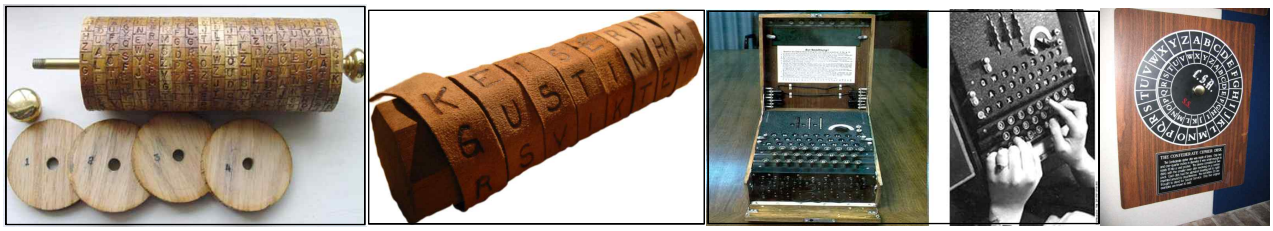
1장
- 암호 / 암호화
- 정보시스템의 역기능
- 정보보호 3요소
- 암호사용 목적
- 암호학 목적
- 암호
- 고대암호 / 근대암호
- 환자암호 / 전치암호
- 도구 이름과 사용법?



2장
- 유클리드 호제법을 이용하여 222와 690의 최대 공약수를 구하여라.
- Euler의 φ함수(φ-function)란 무엇인지 설명하시오.
- 252를 소인수 분해하고 φ(252)을 구하여라.

3장
- 시프트암호 (key 값에 따른 암호문 만들기)
- Affine 암호 (k1, k2 두 개 킷값을 이용한 암호문 만들기)
- Hill 암호 (2글자 암호문 만들기, 2X2 행렬 곱셈연산 이용한 암호문 만들기)
- Nihillist 암호
- Playfair 암호
- 암호해독 4가지 공격방법
- vigenere 암호 / feistel암호 / 스트림암호

암호 문제 예제

1. 시프트 암호의 키가 5일 때, 다음의 평문을 암호화 하는 과정을 보이시오
평문 : This is really important information.

2. Affine 암호의 키가 $k_1 = 9, k_2 = 11$ 일 때, 다음 평문을 암호화하는 과정을 보이시오.
평문 : jungbo

3. Hill 암호의 행렬 $k \equiv \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$를 이용하여 다음 평문을 암호화하는 과정을 보여라.
평문 : olla

4. Korea라는 키워드를 사용하여 Nihilist 암호화 하는 과정을 보이시오
평문 : important information

5. 다음의 표에 따라 ADFGVX 암호화과정을 보이시오. (단, 전치 키워드는 crypto 이다.)
평문 : important information

	A	D	F	G	V	X
A	f	x	a	9	u	1
D	n	g	0	l	d	o
F	5	b	k	2	h	z
G	m	j	s	y	t	v
V	7	4	3	e	8	i
X	c	w	q	6	r	p

6. 키워드가 koreait 일 때 Playfair 암호표를 기술하고(Q생략, Q=Z), Playfair 암호화 하시오.
평문 : important information