

1장. 암호의 기초

학습목표

- 용어 정리
- 역사
- 알고리즘(암호화, 복호화)
- 암호 기법
 - 대치, 치환, 대체, 환자(다른 문자로 치환)
 - 순열, 환치, 전치(암호의 위치를 바꿈)
 - 확산
 - 혼돈

암호의 용어

👤 Cryptography

cryptography

1. 암호 해독법 2. 암호 기술 3. 암호론

- 정보를 안전하게(secure) 지속되도록 하는 방법
- 암호화

👤 메시지(Message = M), 평문(Plaintext = P)

👤 키(Key = K)

👤 암호문(Ciphertext = C)

👤 암호화(Encryption = E)

- 암호화 함수 : E
- 예) $E_k(M) = C$

👤 복호화(Decryption = D)

- 복호화 함수 : D
- 예) $D_k(C) = M$



암호의 용어

암호학(Cryptology)

- 암호 알고리즘 개발과 암호 분석에 관한 학문
- = Cryptos(=hidden) + logos(science)

Cryptanalyst(암호 분석가)

cryptanalyst
암호 해독 전문가

- 암호사용자가 암호화한 것을 해독하려(cryptanalysis)는 사람

Cryptographer

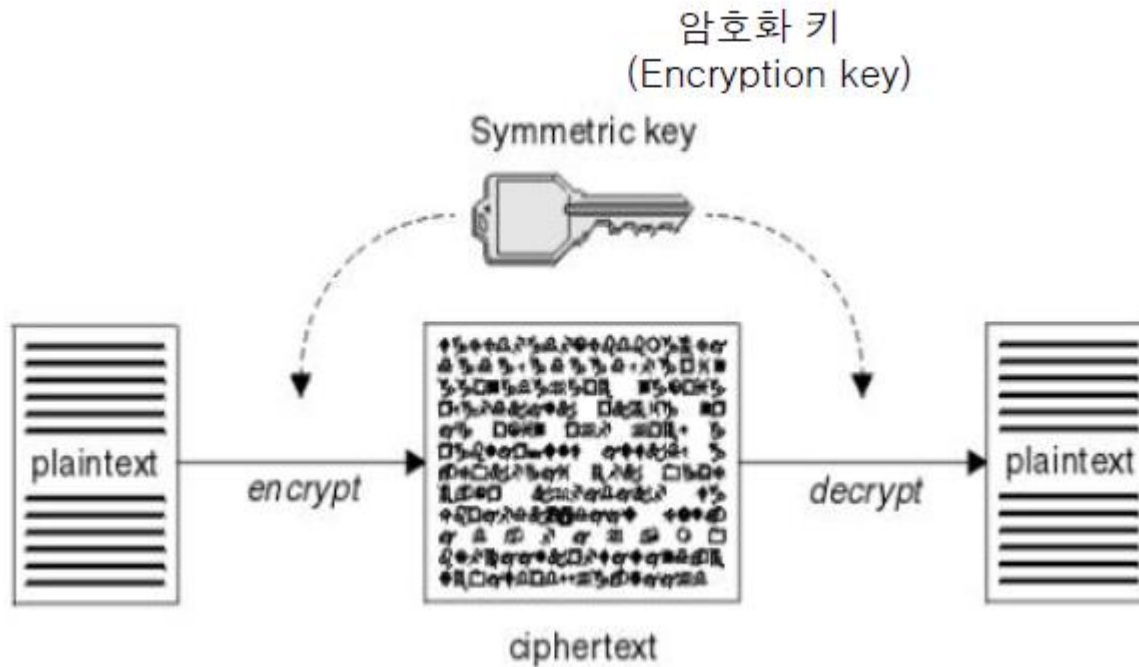
cryptographer
암호 사용자

- 정보의 의미를 숨기려고 암호를 사용하는 사람

암호의 용어

👤 암호화 과정

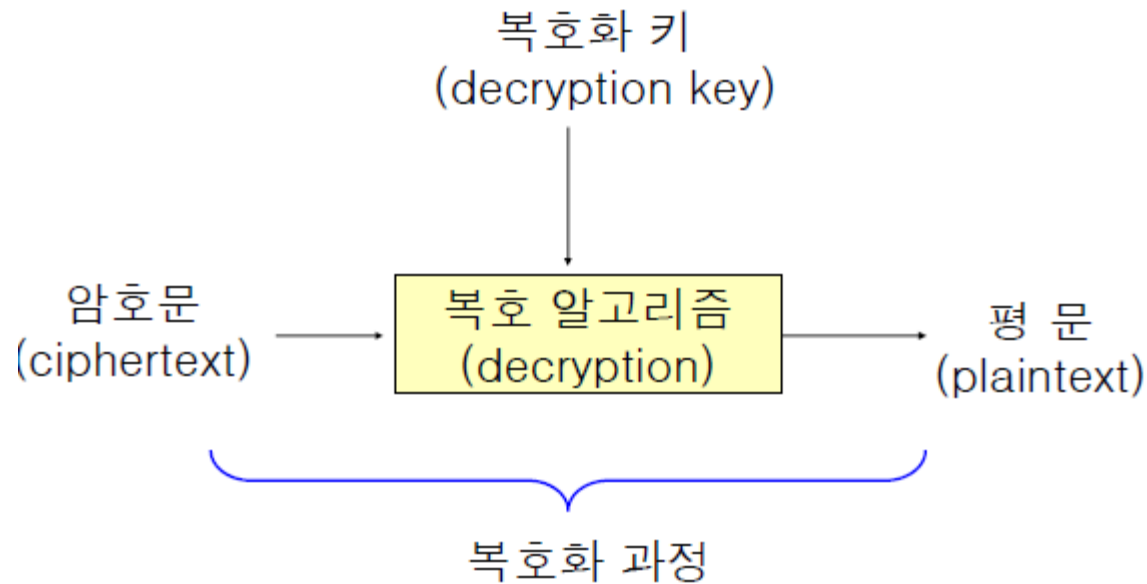
- $E_k(M) = C$, $E_k(P) = C$



암호의 용어

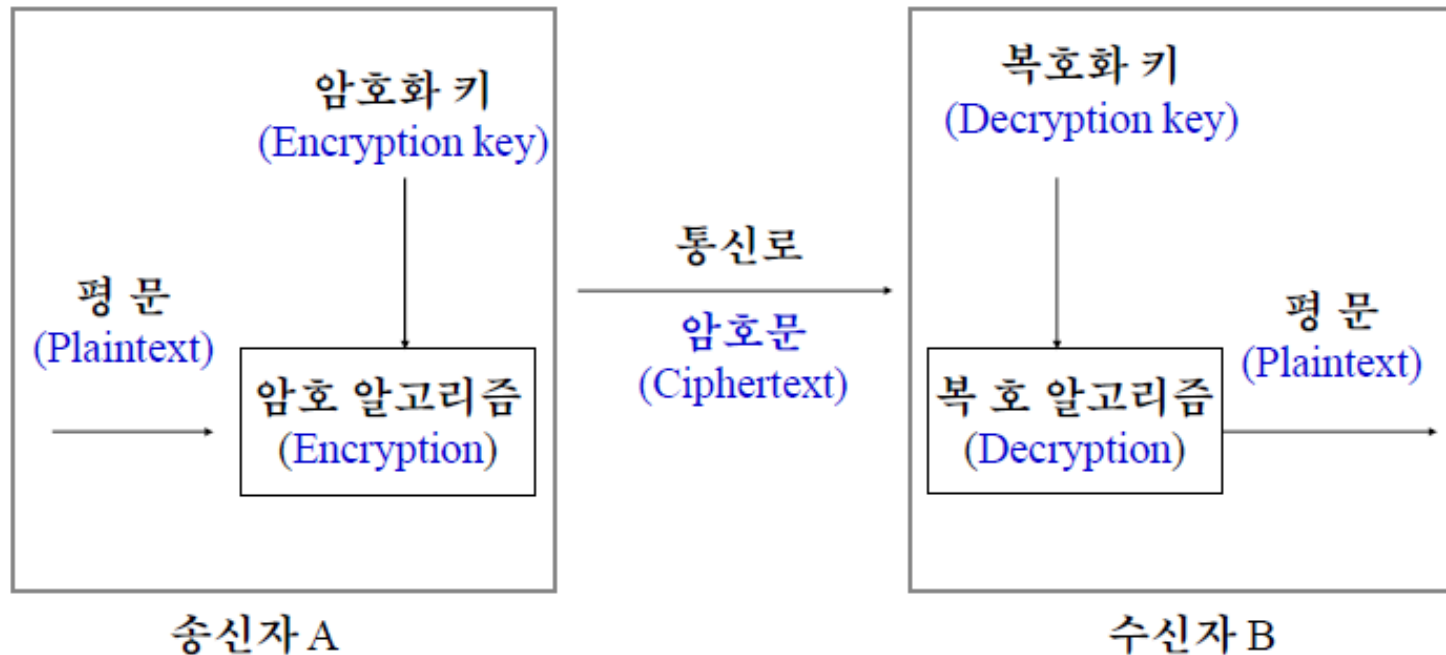
👤 복호화 과정

- $D_k(C) = M$



