p36 복습문제

#1 세 가지 보안 목표를 정의하시오.

- 기밀성

정보 보안에서 가장 널리 알려진 분야로, 조직은 정보의 기밀성을 위협하는 악의적인 행동들에 대응해야 하고 군대에서는 민감한 정보가 노출되는 것을 방지해야 한다. 그리고 산업체에서는 조직의 운명을 위하여 필수적으로 경쟁자에게 정보를 숨겨야하고 은행 업무를 볼 때, 고객의 계좌 정보는 보호되어야 한다.

- 무결성

변경이 인가된 자에 의해서 인가된 매커니즘을 통해서만 이루어져야 한다는 것으로, 은행에서 고객이 돈을 입금하거나 출금할 때, 그 계좌의 금액은 변경되어야 한다. 그러나 무결성 체계이 항상 악의적인 행동의 결과로 나타나는 것이 아니다.

- 가용성

인가된 자가 접근할 수 있어야 한다는 것으로, 고객이 생산하고 저장하는 정보는 인가된 자가 사용할 수 있어야 하며, 정보가 유용하지 않으면 소모가 없다.

#3 두개의 보안 서비스를 기술하고 정의하시오.

- 데이터 기밀성 : 노출 공격으로부터 데이터를 보호하기 위하여 고안되었다. 매우 광범위하고, 메시지의 일부분이나 전체에 대한 기밀성을 포함하며 트래픽 분석에 대응한다. 데이터 기밀성은 스누핑과 트래픽 분석 공격을 막기 위하여 고안되었다.
- 데이터 무결성 : 공격자가 데이터의 변경, 삽입, 삭제, 재전송 등으로부터 데이터를 보호하는 것이며 메시지의 일부나 전부를 보호한다.
- 인증 : 통신의 상대편에 대한 인증을 제공한다. 연결형 통신에서는 연결 설정 시 송신자 또는 수신자에 대한 인증을 제공하고, 비연결형 통신에서는 데이터의 출처를 인증한다.
- 부인봉쇄 : 데이터의 송신자나 수신자가 부인하지 못하도록 한다. 출처 증명을 제공하는 부인봉쇄에서 데이터의 수신자는 그 메시지가 부인될 경우 송신자의 신원을 증명할 수 있다.
- 접근제어 : 비인가된 접근으로부터 데이터를 보호한다. 접근이라는 용어는 읽기, 쓰기, 변경, 프로그램 실행 등을 포함한다.

p70

#16(b) gcd(291, 42)

	s_i	t_i	r_i	q_i	
i=0	1	0	291		
i=1	0	1	42	6	
i=2	1	-6	39	1	gcd(291, 42) = 13
i=3	-1	6	3	13	s = -1, t = 6
i=4			0		

#31 모듈로 20에서 모든 곱셈에 대한 역원 쌍을 나열하시오.

다음의 6쌍의 역원

: (1,1), (3,7), (9,9), (11,11), (13,17), (19,19)

이 존재한다.

#33(a) a. $25x + 10y = 15$ 의 특수해와 일반해를 구하시오.

$d = \gcd(25, 10) = 5$

1. $5x + 2y = 3$

	s_i	t_i	r_i	q_i
$i=0$	1	0	5	
$i=1$	0	1	2	2
$i=2$	1	-2	1	2
$i=3$			0	

$s = 1$, $t = -2$

=> 특수해 : $x_0 = 3$, $y_0 = -6$

=> 일반해 : $x = 3 + 2k$, $y = 3 - 2k$

#37(c) c. $9x + 4 \equiv 12 \pmod 7$ 의 모든 해를 구하시오.

$9x \equiv 8 \pmod 7$

$\gcd(9, 7) = 1$ 이기 때문에, 방정식은 한 근을 가진다.

그 근은 $x_0 = (8 \times 9^{-1}) \bmod 7 = (8 \times 3) \bmod 7 = 3$

#40(c) c. $7x + 3y = 3 \pmod 7$ 에 대한 모든 해를 구하시오.

$4x + 2y = 5 \pmod 7$

$$\begin{pmatrix} 7 & 3 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

$$2^{-1} \begin{bmatrix} 2 & -3 \\ -4 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \end{bmatrix} = 4 \begin{bmatrix} 2 & 4 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \end{bmatrix} = 4 \begin{bmatrix} 6+20 \\ 9 \end{bmatrix}$$

$$4 \begin{bmatrix} 26 \\ 9 \end{bmatrix} = 4 \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 20 \\ 8 \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \end{bmatrix}$$

$x = 6$, $y = 1$

p109

#15 Alice는 흔히 a에서 z까지의 문자와 0에서 9까지의 숫자로 구성된 평문을 암호화해야 한다.

a. 덧셈 암호를 사용하면 키 공간은 Z_{36} 이고 모듈로 값은 36이다.

b. 곱셈 암호를 사용하면 키 공간은 Z_{36}^* 이고 모듈로 값은 36이다.

c. 아핀 암호를 사용하면 키공간은 Z_{36}^* 이고 모듈로 값은 36이다.

#25 Hill 암호를 이용하여 "We live in an insecure world"라는 문장을 암호화하시오. 이때, 다음과 같은 키를 사용한다.

$$K=\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}$$

we	li	ve	in	an	in	se	cu	re	wo	rl	dz
22 04	11 08	21 04	08 13	00 13	08 13	18 04	02 20	17 04	22 14	17 11	03 25

$$[22\ 04]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[66+20\ \ 44+28]=[86\ \ 72]=[8\ \ 20]\quad IU$$

$$[11\ 08]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[33+40\ \ 22+56]=[73\ \ 78]=[21\ \ 0]\quad VA$$

$$[21\ 04]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[63+20\ \ 42+28]=[83\ \ 70]=[5\ \ 18]\quad FS$$

$$[08\ 13]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[24+65\ \ 16+91]=[89\ \ 107]=[11\ \ 3]\quad LD$$

$$[00\ 13]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[65\ \ 91]=[13\ \ 13]\quad NN$$

$$[08\ 13]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[24+65\ \ 16+91]=[89\ \ 107]=[11\ \ 3]\quad LD$$

$$[18\ 04]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[54+20\ \ 36+28]=[74\ \ 64]=[22\ 12]\quad WM$$

$$[02\ 20]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[6+100\ \ 4+140]=[106\ \ 144]=[2\ \ 14]\quad CO$$

$$[17\ 04]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[51+20\ \ 34+28]=[71\ \ 62]=[19\ \ 10]\quad TK$$

$$[22\ 14]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[66+70\ \ 44+98]=[136\ \ 142]=[6\ \ 12]\quad GM$$

$$[17\ 11]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[51+55\ \ 34+77]=[106\ \ 111]=[2\ \ 7]\quad CH$$

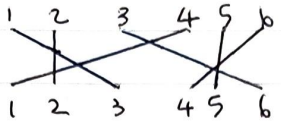
$$[03\ 25]\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}=[9+125\ \ 6+175]=[134\ \ 181]=[4\ \ 25]\quad EZ$$

IU VAFS LD NN LDWMCOTK GMCHEZ

#34 (3, 2, 6, 1, 5, 4)에 대응되는 복호 키를 구하시오.

3 2 6 1 5 4

암호 키



4 2 1 6 5 3

복호 키

#35 (3, 2, 6, 1, 5, 4)를 키로 하는 전치 암호의 암호화 키의 행렬 표현을 적고, 복호 키의 행렬 표현을 구하시오.

3 2 6 1 5 4

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

4 2 1 6 5 3

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$