2)%cek matriks
kunci bujur sangkar atau tidak

m=ukuran_kunci(1,1)*ukuran_kunci
(1,2);%hasil kali jumlah baris
dan kolom(jumlah elemen)
else
    disp('Matriks Kunci Tidak
Sesuai Permintaan');
end
j=size(L,2);
a=size(cP);
a=a(1,2);%jumlah elemen matriks
target
if mod(a,m)==0
    cP=cP;
else
if a>m
    X=zeros(1,abs(m-
mod(a,m)));%a>m
    cP=[cP X];
else
    X=zeros(1,abs(a-
mod(a,m)));%m>a
    cP=[cP X];
end
end
cP;h=size(cP);h=h(1,2);Plain=res
hape(cP,m,(h/m));
n=size(Plain,2);Plain=reshape(Pl
ain,j,j*n);U=[U U U];
C=mod(L*Plain+U,29);l=size(C,1)*
size(C,2);C=reshape(C,1,l);
C=C+65;C=char(C);disp('Ciphertex
t');disp(C);
```

Dekripsi_AHLU

```
%Affine_Hill_Encrypt_Break_Plain
text
P=input('Masukkan Matriks
Cipherteks= ','s');%input
matriks yang akan dipecah
%Menghilangkan Spasi
P=upper(P);%membuat kalimat
menjadi huruf kapital
P=real(P);%membuat karakter pada
kalimat menjadi angka ASCII
cP=P-65;%membuat representasi
huruf a=0 , b=1 dst sampai z=25
indeks_spasi=find(cP<0);%mencari
spasi(nilai indeks spasi)/ spasi
slalu kurang dari 0
cP([indeks_spasi])=[];%menghilan
gkan elemen spasi
K=input('Masukkan kunci (HARUS
MATRIKS BUJUR SANGKAR)=
');%matrik yang akan menjadi
panutan pemecahan
n=size(K);
n=n(1,1);
[L,A]=LU_factor(K,n);
U=A;
if ceil(L)~=L
    Error('Dekomposisi L bukan
anggota Z29!');
else
    L=L;
end
if ceil(U)~=U
    Error('Dekomposisi U bukan
anggota Z29!');
else
    U=U;
end

ukuran_kunci=size(L);%ukuran
matriks kunci
```

 ISBN 978-979-3812-42-7

```
if ukuran_kunci(1,1)==
ukuran_kunci(1,2)%cek matriks
kunci bujur sangkar atau tidak

m=ukuran_kunci(1,1)*ukuran_kunci
(1,2);%hasil kali jumlah baris
dan kolom(jumlah elemen)
else
    disp('Matriks Kunci Tidak
Sesuai Permintaan');
end
j=size(L,2);
a=size(cP);
a=a(1,2);%jumlah elemen matriks
target
if mod(a,m)==0
    cP=cP;
else
if a>m
    X=zeros(1,abs(m-
mod(a,m)));%a>m
    cP=[cP X];
else
    X=zeros(1,abs(a-
mod(a,m)));%m>a
    cP=[cP X];
end
end
cP;h=size(cP);h=h(1,2);Cipher=re
shape(cP,m,(h/m));n=size(Cipher,
2);Cipher=reshape(Cipher,j,j*n);
U=[U U U];
K1=inverse_matix_modulo(L);C=mod
(K1*(Cipher-U),29);
l=size(C,1)*size(C,2);C=reshape(
C,1,l);C=C+65;C=char(C);
disp('Plaintext');disp(C);
```

Implementasi Enkripsi Affine-Hill-LU *Cipher* dengan MATLAB

```
>> Enkripsi_AHLU
Masukkan Matriks Plaintetxt=
matematika uad yogyakarta
Masukkan kunci K(HARUS MATRIKS
BUJUR SANGKAR)= [1 2 -2;2 1 2;0
0 2]
Ciphertext
NYTGRARXMBUAF\OENCLURVGA\GC
```

Implementasi Dekripsi Affine-Hill-LU *Cipher* dengan MATLAB

```
>> Dekripsi_AHLU
Masukkan Matriks Cipherteks=
NYTGRARXMBUAF\OENCLURVGA\GC
Masukkan kunci (HARUS MATRIKS
BUJUR SANGKAR)= [1 2 -2;2 1 2;0
0 2]
Plaintext
MATEMATIKAUADYOGYAKARTAAAAA
```

KESIMPULAN

Dalam penelitian ini sandi Affine-Hill-LU terbukti mampu diimplementasi dengan baik , secara teoritis sandi ini lebih kuat dibandingkan sandi Affine atau Hill saja, terutama terhadap *cryptanalysis* dengan metode *known plaintext attack* dan *statistical analysis* karena lebih banyaknya kemungkinan *ciphertext* yang dihasilkan. Perbedaan mendasar dengan Affine-Hill biasa adalah sandi ini hanya membutuhkan kunci tunggal dengan spesifikasi tertentu sehingga sandi ini cukup sulit untuk dibuat begitu juga untuk dipecahkan. Sandi Affine-Hill-LU ini juga dapat dijadikan sebagai khasanah baru dari perkembangan sandi klasik yang sudah ada dan dapat dikembangkan dengan teori-teori lain.

REFERENSI

Anton Howard. Rorres Chris. 2004. *Aljabar Linear Elementer Versi Aplikasi*.Edisis Kedelapan Jilid 1. Jakarta: Erlangga.

Barr, Thomas.H. 2002. *Invitation to Cryptology.* Upper Saddle River, NJ: Prentice Hall,Inc.

Dian Eka Wijayanti .2016 *Modifikasi Tehnik Transformasi Affine dalam Kriptografi* . Lembaga Penelitian dan Pengembangan Universitas Ahmad Dahlan Yogyakarta .

Epperson James F. 2013. *An Introduction to Numerical Methods amd Analysis* . Second Edition .New York :John Willey & Sons.Inc

M.G.Vara Prasad, P.Pari Purna Chari, K.Pydi Satyam 2016. *Affine Hill cipher key generation matrix of order 3 by using in an arbitrary line y=ax+b*. International Journal of Science Technology and Management Vol. No 5, Issue No. 8, Agustus Hal. (268-272).

Schneier, B. 1996. *Applied Cryptography : Protocols, Algorithms, and Source Code in C.* SecondEdition . New York : John Wiley & Sons, Inc.

Setyaningsih Emi. 2015 . *Kriptografi & Implementasinya menggunakan MATLAB.* Yogyakarta : Penerbit Andi

Stinson, R.D. 2006. *Cryptography Theory and Practice* .Third Edition. New York: Chapman & Hall/CRC.