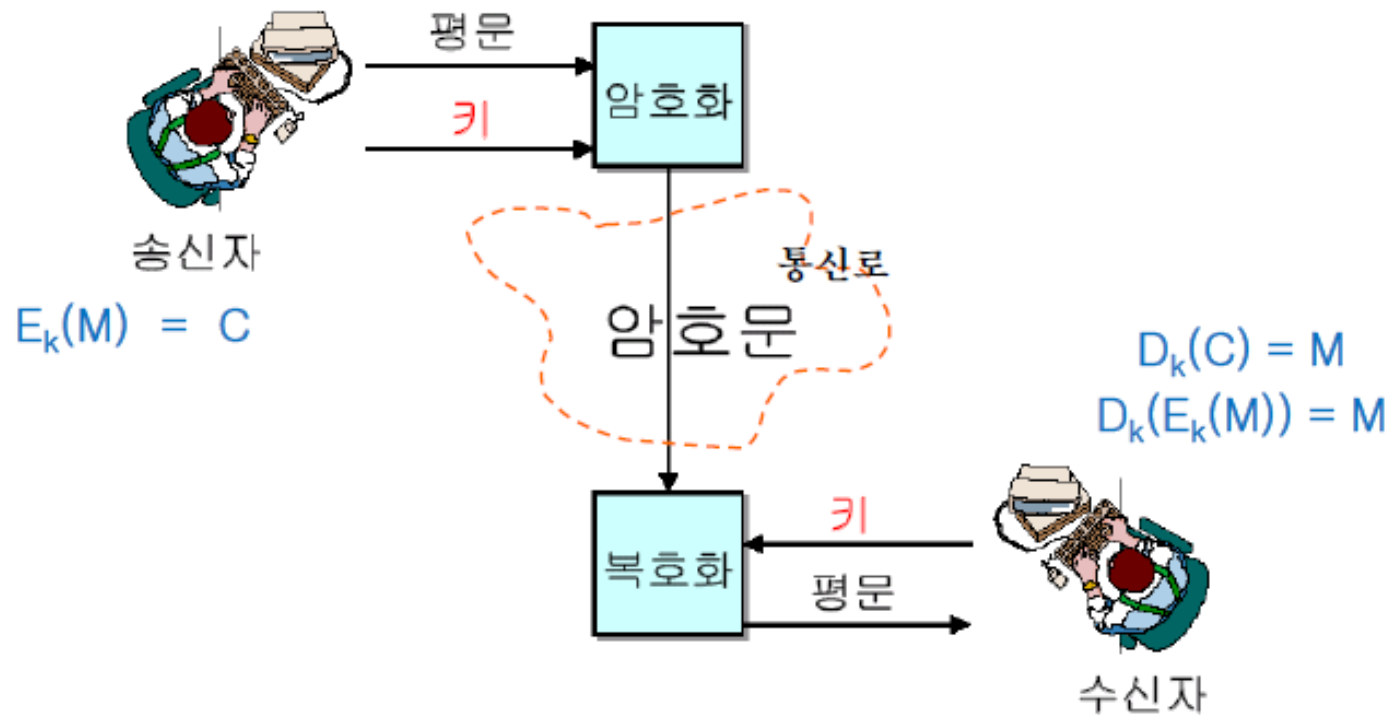
암호의 용어

👤 암호화와 복호화의 전체 과정



암호의 용어

암호화와 복호화의 전체 과정



암호의 용어

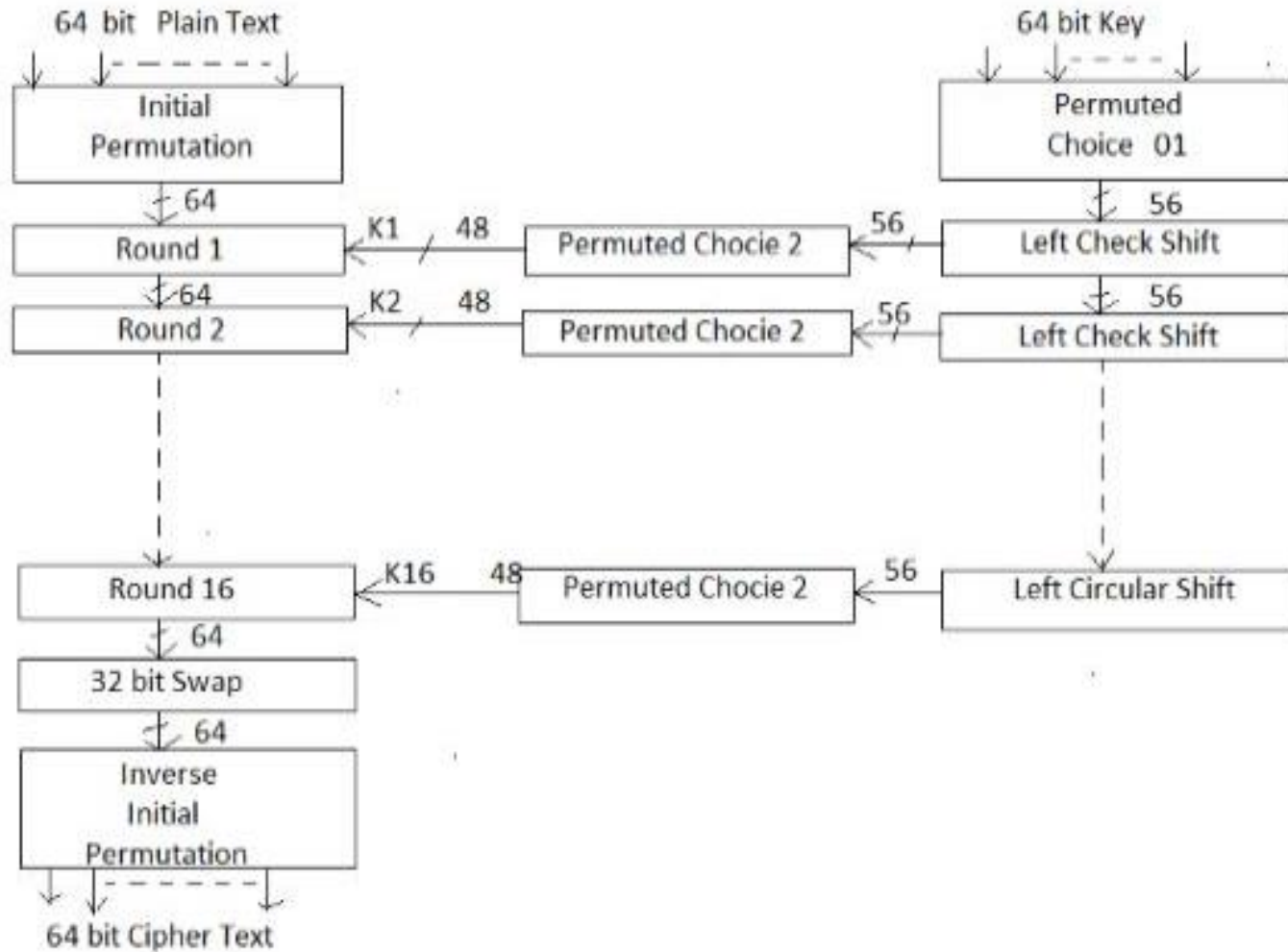
DES 알고리즘의 예

- 키(key) : 5e d9 20 4f ec e0 b9 67
- 평문(plaintext) :
“The unknown message is : The DES-test contest’s plaintext”
- 암호문(ciphertext) :

```
3e a7 86 f9 1d 76 bb d3 66 c6 3f 54 eb 3f e3 3f
39 88 81 4c 8b a1 97 f7 be 1b dd 7e fb 39 96 31
3c 3d 3b 65 c8 b8 3e 31 89 f9 04 14 fb cd c3 70
c1 11 a5 2f 3a ef 80 f4 cf f5 43 a4 b1 65 5b ae
```


DES

DES의 동작 원리



암호의 용어

👤 비밀키(Secret Key)

- 키의 소유자만 비밀스럽게 간직하는 키

👤 개인키(Private Key)

- 공개키 암호 방식에서 사용하는 비밀키에 해당하는 키

👤 공개키(Public Key)

- 모든 사람들에게 공개되는 키

👤 서명(Signature)

- 디지털 서명(digital signature)
- 인감 도장과 같은 역할


👤 인증서(Certificate)



암호의 용어

Exclusive-OR(XOR)

XOR	A	B
0	0	0
1	0	1
1	1	0
0	1	1

 암호문 : 평문 + 암호 알고리즘 + 암호(화) 키

 복호문 : 암호문 + 암호 알고리즘 + 복호(화) 키

