암호문: THANKW TC ETEHYMNM, f(T O)=(T C), f(N E)=(N M)

1) f(T O)=(T C)와 f(N E)=(N M)을 수식으로 나타내시오.

f(19 14)=(19 2), f(13 4)=(13 12)

2) 위의 1)식을 Hill암호에 적용 K= $\begin{pmatrix} & b \\ c & d \end{pmatrix}$ 하여 수식으로 나타내시오.

(19 14)$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$=(19 2), (13 4)$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$=(13 12)

3) 위의 2)식을 변수(a, c)와 변수(b, d)로 나누어 나타내시오.

$19a + 14c = 19 \pmod{26}$ $\quad$ $\begin{cases} 19b + 14d = 2 \pmod{26} \\ 13b + 4d = 12 \pmod{26} \end{cases}$
$13a + 4c = 13 \pmod{26}$

4) 변수 $\begin{pmatrix} a \\ c \end{pmatrix}$의 값을 구하시오(과정도 쓰세요)

$\begin{cases} 19a + 14c = 19 \pmod{26} \\ 13a + 4c = 13 \pmod{26} \end{cases}$는 $\begin{cases} 38a + 28c = 38 \pmod{26} \\ 91a + 28c = 91 \pmod{26} \end{cases}$, $\begin{cases} 247a + 182c = 247 \pmod{26} \\ 247a + 76c = 247 \pmod{26} \end{cases}$과 같다.

53a=53, 즉 a=1이며 gcd(1,26)=1|1이므로 1개의 해가 존재한다. 즉, a=1이다.

또한 106c=0, 즉 2c=0, 26 ... 이며 gcd(2,26)=2|26이므로 2개의 해가 존재한다.

대입을 통해, c=0, 13임을 알 수 있다. 따라서 $\begin{pmatrix} a \\ c \end{pmatrix}$ = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 13 \end{pmatrix}$이다.

5) 변수 $\begin{pmatrix} b \\ d \end{pmatrix}$의 값을 구하시오(과정도 쓰세요)

$\begin{cases} 19b + 14d = 2 \pmod{26} \\ 13b + 4d = 12 \pmod{26} \end{cases}$는 $\begin{cases} 38b + 28d = 4 \pmod{26} \\ 91b + 28d = 84 \pmod{26} \end{cases}$, $\begin{cases} 247b + 182d = 26 \pmod{26} \\ 247b + 76d = 228 \pmod{26} \end{cases}$과 같다.

53b=80, 즉 b=2이며 gcd(1,26)=1|2이므로 1개의 해가 존재한다. 즉, b=2이다.

또한 106d=-202, 즉 2d=6, 32 ... 이며 gcd(2,26)=2|6이므로 2개의 해가 존재한다.

대입을 통해, d=3, 16임을 알 수 있다. 따라서 $\begin{pmatrix} b \\ d \end{pmatrix}$ = $\begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 16 \end{pmatrix}$이다.

6) 암호키의 후보 K= $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$의 값을 구하시오.

해는 다음과 같으며,

$\begin{pmatrix} a \\ c \end{pmatrix}$ = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ 은 $\begin{pmatrix} 1 \\ 13 \end{pmatrix}$, $\begin{pmatrix} b \\ d \end{pmatrix}$ = $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ 혹은 $\begin{pmatrix} 2 \\ 16 \end{pmatrix}$

따라서 암호키의 후보는 아래와 같이 4가지이다.

① $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$= $\begin{matrix} 1 & 2 \\ 0 & 3 \end{matrix}$, ② $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$=$\begin{pmatrix} 1 & 2 \\ 0 & 16 \end{pmatrix}$, ③ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$=$\begin{pmatrix} 1 & 2 \\ 13 & 3 \end{pmatrix}$, ④ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$=$\begin{pmatrix} 1 & 2 \\ 13 & 16 \end{pmatrix}$

7) 위의 암호키 K= $\begin{pmatrix} & b \\ c & d \end{pmatrix}$에 대한 복호키의 유무를 결정하시오.

① |K|= $\begin{vmatrix} 1 & 2 \\ 0 & 3 \end{vmatrix}$ = 3-0=3이므로 역행렬이 존재한다.

② |K|= $\begin{vmatrix} 1 & 2 \\ 0 & 16 \end{vmatrix}$ = 16-0=16이므로 역행렬이 존재하지 않아 복호키가 될 수 없다.

