Diketahui Matriks kunci K 3x3

0 sd 36

P= 26(Huruf)+10(

| | | | |
|---|---|---|---|
| K = | 11 | 23 | 9 |
| | 26 | 7 | 17 |
| | 19 | 13 | 3 |

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 | | -0.04 |
| | | | 0.046 |
| | | | 0.039 |

A=Det K Mod P = 5280 mod 37 = 26 Langsu

Ini tida

Langkah 2: Hitung Det^-1 Mod 37 atau (1/Det) 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 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 | C12= | -1 | 23 | 9 |
| | | 13 | 3 | | | 13 | 3 |
| C11= | 22 | | | C12= | 11 | | |
| | -200 | | | | 48 | 11 | |
| C21= | -1 | 26 | 17 | C22= | 1 | 11 | 9 |
| | | 19 | 3 | | | 19 | 3 |
| C21= | 23 | | | C22= | 10 | | |
| C31= | 1 | 26 | 7 | C32= | -1 | 11 | 23 |
| | | 19 | 13 | | | 19 | 13 |
| C31= | 20 | | | C32= | 35 | | |
| | | | | | 294 | 35 | |

**Perhitungan Kofaktor Cij di atas sudah langsung dilakukan transpose, s**

Langkah 4: Kalikan 1/Det dengan matriks Adjoint K dan modulokan dengan 37 untuk mendapatkan K Inv

inv(K)= 26 × Adjoint

| | | |
|---|---|---|
| 22 | 11 | 32 |
| 23 | 10 | 10 |
| 20 | 35 | 34 |

mod 37 =

| |
|---|
| 572 |
| 598 |
| 520 |

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

K

| | | |
|---|---|---|
| 11 | 23 | 9 |
| 26 | 7 | 17 |
| 19 | 13 | 3 |

x Inv(K)

| | | |
|---|---|---|
| 17 | 27 | 18 |
| 6 | 1 | 1 |
| 2 | 22 | 33 |

=

B. Enkripsi:

Plaintext

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

p1= C1P
p2=HER

C1= K

| | | |
|---|---|---|
| 11 | 23 | 9 |
| 26 | 7 | 17 |
| 19 | 13 | 3 |

* P

| |
|---|
| 2 |
| 27 |
| 15 |

mod 37 =

C2= K

| | | |
|---|---|---|
| 11 | 23 | 9 |
| 26 | 7 | 17 |
| 19 | 13 | 3 |

* P

| |
|---|
| 7 |
| 4 |
| 17 |

mod 37 =

Chipertext

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

C. Dekripsi:

P1 = inv(K)

| | | |
|---|---|---|
| 12 | 24 | 6 |
| 32 | 33 | 7 |
| 25 | 9 | 36 |

* C

| |
|---|
| 1 |
| 15 |
| 27 |

mod 37 =

P2 = inv(K)

| | | |
|---|---|---|
| 12 | 24 | 6 |
| 32 | 33 | 7 |
| 25 | 9 | 36 |

* C

| |
|---|
| 26 |
| 18 |
| 14 |

mod 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=KxP
5. Dekrip P=invers(K)xC

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

K =

| | |
|---|---|
| 8 | 12 |
| 32 | 5 |

Bilangan kita = 0 sd 36

-344

1. det(K) = -344 26 Berapa 26^(-1) Mod 37

1 2 2 1 3

2.

| | | | | | | |
|---|---|---|---|---|---|---|
| 37 | 26 | 11 | 4 | 3 | 1 | 0 |
| 0 | 1 | -1 | 3 | -7 | 10 | STOP |

Bukti: 1

3. Invers(K) = |K|^-1 * Adjoint K

K

| | |
|---|---|
| a | b |
| c | d |

| | |
|---|---|
| 8 | 12 |
| 32 | 5 |

Adjoint (K)

| | |
|---|---|
| d | -b |
| -c | a |

| | |
|---|---|
| 5 | -12 |
| -32 | 8 |

Invers (K)

10

| | |
|---|---|
| 5 | 25 |
| 5 | 8 |

50 250
50 80

Bukti : K * Invers (K) = Identitas

260 296
481 926

| | |
|---|---|
| 1 | 0 |
| 0 | 1 |

4. Enkrip

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

K P

c1=

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | 12 | * | 18 | = | 144 | = 33 |
| 32 | 5 | | 0 | | 576 | 21 |

c2=

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | 12 | * | 19 | = | 392 | = 22 |

| | | | | |
|---|---|---|---|---|
| 32 | 5 | 20 | 708 | 5 |

CT: **7VWF** 33 21 22 5

5. Dekrip P = invers(K) * C

p1=

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 13 | 28 | * | 33 | = | 1017 | = | 18 |
| 13 | 6 | | 21 | | 555 | | 0 |

p2=

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 13 | 28 | * | 22 | = | 426 | = | 19 |
| 13 | 6 | | 5 | | 316 | | 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

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 |

I

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 343 | 518 | 518 | | 10 | 0 | 0 |
| 518 | 1083 | 1036 | Mod 37 = | 0 | 10 | 0 |
| 407 | 592 | 454 | | 0 | 0 | 10 |

cT **3OWJF5**

c1=3OW

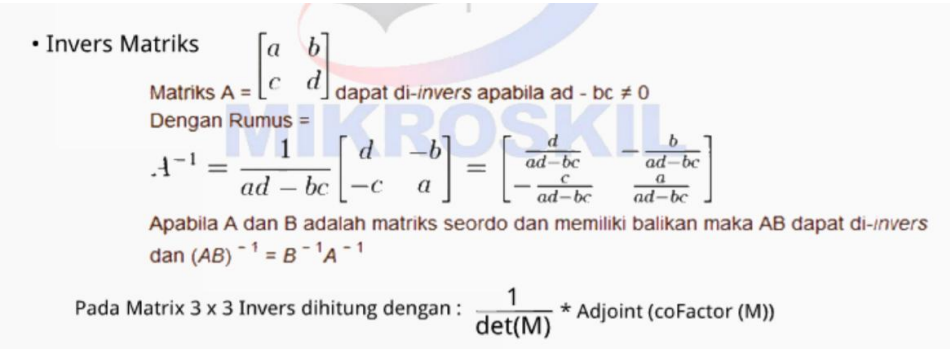
| | | | | | |
|---|---|---|---|---|---|
| 778 | | 1 | | 3 | |
| 496 | mod 37 = | 15 | C1= | O | |
| 434 | | 27 | | W | |

| | | | | | |
|---|---|---|---|---|---|
| 322 | | 26 | | J | c2=JF5 |
| 499 | mod 37 = | 18 | C2= | F | |
| 236 | | 14 | | 5 | |

| | | | | | |
|---|---|---|---|---|---|
| 534 | | 16 | | C | |
| 716 | mod 37 = | 13 | P1= | 1 | |
| 1132 | | 22 | | P | |

| | | | | | |
|---|---|---|---|---|---|
| 828 | | 14 | | H | |
| 1524 | mod 37 = | 7 | P2= | E | |
| 1316 | | 21 | | R | |

inversnya) dalam Mod N (N = jumlah karakter)




;i

K*invers(K) = 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 |