암호의 발전 과정

구분	1세대 (고전암호)	2세대	3세대 (현대암호)
시대	고대 ~19세기후반	20세기초 ~1940년대후반	1940년대 말 ~현재
알고리즘	<ul style="list-style-type: none"> - 시저암호 - 비게네르 암호 - 뷰포트 암호 	<ul style="list-style-type: none"> - ENIGMA - Schlüsselzusatz - M-209 	<ul style="list-style-type: none"> - 암호 알고리즘 - 암호 프로토콜
특징	암호화 과정이 단순히 문자를 대입 또는 대치하는 방법	Roter Machine 과 같은 복잡한 기계를 사용하여 암호화	Shannon의 정보이론을 시작으로 복잡도가 높은 암호 알고리즘 사용

암호의 발전 과정

👤 신성문자를 암호로 사용

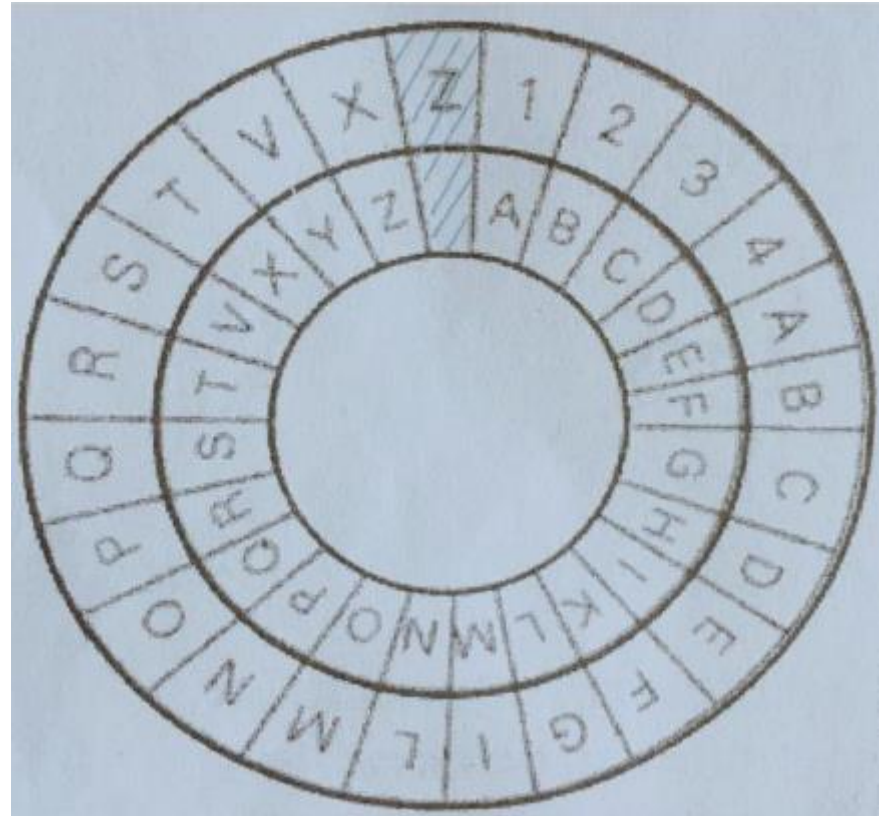
- 문신, 스키탈레(scytale, 스키테일), 시저(caesar), 중국인의 잉여(나머지) 정리
- 스키테일(scytale)
 - BC 400년 스파르타에서 군사용으로 사용한 암호화 방식
 - 나무의 굽기가 키가 된다



암호의 발전 과정

알베르티 암호원판

- 초기화
 - 빗금친 부분
- 키 : Z
- 평문 :
 - 'mathematics'
- 암호문 :
 - 'I1RDAI1RE3Q'



암호의 발전 과정

비지네르(Vigenere)

- 최초의 근대 암호(16세기 프랑스 외교관)
- 복잡한 표(26x26)를 미리 암호를 조합하거나 품.
- 다중 치환의 대표적인 예
- 예) 암호 키: HOME 평문: enemy
암호문 : lbqqf

-복호화 : 암호 키를 가로축
에서 먼저 찾고 다음으로
세로축에서 평문을 찾는다.

