

Diketahui Matriks kunci K 3x3

K =

11	23	9
26	7	17
19	13	3

0 sd 36

P= 26(Huruf)+10(

5280

Teks terdiri dari huruf besar (26), angka (10) dan spasi. Total 37 karakter

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8

T	U	V	W	X	Y	Z	0	1
19	20	21	22	23	24	25	26	27

A. Pembentukan K^{-1}

Langkah 1: Hitung determinan K

Determinan K =

5280

$A = \text{Det } K \text{ Mod } P = 5280 \text{ mod } 37 =$

26

-0.04
0.046
0.039

Langsu
Ini tida

Langkah 2: Hitung $\text{Det}^{-1} \text{ Mod } 37$ atau $(1/\text{Det}) \text{ Mod } 37$

Dengan algoritma EEA

N	Det	1	2	2	1	3	
37	26	11	4	3	1	0	
0	1	-1	3	-7	10	-37	

Sehingga $\text{Det}^{-1} =$

30

Langkah 3: Hitung Kofaktor matriks K

C11 diperoleh dengan menghilangkan Baris 1 dan Kolom 1

Secara umum:

Untuk menghitung Cij hilangkan baris i dan kolom j

C11=

1	7	17
	13	3

C12=

-1	23	9
	13	3

C11=

22
-200

C12=

11
48 11

C21=

-1	26	17
	19	3

C22=

1	11	9
	19	3

C21=

23

C22=

10

C31=

1	26	7
	19	13

C32=

-1	11	23
	19	13

C31=

20

C32=

35
294 35

Perhitungan Kofaktor Cij di atas sudah langsung dilakukan transpose, s

Langkah 4: Kalikan $1/\text{Det}$ dengan matriks Adjoint K dan modulkan dengan 37 untuk mendapatkan K^{-1}

$$\text{inv}(K) = \begin{matrix} & \text{Adjoint} \\ 26 & \begin{bmatrix} 22 & 11 & 32 \\ 23 & 10 & 10 \\ 20 & 35 & 34 \end{bmatrix} \end{matrix} \pmod{37} = \begin{bmatrix} 572 \\ 598 \\ 520 \end{bmatrix}$$

Bukti: Kalikan K dengan Inv(K) harus menghasilkan matriks Identitas I

$$\begin{matrix} & K \\ \begin{bmatrix} 11 & 23 & 9 \\ 26 & 7 & 17 \\ 19 & 13 & 3 \end{bmatrix} & \times \end{matrix} \begin{matrix} & \text{Inv}(K) \\ \begin{bmatrix} 17 & 27 & 18 \\ 6 & 1 & 1 \\ 2 & 22 & 33 \end{bmatrix} \end{matrix} =$$

B. Enkripsi:

Plaintext

C	1	P	H	E	R
2	27	15	7	4	17

p1= C1P

p2=HER

C1=

$$\begin{matrix} & K \\ \begin{bmatrix} 11 & 23 & 9 \\ 26 & 7 & 17 \\ 19 & 13 & 3 \end{bmatrix} & * \end{matrix} \begin{matrix} & P \\ \begin{bmatrix} 2 \\ 27 \\ 15 \end{bmatrix} \end{matrix} \pmod{37} =$$

C2=

$$\begin{matrix} & K \\ \begin{bmatrix} 11 & 23 & 9 \\ 26 & 7 & 17 \\ 19 & 13 & 3 \end{bmatrix} & * \end{matrix} \begin{matrix} & P \\ \begin{bmatrix} 7 \\ 4 \\ 17 \end{bmatrix} \end{matrix} \pmod{37} =$$

Chipertext

3	O	W	J	F	5
1	15	27	26	18	14

C. Dekripsi:

P1 =

$$\begin{matrix} & \text{inv}(K) \\ \begin{bmatrix} 12 & 24 & 6 \\ 32 & 33 & 7 \\ 25 & 9 & 36 \end{bmatrix} & * \end{matrix} \begin{matrix} & C \\ \begin{bmatrix} 1 \\ 15 \\ 27 \end{bmatrix} \end{matrix} \pmod{37} =$$

P2 =

$$\begin{matrix} & \text{inv}(K) \\ \begin{bmatrix} 12 & 24 & 6 \\ 32 & 33 & 7 \\ 25 & 9 & 36 \end{bmatrix} & * \end{matrix} \begin{matrix} & C \\ \begin{bmatrix} 26 \\ 18 \\ 14 \end{bmatrix} \end{matrix} \pmod{37} =$$

Plaintext

C	1	P	H	E	R
---	---	---	---	---	---

Kembali ke teks semula

Hill Cipher:

Enkrip / Dekrip minimum 2 karakter maksimum tidak dibatasi

Matriks 2x2 ==> blok = 2

Matriks 3x3 ==> blok = 3

Matriks 4x4 ==> blok = 4

Matriks harus invertible (ada

Matriks 2x2

bilangan dalam matriks adalah 0 s.d N-1

1. Hitung $|K|$ determinan K
2. Hitung $|K|^{-1}$ dalam MOD N
3. Hitung invers (K)
4. Enkrip $C=K \times P$
5. Dekrip $P=\text{invers}(K) \times C$

$$K = \begin{bmatrix} 8 & 12 \\ 32 & 5 \end{bmatrix}$$

Mod 37 ==> 26 huruf; 10 angka; spas

Bilangan kita = 0 sd 36

-344

$$1. \det(K) = \begin{matrix} & & -344 & 26 & \text{Berapa } 26^{-1} \text{ Mod } 37 \\ & 1 & 2 & 2 & 1 & 3 \end{matrix}$$

$$2. \begin{bmatrix} 37 & 26 & 11 & 4 & 3 & 1 & 0 \\ 0 & 1 & -1 & 3 & -7 & 10 & \text{STOP} \end{bmatrix}$$

