Nama : **Panji Iman Baskoro**
NRP : **171111023**
Program Studi : **Teknik Informatika**

1. Berikut ini ada sebuah pesen asli : " **UJIAN TENGAH SEMESTER** " lakukan enkripsi dan deskripsi (Dengan algoritma Kode Hill).

   Kunci yang digunakan :

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$$

Jawab :

A = 0, … , Z = 25

Plaintext :

U	J	I	A	N	T	E	N	G	A	H	S	E	M	E	S	T	E	R	R
20	9	8	0	13	19	4	13	6	0	7	18	4	12	4	18	19	4	17	17
BLOK 1		BLOK 2		BLOK 3		BLOK 4		BLOK 5		BLOK 6		BLOK 7		BLOK 8		BLOK 9		BLOK 10	

Perkalian Key Matriks :

BLOK 1

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \times \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} 67 \\ 105 \end{bmatrix}$$

$$\text{Mod } 26 = \begin{bmatrix} 15 \\ 1 \end{bmatrix} = \begin{bmatrix} P \\ B \end{bmatrix}$$

BLOK 2

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \times \begin{bmatrix} 8 \\ 0 \end{bmatrix} = \begin{bmatrix} 16 \\ 24 \end{bmatrix}$$

$$\text{Mod } 26 = \begin{bmatrix} 16 \\ 24 \end{bmatrix} = \begin{bmatrix} Q \\ Y \end{bmatrix}$$

BLOK 3

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \times \begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} 83 \\ 134 \end{bmatrix}$$

$$\text{Mod } 26 = \begin{bmatrix} 5 \\ 4 \end{bmatrix} = \begin{bmatrix} F \\ E \end{bmatrix}$$

BLOK 6

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \times \begin{bmatrix} 7 \\ 18 \end{bmatrix} = \begin{bmatrix} 68 \\ 111 \end{bmatrix}$$

$$\text{Mod } 26 = \begin{bmatrix} 16 \\ 7 \end{bmatrix} = \begin{bmatrix} Q \\ H \end{bmatrix}$$

BLOK 7

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \times \begin{bmatrix} 4 \\ 12 \end{bmatrix} = \begin{bmatrix} 42 \\ 72 \end{bmatrix}$$

$$\text{Mod } 26 = \begin{bmatrix} 18 \\ 20 \end{bmatrix} = \begin{bmatrix} S \\ U \end{bmatrix}$$

BLOK 8

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \times \begin{bmatrix} 4 \\ 18 \end{bmatrix} = \begin{bmatrix} 62 \\ 102 \end{bmatrix}$$

$$\text{Mod } 26 = \begin{bmatrix} 10 \\ 24 \end{bmatrix} = \begin{bmatrix} K \\ Y \end{bmatrix}$$

BLOK 4

$$\begin{bmatrix}2 & 3\\3 & 5\end{bmatrix} \times \begin{bmatrix}4\\13\end{bmatrix} = \begin{bmatrix}47\\77\end{bmatrix}$$

$$\text{Mod 26} \quad = \begin{bmatrix}21\\25\end{bmatrix} = \begin{bmatrix}V\\Z\end{bmatrix}$$

BLOK 5

$$\begin{bmatrix}2 & 3\\3 & 5\end{bmatrix} \times \begin{bmatrix}6\\0\end{bmatrix} = \begin{bmatrix}12\\18\end{bmatrix}$$

$$\text{Mod 26} \quad = \begin{bmatrix}12\\18\end{bmatrix} = \begin{bmatrix}M\\S\end{bmatrix}$$

BLOK 9

$$\begin{bmatrix}2 & 3\\3 & 5\end{bmatrix} \times \begin{bmatrix}19\\4\end{bmatrix} = \begin{bmatrix}50\\77\end{bmatrix}$$

$$\text{Mod 26} \quad = \begin{bmatrix}24\\25\end{bmatrix} = \begin{bmatrix}Y\\Z\end{bmatrix}$$

BLOK 10

$$\begin{bmatrix}2 & 3\\3 & 5\end{bmatrix} \times \begin{bmatrix}17\\17\end{bmatrix} = \begin{bmatrix}85\\136\end{bmatrix}$$

$$\text{Mod 26} \quad = \begin{bmatrix}7\\6\end{bmatrix} = \begin{bmatrix}H\\G\end{bmatrix}$$

Hasil Enkripsi :