통신문글자 →		...	E	F	G	H	I	J	K	L	M	N	O	...	Y
암호문 ↓	E	...	i	j	k	l	m	n	o	p	q	r	s	...	c
	F	...	j	k	l	m	n	o	p	q	r	s	t	...	d
	G	...	k	l	m	n	o	p	q	r	s	t	u	...	e
	H	...	l	m	n	o	p	q	r	s	t	u	v	...	f

	M	...	q	r	s	t	u	v	w	x	y	z	a	...	k
	N	...	r	s	t	u	v	w	x	y	z	a	b	...	l
	O	...	s	t	u	v	w	x	y	z	a	b	c	...	m

암호의 발전 과정

- 👤 제퍼슨(wheel cipher), 바제리
- 👤 Vernam(one-time pad), enigma, M-209 암호기
- 👤 DES, RSA, 양자 암호

기념상품



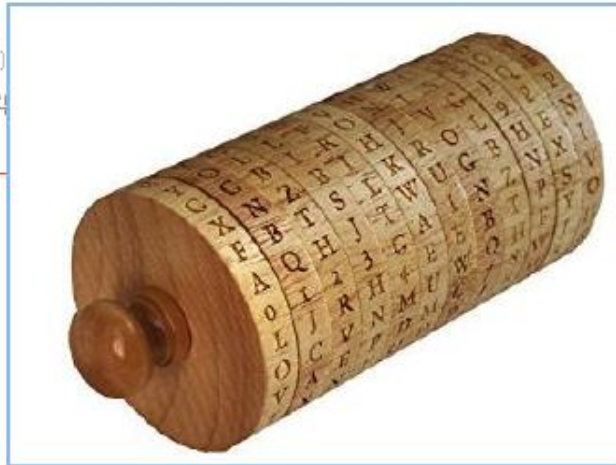
Secret Cipher Decoder Wheel - Jefferson Wheel

53,440원 구매하기 AUCTION.

무도버승 등록일: 2018.03

★★★★★ 5 (상품평 0)

완구/교육/교구 > 퍼즐/감각

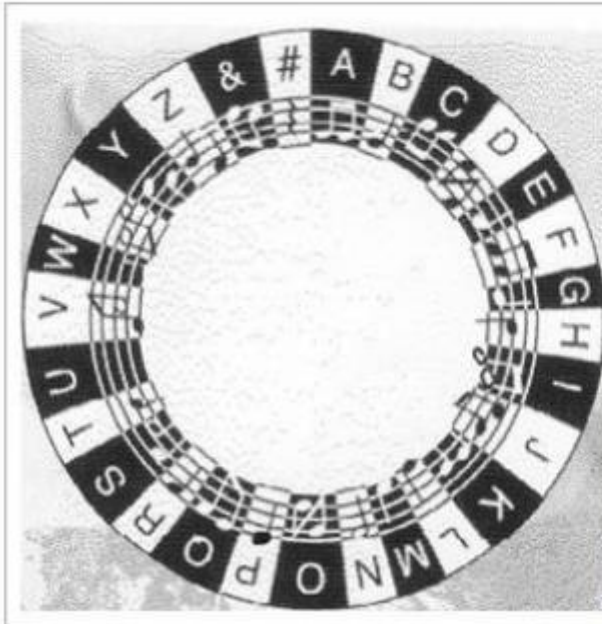


[M-209]

암호의 발전 과정

악보암호 해독표

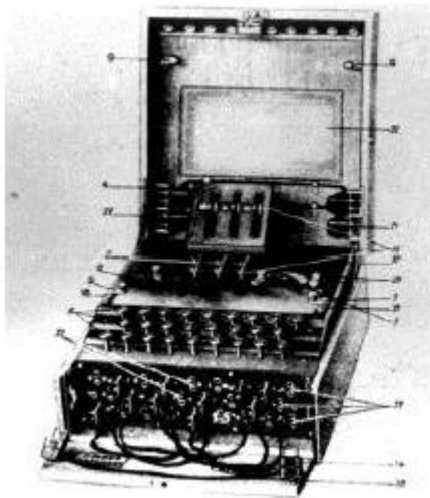
- 제1차 세계대전 당시 독일과 프랑스를 오가며 이중간첩 활동



암호의 발전 과정

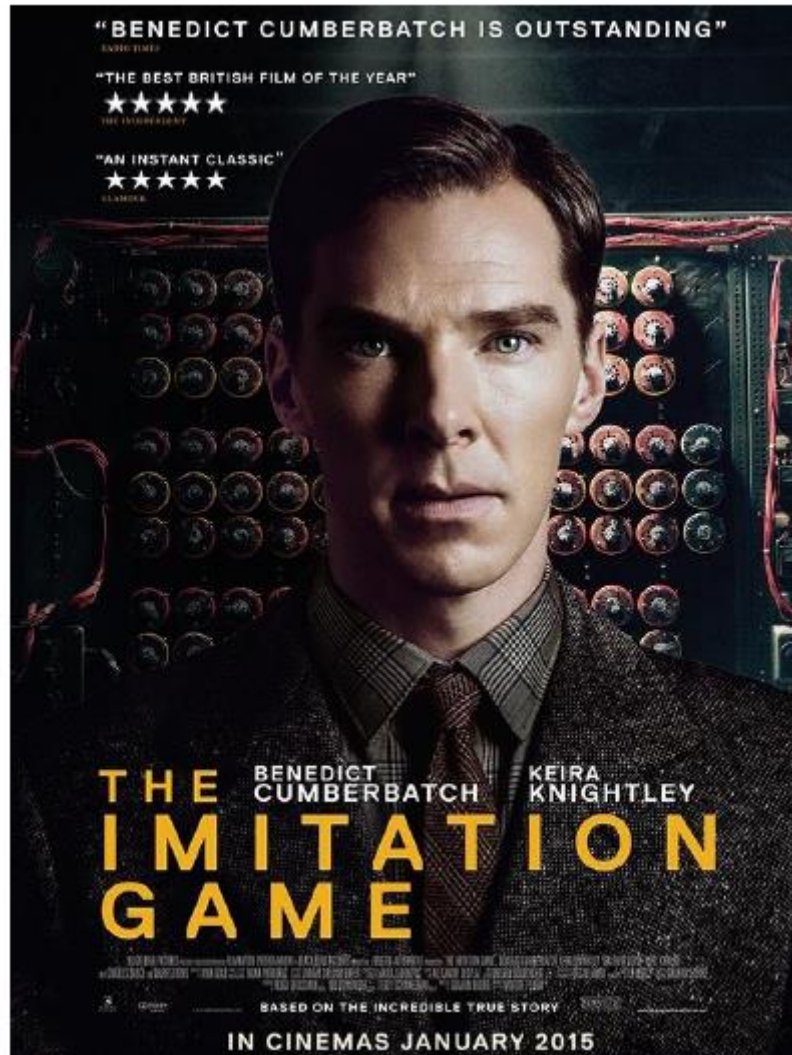
👤 Enigma

- 암호의 작성과 해독을 할 수 있는 암호 기계
- 다중 치환의 발전된 형태인 플레이페어(playfair) 암호의 종류
- 1918년 아르투르 슈르비우스(Arthur Schrbius)가 처음 고안
 - 여러 회사와 국가에 의해 사용
- ‘악마의 기계’
- 제2차 세계대전, 독일이 군 정보를 암호화하는데 사용