Bukti: 1

$$3. \text{Invers}(K) = |K|^{-1} * \text{Adjoint } K$$

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 8 & 12 \\ 32 & 5 \end{bmatrix}$$

$$\text{Adjoint}(K) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 5 & -12 \\ -32 & 8 \end{bmatrix}$$

$$\text{Invers}(K) = \begin{matrix} 10 & \begin{bmatrix} 5 & 25 \\ 5 & 8 \end{bmatrix} & \begin{matrix} 50 & 250 \\ 50 & 80 \end{matrix} \end{matrix}$$

Bukti : $K * \text{Invers}(K) = \text{Identitas}$

$$\begin{matrix} 260 & 296 \\ 481 & 926 \end{matrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

4. Enkrip

Teks: SATU p1=SA p2=TU p1=(18 0) p2=(19 20)

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8

T	U	V	W	X	Y	Z	0	1
19	20	21	22	23	24	25	26	27

$$c1 = \begin{bmatrix} 8 & 12 \\ 32 & 5 \end{bmatrix} * \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 144 \\ 576 \end{bmatrix} = \begin{bmatrix} 33 \\ 21 \end{bmatrix}$$

$$c2 = \begin{bmatrix} 8 & 12 \end{bmatrix} * \begin{bmatrix} 19 \end{bmatrix} = \begin{bmatrix} 392 \end{bmatrix} = 22$$

32	5
----	---

20

708

5

CT:

7VWF

33 21 22 5

5. Dekrip $P = \text{invers}(K) * C$

p1=

13	28
13	6

*

33
21

=

1017
555

=

18
0

p2=

13	28
13	6

*

22
5

=

426
316

=

19
20

Angka)- 37 k

J	K	L	M	N	O	P	Q	R	S
9	10	11	12	13	14	15	16	17	18

2	3	4	5	6	7	8	9	
28	29	30	31	32	33	34	35	36

Kinvers

0.009	0.062
-0.03	0.009
0.056	-0.099

I

1	0	0
0	1	0
0	0	1

ng menggunakan excel untuk menghitung invers dari K

k kita lakukan karena K Invers harus berisi bilangan bulat antara 0 sampai 36 juga

$$26 + 10 = 30$$

$$\text{Bukti} = 1$$

brs+kolom genap (+1)

brs+kolom ganjil (-1)

aturan penentuan + atau -

C13=	1	23	9
		7	17

$$C13 = 32$$

C23=	-1	11	9
		26	17

$$C23 = 10$$

C33=	1	11	23
		26	7

$$C33 = 34$$

ehingga untuk menghitung invers kita tidak perlu lagi melakukan transpose

286	832	=	17	27	18
260	260		6	1	1
910	884		2	22	33

343	518	518
518	1083	1036
407	592	454

Mod 37 =

10	0	0
0	10	0
0	0	10

cT 30WJF5

c1=30W

$$\begin{array}{|c|} \hline 778 \\ \hline 496 \\ \hline 434 \\ \hline \end{array} \bmod 37 = \begin{array}{|c|} \hline 1 \\ \hline 15 \\ \hline 27 \\ \hline \end{array}$$

C1=	3
	0
	W

$$\begin{array}{|c|} \hline 322 \\ \hline 499 \\ \hline 236 \\ \hline \end{array} \bmod 37 = \begin{array}{|c|} \hline 26 \\ \hline 18 \\ \hline 14 \\ \hline \end{array}$$

J
F
5

C2=JF5

$$\begin{array}{|c|} \hline 534 \\ \hline 716 \\ \hline 1132 \\ \hline \end{array} \bmod 37 = \begin{array}{|c|} \hline 16 \\ \hline 13 \\ \hline 22 \\ \hline \end{array}$$

P1=	C
	1
	P

$$\begin{array}{|c|} \hline 828 \\ \hline 1524 \\ \hline 1316 \\ \hline \end{array} \bmod 37 = \begin{array}{|c|} \hline 14 \\ \hline 7 \\ \hline 21 \\ \hline \end{array}$$

P2=	H
	E
	R

inversnya) dalam Mod N ($N = \text{jumlah karakter}$)

• Invers Matriks

Matriks $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dapat di-invers apabila $ad - bc \neq 0$
 Dengan Rumus =

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

Apabila A dan B adalah matriks seordo dan memiliki balikan maka AB dapat di-invers
 dan $(AB)^{-1} = B^{-1}A^{-1}$

Pada Matrix 3 x 3 Invers dihitung dengan : $\frac{1}{\det(M)} * \text{Adjoint (coFactor (M))}$

$$K * \text{invers}(K) = \text{Identitas}$$

5	25
5	8

13	28
13	6

J	K	L	M	N	O	P	Q	R	S
9	10	11	12	13	14	15	16	17	18

2	3	4	5	6	7	8	9	
28	29	30	31	32	33	34	35	36

==> 7
 V

==> W

F

S

A

T
U