U	J	I	A	N	T	E	N	G	A	H	S	E	M	E	S	T	E	R	R
P	B	Q	Y	F	E	V	Z	M	S	Q	H	S	U	K	Y	Y	Z	H	G

Proses Dekripsi :

a) Determinan Matrix

$$\text{Det} = \begin{bmatrix}2 & 3\\3 & 5\end{bmatrix} = 2.5 - 3.3 = 1$$

b) Invers Matrix

$$Mk^{-1} = \begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}$$

c) Invers Mod Determinan

$$k = n = \frac{1+n(k)}{det}$$

$$k = 0 = \frac{1+26(0)}{1} = 1$$

$$1 \times \begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix} = \begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix} \text{mod26}$$

$$= \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}$$

Perkalian Key Matrix :

Blok 1

$$\begin{bmatrix}P\\B\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}15\\1\end{bmatrix}$$

$$= \begin{bmatrix}98\\347\end{bmatrix} \text{mod 26}$$

$$= \begin{bmatrix}20\\29\end{bmatrix} = \begin{bmatrix}U\\J\end{bmatrix}$$

Blok 2

$$\begin{bmatrix}Q\\Y\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}16\\24\end{bmatrix}$$

$$= \begin{bmatrix}632\\416\end{bmatrix} \text{mod 26}$$

$$= \begin{bmatrix}8\\0\end{bmatrix} = \begin{bmatrix}I\\A\end{bmatrix}$$

Blok 3

$$\begin{bmatrix}F\\E\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}$$

Blok 6

$$\begin{bmatrix}Q\\H\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}16\\7\end{bmatrix}$$

$$= \begin{bmatrix}241\\382\end{bmatrix} \text{mod 26}$$

$$= \begin{bmatrix}7\\18\end{bmatrix} = \begin{bmatrix}H\\S\end{bmatrix}$$

Blok 7

$$\begin{bmatrix}S\\U\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}18\\20\end{bmatrix}$$

$$= \begin{bmatrix}550\\454\end{bmatrix} \text{mod 26}$$

$$= \begin{bmatrix}4\\12\end{bmatrix} = \begin{bmatrix}E\\M\end{bmatrix}$$

Blok 8

$$\begin{bmatrix}K\\Y\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}10\\24\end{bmatrix}$$

$= \begin{bmatrix}117\\123\end{bmatrix} \bmod 26$

$= \begin{bmatrix}13\\19\end{bmatrix} = \begin{bmatrix}N\\T\end{bmatrix}$

$= \begin{bmatrix}602\\278\end{bmatrix} \bmod 26$

$= \begin{bmatrix}4\\18\end{bmatrix} = \begin{bmatrix}E\\S\end{bmatrix}$

Blok 4

$\begin{bmatrix}V\\Z\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}21\\25\end{bmatrix}$

$= \begin{bmatrix}680\\533\end{bmatrix} \bmod 26$

$= \begin{bmatrix}4\\13\end{bmatrix} = \begin{bmatrix}E\\N\end{bmatrix}$

Blok 5

$\begin{bmatrix}M\\S\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}12\\18\end{bmatrix}$

$= \begin{bmatrix}474\\312\end{bmatrix} \bmod 26$

$= \begin{bmatrix}6\\0\end{bmatrix} = \begin{bmatrix}G\\A\end{bmatrix}$

Blok 9

$\begin{bmatrix}Y\\Z\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}24\\25\end{bmatrix}$

$= \begin{bmatrix}695\\602\end{bmatrix} \bmod 26$

$= \begin{bmatrix}19\\4\end{bmatrix} = \begin{bmatrix}T\\E\end{bmatrix}$

Blok 10

$\begin{bmatrix}H\\G\end{bmatrix} = \begin{bmatrix}5 & 23\\23 & 2\end{bmatrix}\begin{bmatrix}7\\6\end{bmatrix}$

$= [173] \bmod 26$

$= \begin{bmatrix}17\\17\end{bmatrix} = \begin{bmatrix}R\\R\end{bmatrix}$

Hasil Dekripsi :

P	B	Q	Y	F	E	V	Z	M	S	Q	H	S	U	K	Y	Y	Z	H	G
U	J	I	A	N	T	E	N	G	A	H	S	E	M	E	S	T	E	R	R

2. Dari nomer 1, namun pesen asli tersebut anda ubah dulu menjadi ASCI (A=65) dan dalam bentuk biner (dengan cara BCD saja). Selanjutnya lakukan enkripsi (metode geser 1 Key : 1010) dan pengiriman data secara blok :
   a. ECB (Mode Electronic Code Book)
   b. CBC (Mode Cipher Blok Chaining)

   Jawab :

   ECB (Mode Electronic Code Book)

U	J	I	A	N	T	E	N
85	74	73	65	78	84	69	78
01010101	01001010	01001001	01000001	01001110	01010100	01000101	01001110

G	A	H	S	E	M	E	S
71	65	72	83	69	77	69	83
01000111	01000001	01001000	01010011	01000101	01001101	01000101	01010011

T	E	R
84	69	82
01010100	01000101	01010010

Plaintext to Biner :