암호의 발전 과정

🧑 Enigma



암호의 발전 과정

👤 Enigma

- 알란 튜링(Alan Turing)
 - 컴퓨터의 아버지
- 현대 컴퓨터의 이론적 모델을 최초로 고안 – ‘튜링 머신’
 - 세계 최초의 해커



암호의 발전 과정

👤 M-209 암호기

- 미국
- Roter machine
 - 회전하는 부분을 가진 기계
- Rotor
 - 발전기, 전동기 등의 회전하는 부분을 통틀어 지칭



[M-209]

암호의 기법

암호 시스템 3가지 영역

1. 평문을 암호화하기 위한 연산자의 유형

- 치환(Substitution) : 평문의 각 원소를 다른 원소로 사상
- 전치(Transposition) : 평문의 각 원소를 재배열

2. 사용된 키의 수

- 관용키 : 송·수신자가 같은 키를 사용
 - single-key, symmetric key(대칭키), secret-key(비밀키)
- 공개키 : 송·수신자가 다른 키를 사용
 - two-key, asymmetric key (비대칭키), public-key

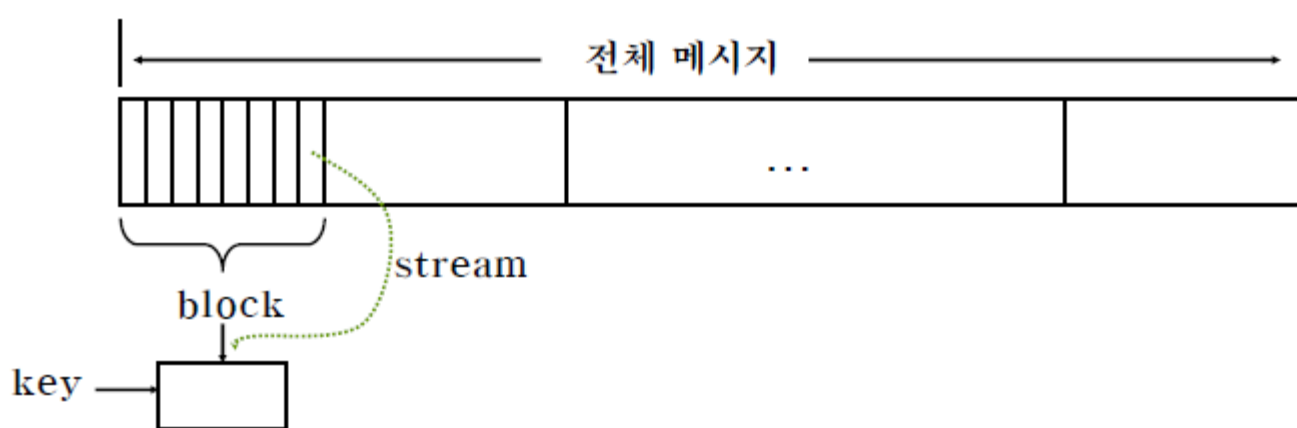
3. 평문 처리 방법

- 스트림 암호화(Stream cipher)
 - 입력을 연속적(비트 단위)로 처리
 - 주로 인터넷 및 이동통신환경에서 무선 데이터 암호에 사용
 - 키 스트림과 XOR 연산
- 블록 암호화(Block cipher)
 - 연산을 블록 단위로 처리

암호의 기법

3. 평문 처리 방법

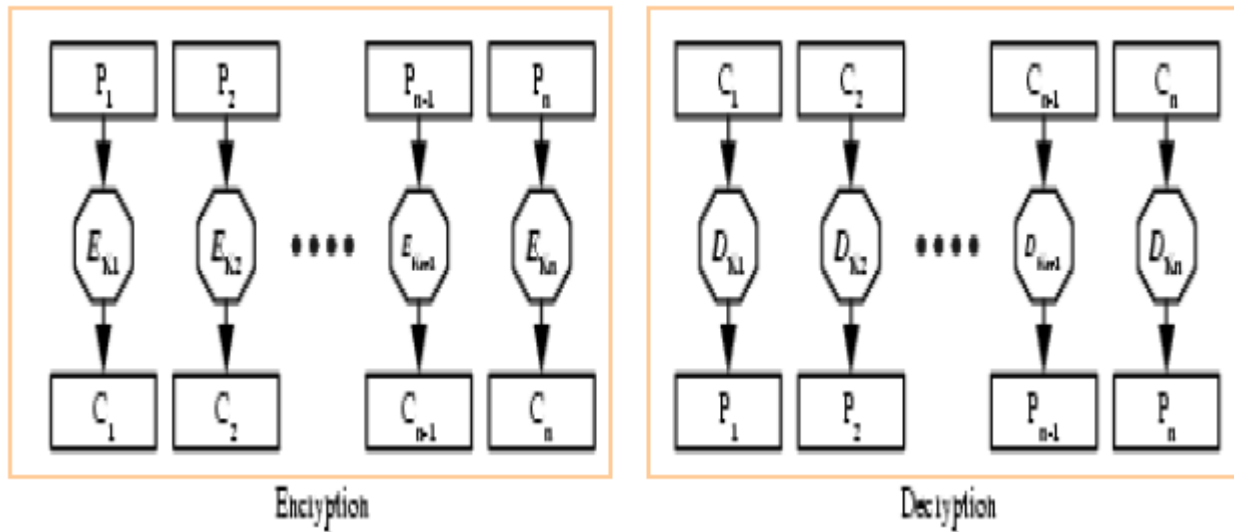
- 스트림 암호화(Stream cipher)
 - 1 bit, 1byte
 - 예) LFSR, one time-pad
- 블록 암호화(Block cipher)
 - 연산을 블록 단위로 처리
 - 예) DES, IDEA, SEED, RC5, AES