③ |K|= $\begin{vmatrix} 1 & 2 \\ 13 & 3 \end{vmatrix}$ = 3-26=-23=3이므로 역행렬이 존재한다.

④ |K|= $\begin{vmatrix} 1 & 2 \\ 13 & 16 \end{vmatrix}$ = 16-26=-10=16이므로 역행렬이 존재하지 않아 복호키가 될 수 없다.

8) 암호키 K= $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$에 대하여 존재하는 복호키와 복호문을 구하시오.

① $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$= $\begin{pmatrix} 1 & 2 \\ 13 & 3 \end{pmatrix}$의 복호키를 구하는 과정은 다음과 같다.

|K|= $\begin{vmatrix} 1 & 2 \\ 13 & 3 \end{vmatrix}$ =3-26=-23=3이고, K의 역행렬 ^{1}는 다음과 같이 계산된다.

$$3^{-1}\begin{pmatrix} 3 & -2 \\ -13 & 1 \end{pmatrix} = 9\begin{pmatrix} 3 & -2 \\ -13 & 1 \end{pmatrix} = \begin{pmatrix} 27 & -18 \\ -117 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 13 & 9 \end{pmatrix} \pmod{26}$$

그러므로 복호키 K^{-1}= $\begin{pmatrix} 1 & 8 \\ 13 & 9 \end{pmatrix}$ 이다.

따라서 복호문을 다음과 같이 구할 수 있다.

(19 7)$\begin{pmatrix} 1 & 8 \\ 13 & 9 \end{pmatrix}$ =(19+91 152+63)=(100 215)=(22 7)=(W H)

(0 13)$\begin{pmatrix} 1 & 8 \\ 13 & 9 \end{pmatrix}$ =(169 117)=(13 13)=(N N)

즉, THAN => WHNN이므로 올바른 복호키가 아님을 알 수 있다.

② $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$= $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$의 복호키를 구하는 과정은 다음과 같다.

|K|= $\begin{vmatrix} 1 & 2 \\ 0 & 3 \end{vmatrix}$ =3-0=3이고, K의 역행렬 K^{-1}는 다음과 같이 계산된다.

$$3^{-1}\begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = 9\begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 27 & -18 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix} \pmod{26}$$

그러므로 복호키 K^{-1}= $\begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix}$ 이다.

따라서 복호문을 다음과 같이 구할 수 있다.

(19 7)$\begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix}$ =(19 152+63)=(19 215)=(19 7)=(T H)

(0 13)$\begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix}$ =(0 117)=(0 13)=(A N)

즉, THAN => THAN이므로 올바른 복호키임을 알 수 있다.

9) 암호문 THANKW TC ETEHYMNM의 복호문을 구하시오.

해답: 암호키 K= $\begin{matrix} b \\ c\ d \end{pmatrix}$= $\begin{matrix} 1\ 2 \\ 0\ 3 \end{pmatrix}$의 복호키 ^{1}는 K^{-1}=$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ 이므로 다음과 같다.

암호문 (T H)에 대한 복호문은 CK^{-1}=(19 7)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(19 7)=(T H) 이다.

암호문 (A N)에 대한 복호문은 CK^{-1}=(0 13)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(0 13)=(A N) 이다.

암호문 (K W)에 대한 복호문은 CK^{-1}=(10 22)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(10 18)=(K S) 이다.

암호문 (T C)에 대한 복호문은 CK^{-1}=(19 2)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(19 14)=(T O) 이다.

암호문 (E T)에 대한 복호문은 CK^{-1}=(4 19)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(4 21)=(E V) 이다.

암호문 (E H)에 대한 복호문은 CK^{-1}=(4 7)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(4 17)=(E R) 이다.

암호문 (Y M)에 대한 복호문은 CK^{-1}=(24 12)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(24 14)=(Y O) 이다.

암호문 (N M)에 대한 복호문은 CK^{-1}=(13 12)$\begin{pmatrix} 1\ 8 \\ 0\ 9 \end{pmatrix}$ =(13 4)=(N E) 이다.

T	H	A	N	K	S	T	O	E	V	E	R	Y	O	N	E
19	7	0	13	10	18	19	14	4	21	4	17	24	14	13	4
19	7	0	13	10	22	19	2	4	19	4	7	24	12	13	12
T	H	A	N	K	W	T	C	E	T	E	H	Y	M	N	M

그러므로 THANKW TC ETEHYMNM의 복호문은 THANKS TO EVERYONE 이다.