01010101010010100100100101000001010011100101010001000101010011100100011101
00000101001000010100110100010101001101010001010101001101010100010001010101
0010

Plot to 4 Block :

0101 0101 0100 1010 0100 1001 0100 0001 0100 1110 0101 0100
0100 0101 0100 1110 0100 0111 0100 0001 0100 1000 0101 0011
0100 0101 0100 1101 0100 0101 0101 0011 0101 0100 0100 0101
0101 0010

Blok Biner :

Blok	0101	0101	0100	1010	0100	1001	0100	0001	0100
Key	1010	1010	1010	1010	1010	1010	1010	1010	1010
XOR	1111	1111	1110	0000	1110	0011	1110	1011	1110
Geser 1	1111	1111	1101	0000	1101	0110	1101	0111	1101

Blok	1110	0101	0100	0100	0101	0100	1110	0100	0111
Key	1010	1010	1010	1010	1010	1010	1010	1010	1010
XOR	0100	1111	1110	1110	1111	1110	0100	1110	1101
Geser 1	1000	1111	1101	1101	1111	1101	1000	1101	1011

Blok	0100	0001	0100	1000	0101	0011	0100	0101	0100
Key	1010	1010	1010	1010	1010	1010	1010	1010	1010
XOR	1110	1011	1110	0010	1111	1001	1110	1111	1110
Geser 1	1101	0111	1101	0100	1111	0011	1101	1111	1101

Blok	1101	0100	0101	0101	0011	0101	0100	0100	0101
Key	1010	1010	1010	1010	1010	1010	1010	1010	1010
XOR	0111	1110	1111	1111	1001	1111	1110	1110	1111
Geser 1	1110	1101	1111	1111	0011	1111	1101	1101	1111

Blok	0101	0010
Key	1010	1010
XOR	1111	1000
Geser 1	1111	0001

Hasil Geser 1 Block :

11111111 11010000 11010110 11010111 11011000 11111101 11011111 11011000 11011011 11010111 11010100 11110011 11011111 11011110 11011111 11110011 11111101 11011111 11110001	**Chiper**
255 208 214 215 216 253 223 216 219 215 212 243 223 222 223 243 253 223 241	**Decimal**

FF D0 D6 D7 D8 FD DF D8 DB D7 D4 F3 DF DE DF F3 FD DF F1	**Hexa**

CBC (Mode Cipher Blok Chaining)

U	J	I	A	N	T	E	N
55	4A	49	41	4E	54	45	4E
01010101	01001010	01001001	01000001	01001110	01010100	01000101	01001110

G	A	H	S	E	M	E	S
47	41	48	53	45	4D	45	53
01000111	01000001	01001000	01010011	01000101	01001101	01000101	01010011

T	E	R
54	45	52
01010100	01000101	01010010

Enkripsi Biner

Inisialisasi Vektor (C0) = 01001110

Kunci (K) harus 8 bit = 00001010

Biner	01010101	01001010	01001001	01000001	01001110	01010100	01000101
C_{n-1}	01001110	00100010	11000100	00001111	10001000	10011001	10001111
Hasil XOR Biner Baru (P_n)	00011011	01101000	10001101	01001110	11000110	11001101	11001010
K	00001010	00001010	00001010	00001010	00001010	00001010	00001010
XOR	00010001	01100010	10000111	01000100	11001100	11000111	11000000
Geser 1 (C_n)	00100010	11000100	00001111	10001000	10011001	10001111	10000001
HEXA	22	C4	0F	88	99	8F	81

Biner	01001110	01000111	01000001	01001000	01010011	01000101	01001101
C_{n-1}	10000001	10001011	10001101	10001101	10011111	10001101	10000101
Hasil XOR Biner Baru (P_n)	11001111	11001100	11001100	11000101	11001100	11001000	11001000

K	00001010	00001010	00001010	00001010	00001010	00001010	00001010
XOR	11000101	11000110	11000110	11001111	11000110	11000010	11000010
Geser 1 (C_n)	10001011	10001101	10001101	10011111	10001101	10000101	10000101
HEXA	8B	8D	8D	9F	8D	85	85

Biner	01000101	01010011	01010100	01000101	01010010
C_{n-1}	10000101	10010101	10011001	10001111	10000001
Hasil XOR Biner Baru (P_n)	11000000	11000110	11001101	11001010	11010011
K	00001010	00001010	00001010	00001010	00001010
XOR	11001010	11001100	11000111	11000000	11011001
Geser 1 (C_n)	10010101	10011001	10001111	10000001	10110011
HEXA	95	99	8F	81	B3

Hasil Chiperteks Enkripsi CBC : 22C40F88998F818B8D8D9F8D858595998F81B3