암호의 기법

👤 평문(P)의 크기

- 1 : stream cipher
- 1이상이면 : block cipher



암호의 기법

일반화

■ 암호화

- $C = E(P) = (P + k) \bmod (26)$

■ 복호화

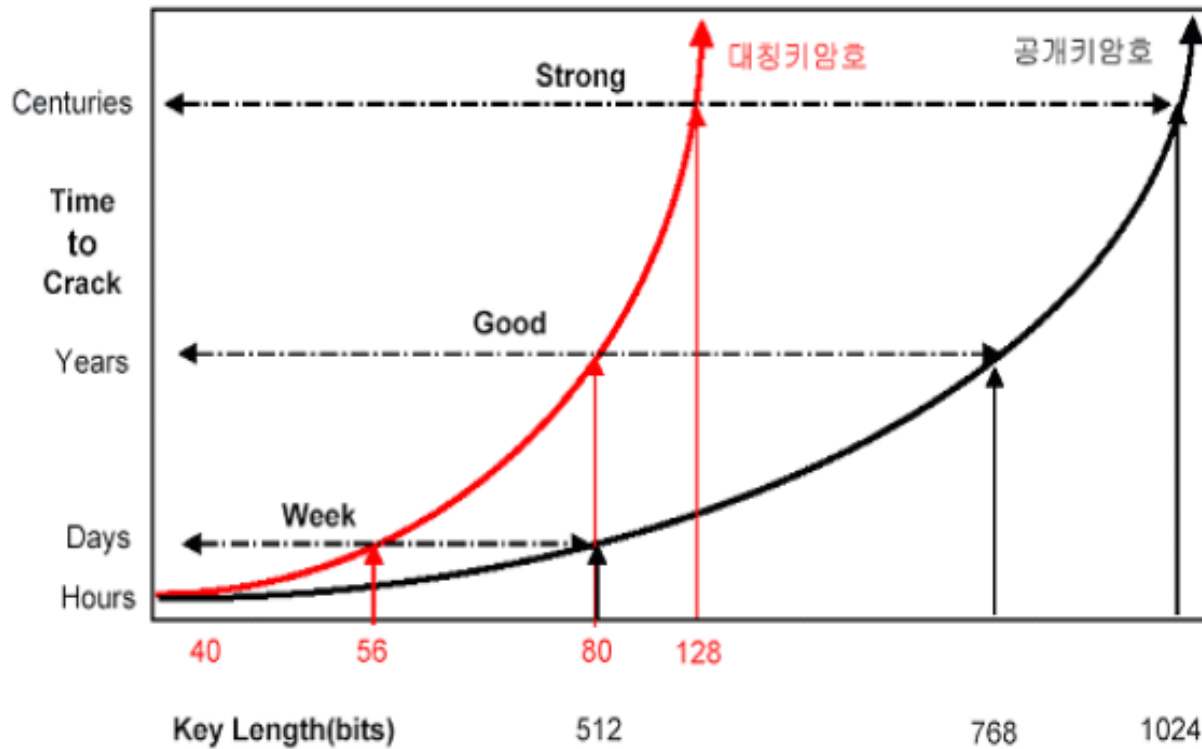
- $P = D(C) = (C - k) \bmod (26)$

■ 단점

- 암호화 및 해독 알고리즘이 단순

Key size	가능한 키 수	Crack Time
40 bits	1×10^{12}	2시간
56 bits	7×10^{16}	20시간
64 bits	2×10^{19}	9년
128 bits	3×10^{28}	10^{19} 년(2조년)

암호의 기법



암호의 기법

단점

- 단순 대치이므로 문자 출현 빈도수에 의한 복호가 용이
- 한 키가 25개 뿐이다.
 - Brute-force attack(전수키 조사/전수 공격)이 가능
 - 가능한 모든 경우의 수를 시도
- 추정 단어 공격(Probable-Word Attack)
- 사전 공격(Dictionary attack)

- 평문의 언어를 알고 있으며 쉽게 인식할 수 있다.
 - 평문 유형을 알 수 없도록 암호화 이전에 압축하여 인식을 어렵게 변환

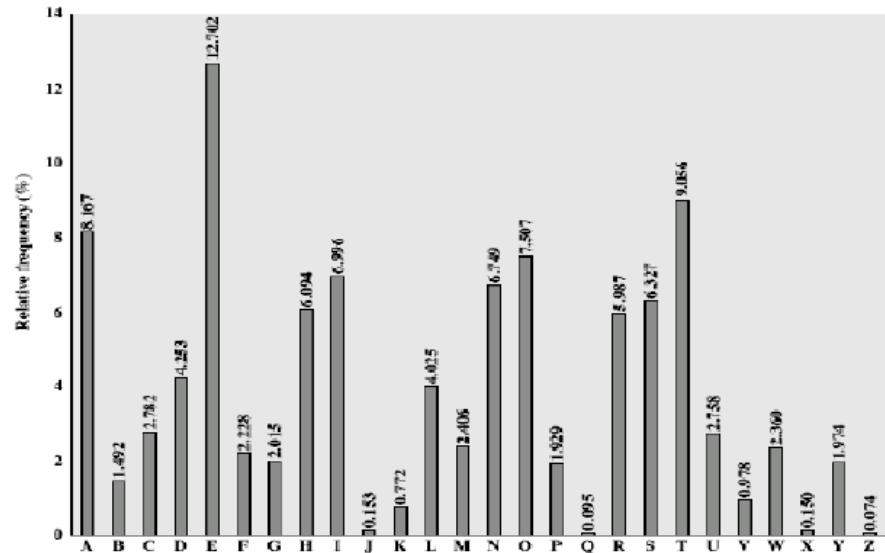
암호의 기법

알파벳의 통계 특성

- 평문의 통계적 분포와 암호문의 통계적 분포는 일치
- 영문자의 통계 분포 예

글자	빈도	글자	빈도	글자	빈도	글자	빈도
e	12.31%	t	9.59%	a	8.05%	o	7.94%
n	7.19%	i	7.18%	s	6.59%	r	6.03%
h	5.14%	l	4.03%	d	3.65%	c	3.20%
u	3.10%	p	2.29%	f	2.28%	m	2.25%
w	2.03%	y	1.88%	b	1.62%	g	1.61%
v	0.93%	k	0.52%	q	0.20%	x	0.20%
j	0.10%	z	0.09%				

알파벳의 통계 특성



영문자의 출현 빈도

암호의 기법

암호 해독(Cryptanalysis)

- 평문이나 키 또는 이 두 가지를 모두 발견하려는 시도 과정

전사적 공격(Brute-Force Attack)

- 추정 단어 공격(Probable-Word Attack)

안전성

- 무조건 절대 안전성
 - 비용과 시간이 충분하여도 복호하기가 불가능
- 계산상 안전성
 - 해독 비용이 복호된 정보의 가치를 초과
 - 해독 시간이 정보의 유효한 수명 주기를 초과

암호의 기법

👤 대체, 대치(substitution)

- 평문의 문자를 문자, 숫자, 기호로 대체시키는 방법
- 간단한 치환 암호 기법
- 예) 평문 : Come here at once

암호문: 

👤 단순 대치

- shift사용 Caesar 암호, 키워드, 키 문장을 사용한 단순 대치
- $X = Y + Z \pmod{26}$

👤 다중 대치(다중 치환)

- 비지네르(Vigenere), 키 수열 사용
- $X = Y + Z_i \pmod{26}$, $Z=3, 7, 4, 2, 5$

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

비지네르 표

암호의 기법

👤 대체, 대치(substitution)

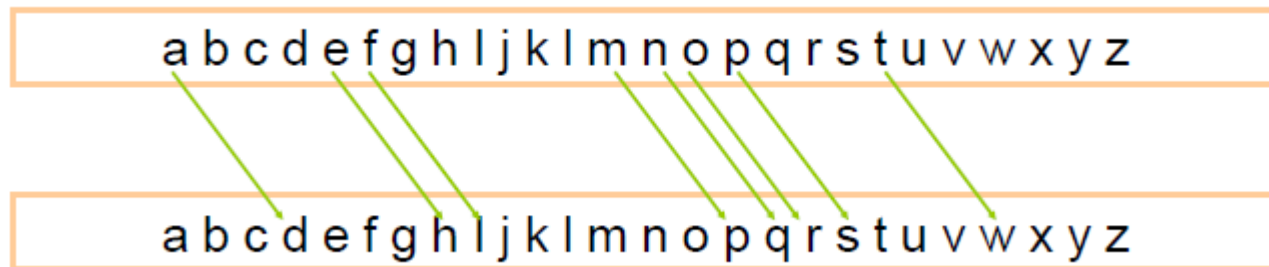
■ 줄리어스 시저가 개발

- Caesar Cipher, 시저 암호
- 원래 써야 할 알파벳을 옆으로 3칸 이동한 자리의 알파벳으로 대체하여 쓰는 방식

■ 예) Key : ?

평 문 : meet me after the toga party

암호문 : PHHW PH DIWHU WKH WRJD SDUWB



암호의 기법

암호화

- 문자 P를 암호화
- $C = Ek(P) = (P + 3) \bmod 26$
- $P = Dk(C) = (C - 3) \bmod 26$

a b c d e f g h i j k l m n o p q r s t u v w x y z

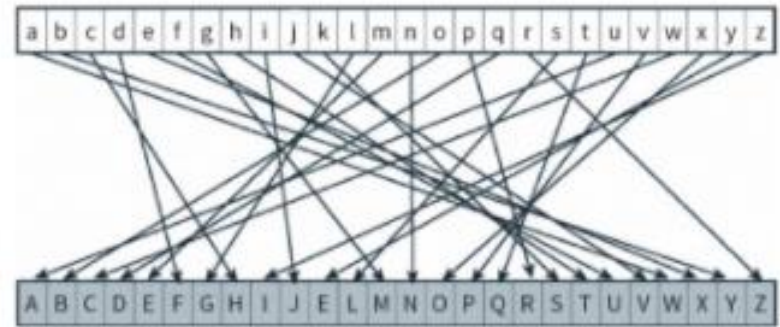
a b c d e f g h i j k l m n o p q r s t u v w x y z

암호의 기법

단일 치환 암호

■ 모노 알파벳 암호(Mono-alphabetic)

- 시저 암호와 마찬가지로 단일 치환 암호 방식이지만 알고리즘의 개선을 통해 보안성을 강화시킨 알고리즘
- 암호화 : 알파벳 26 글자를 각각 다른 알파벳에 대응시키는 방식
- 전사 공격에 다소 강하나, 빈도 분석법에는 쉽게 해독됨
 - 모든 경우의 수 : 26!



- Shift cipher
 - Shift 3

평문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	Z
숫자	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	25
암호문	D	E	F	G	H	I	J	K	L	M	N	O	P	Q				C

- $C = (M + K) \bmod 26 = (M + 3) \bmod 26$
- 예) Key = 9, M = ENCRYPTIONISIMPORTANT

암호의 기법

👤 Affine 암호

- $C = f(p) = (aP + b) \bmod N$
 - a, b : 임의의 정수 값
 - N : 알파벳 문자 총 개수(26)
- $f(p) = (3P + 8) \bmod 26$
- 평문 : FIRE AT NOON

평문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	Z
숫자	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	25

- 수치로 바꾼다
 - 5, 8, 17, 4, 0, 19, 13, 14, 14, 13

암호의 기법

■ 수치로 바꾼다

- 5, 8, 17, 4, 0, 19, 13, 14, 14, 13

■ 숫자 5와 8을 각 함수에 적용

- $f(5) = (3 \times 5 + 8) \bmod 26 = 23 \bmod 26 = 23$
- $f(8) = (3 \times 8 + 8) \bmod 26 = 32 \bmod 26 = 6$
- 결과 : 23, 6, 7, 20, 8, 13, 21, 24, 24, 21
- 문자 변환(암호화)
 - XGHU IN VYYV

평문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	X	Y	Z
숫자	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	23	24	25

암호의 기법

Affine 암호

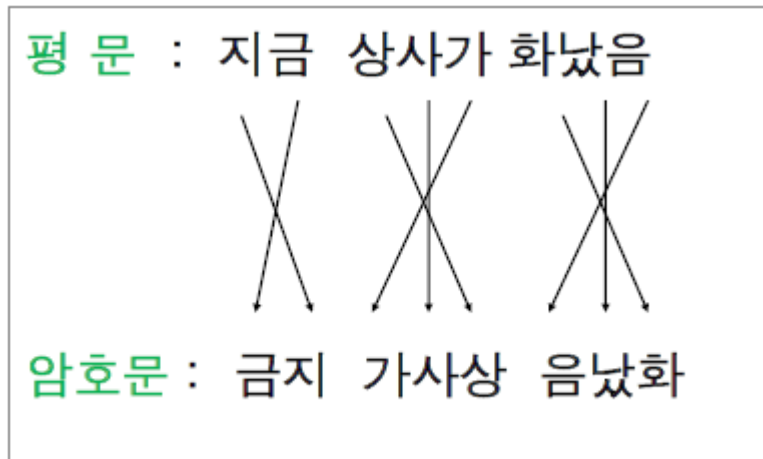
■ 혼자 놀기

- $f(P) = (3P + 2) \bmod 26$ 을 사용해서 메시지 DON'T FEED THE BEARS를 암호화하시오.

암호의 기법

👤 전치, 환치(permutation, transposition)

- 평문의 각 문자 위치만 바꾸어 암호화시킨다
- 평문을 고정된 길이의 블록으로 나눈 후 각 블록 내에 있는 문자들을 일정한 규칙에 의해 재배치
- 예)



암호의 기법

- 예) 한 문자 좌측으로 한 칸씩 이동시켜 암호화하면
 - 평문 : “FIVE AM”
 - 암호문 : “IVEA MF”
- 메시지가 행으로 작성되고 열로서 읽히는 방식
- 평문의 모든 문자를 재배치하여 생성된 암호문의 모든 문자들은 평문의 문자들과 동일함
- 평문에 있던 문자의 개수만큼 암호문이 만들어짐
- 단순 전치암호

암호의 기법

전치 암호화(Transposition)

- 키 단어 사용

- 예) CONVENIENCE

- 여기에 알파벳 순서로 각 문자에 번호 할당

- 알파벳 순서로 1부터 할당

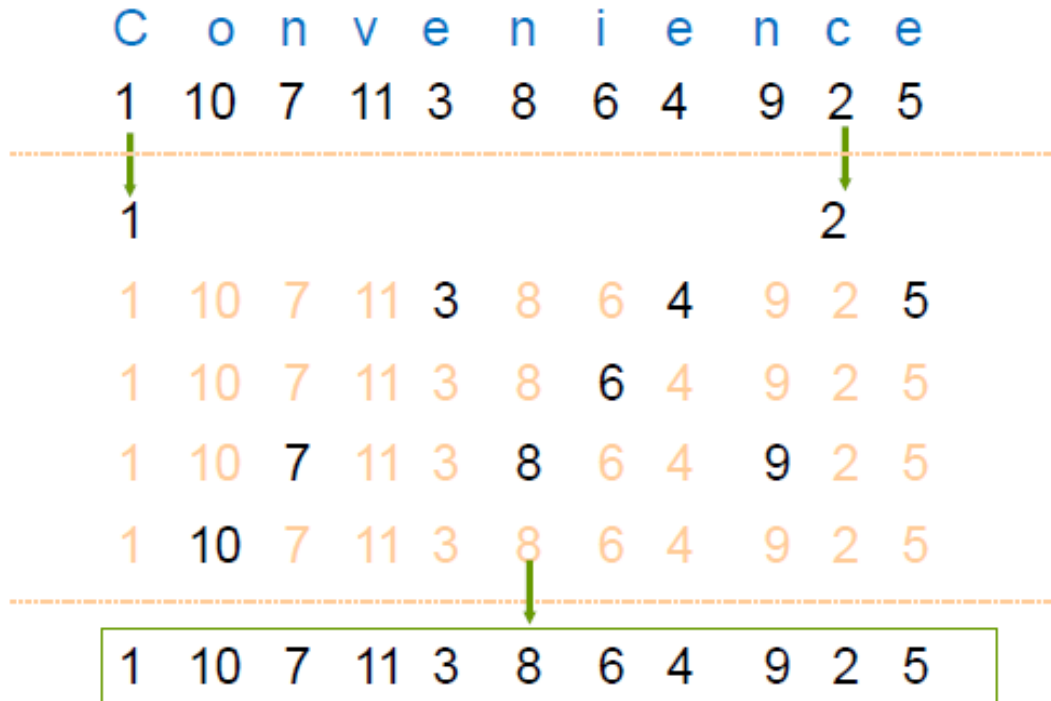
- 같은 문자 두 번 반복 시 앞 번호가 앞선다.

- 예) 평문 : HERE IS A SECRET MESSAGE ENCIPHERED BY
TRANSPOSITION

- KEY : CONVENIENCE

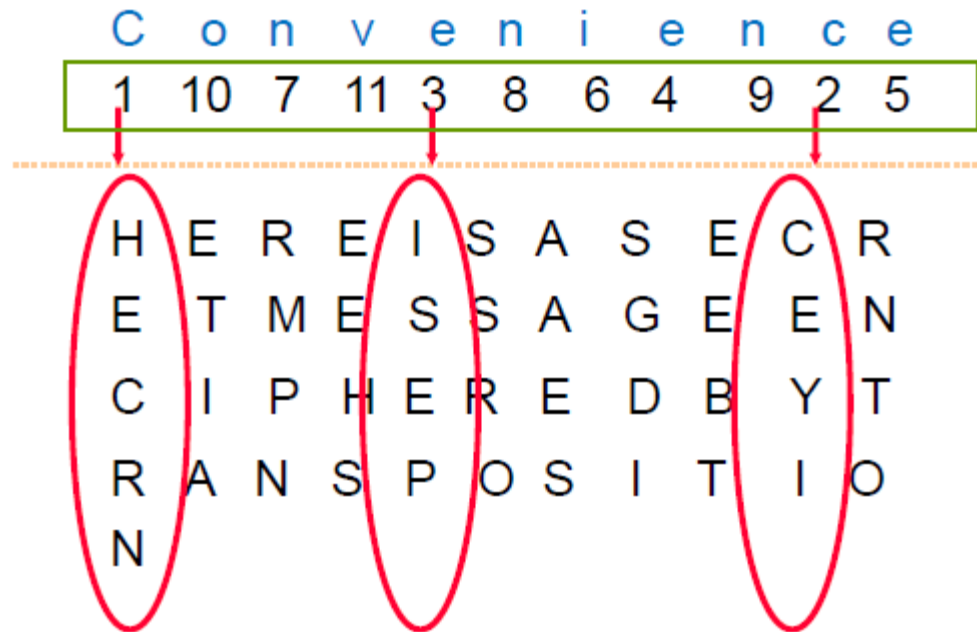
암호의 기법

- 예) 평문 : HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION
 - KEY : CONVENIENCE



암호의 기법

- 예) 평문 : HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION
 - KEY : CONVENIENCE



암호의 기법

치환과 전치 암호의 결합

- 암호문 해독을 더욱 복잡하게 하는 암호문 생성
- 더욱 안전한 암호 방법임
- DES 암호 알고리즘은 치환 암호와 전치 암호의 결합을 이용하는 암호 알고리즘

암호 분석에 대한 대응

- 암호문에 암호해독을 위한 어떠한 단서를 남겨두지 않아야 함
- 치환 암호와 전치 암호 방법을 같이 사용하여 암호문에 나타나는 평문의 특성을 숨긴다
- 그러나, 완전하게 언어적인 특성을 숨기는 것은 어렵다
- 영어 단어(문장)에 나타나는 알파벳 또는 단어의 통계적 패턴을 이용하여 컴퓨터를 통한 효과적인 분석방법이 존재

암호의 기법

Shannon의 암호 이론

■ Confusion(혼돈)

- 평문과 암호문 사이의 상관 관계를 숨김
- 예) s-box

■ Diffusion(확산)

- 평문의 통계적 특성을 암호문 전반에 퍼트림
- 평문의 각각의 비트가 암호문의 많은 비트들에 영향을 줌으로써 평문과 암호문 사이의 관계를 복잡하게 하는 것
- 즉, 개개의 평문 문자들의 영향을 가능한 암호문의 많은 부분에 퍼뜨리는 것
- Polybius 암호 방법을 응용함
- 대체 암호문(Substitution)은 Diffusion이 나쁨
- 전치 암호문(Transposition)은 Diffusion이 좋음
- 예) p-box

암호의 기법

Polybius(폴리비우스) 암호

- 고대 그리스의 역사가
- 문자를 숫자(행X열)로 바꾸는 암호화 방법
- 암호화하고자 하는 알파벳을 표에서 찾아서 (행,열)의 순서로 숫자를 써넣는다.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

■ 예)

- 본문에 A가 있으면 표 안의 A가 1행 1열 -> A=11
- 본문에 B가 있으면 표 안의 B가 1행 2열 -> B=12
- HOLMES = 23 34 31 32 15 43
= 233431321543

암호의 기법

	1	2	3	4	5
1	S	H	E	R	L
2	O	C	K	A	B
3	D	F	G	I/J	M
4	N	P	Q	T	U
5	V	W	X	Y	Z

👤 암호를 더 복잡하고 싶을 경우

■ 키워드 활용

■ 예)

1. 자신이 원하는 키워드를 하나 설정한 다음 5행 5열의 표 안에 키워드의 알파벳을 차례대로 써넣는다.
2. 그 다음 키워드에 들어가지 않은 알파벳을 차례대로 써넣는다.
3. 그렇게 완성된 표를 토대로 암호문을 작성한다.
4. 만약 키워드의 알파벳들 중에 중복되는 것이 있다면 2번째로 나오는 것은 쓰지 않는다.
 - 예) 키워드가 MOMENT라면 표 안에 써넣을 때에는 뒤에 중복되는 M을 생략하고 MOENT만 써넣는다.

암호의 기법

■ 예) 키워드 : SHERLOCK 사용

■ 키워드 “SHERLOCK”의
알파벳을 표 안에 차례대로
써넣은 다음 나머지 알파벳을
써넣으면 옆의 그림과 같다.

	1	2	3	4	5
1	S	H	E	R	L
2	O	C	K	A	B
3	D	F	G	I/J	M
4	N	P	Q	T	U
5	V	W	X	Y	Z

■ 이 표를 토대로 HOLMES를 암호화하면?

• HOLMES = 12 21 15 35 13 11
= 122115351311

암호의 기법

■ 혼돈(Confusion)

- 암호분석가는 암호문과 암호 방법을 이용하여 평문을 찾으려 한다.
- 암호화 과정이 공격자에 의해서 이용되지 못하도록 키와 암호문 사이의 관계를 가능한 복잡하게 하는 것
- 암호문의 통계가 평문의 통계에 좌우되지 못하도록 하는 것 (one-time pad)
- Caesar, Vigenere 암호는 비밀키를 알아내는 것을 막기엔 강력하지 못함
- 복잡한 치환 암호방법으로 혼돈 성질을 제공함
 - DES는 Confusion, Diffusion 원리 기반
- 키의 길이가 메시지 길이를 초과하는 Polyalphabetic 대체는 좋음

암호의 기법

👤 적(Product) 암호

- 대체(substitution) 암호와 전치(transposition) 암호가 합쳐진 암호
- 예) Jefferson's Wheel Cipher

- 알고리즘의 종류

- RC2
- IDEA
- Blowfish
- DES
- 3DES
- AES(Advanced Encryption Standard)



비밀키 암호 시스템