제 2 장
고전 암호 기법

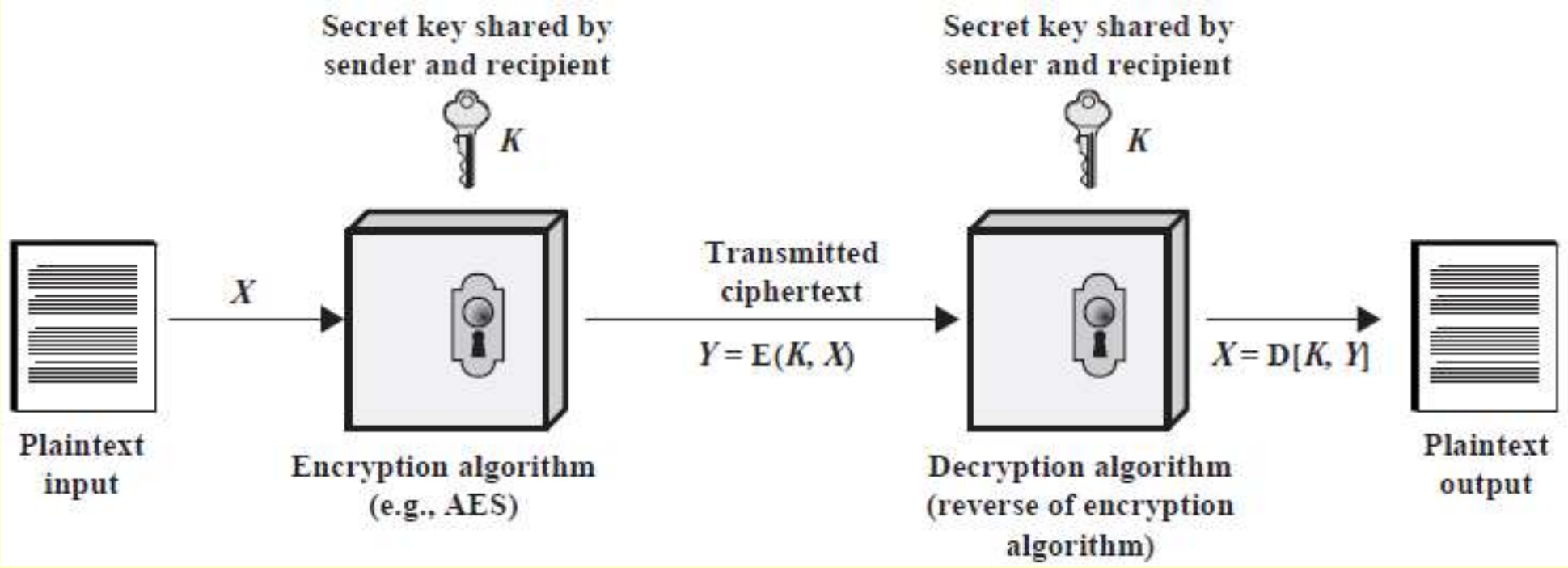
❑ 목 차

- ❖대칭 암호 모델
- ❖치환 기법
- ❖전치 기법
- ❖회전자 기계
- ❖Steganography

암호 모델

- 平文(평문 Plaintext): 이해하기 쉬운 일반 메시지
- 暗號文(암호문 Ciphertext): 이해할 수 없도록 변형된 메시지
- 암호화 과정: 특정한 방식의 **알고리즘**에 비밀 유지되는 **키**를 적용하여 알기 쉬운 **평문을 알 수 없는 암호문으로 변환**
  - 동일한 메시지도 키에 따라서 알고리즘의 변환 결과가 다르게 출현
- 암호 방식의 구성 요소
  - **평문(Plaintext)**
  - **암호 알고리즘(Encryption algorithm)**
  - **비밀 키(Secret key)**
  - **암호문(Ciphertext)**
  - **복호 알고리즘(Decryption algorithm)**

암호 모델



대칭 암호 방식에 대한 단순화된 모델

❑ 암호방식

❖관용 암호 방식(Conventional Cryptosystem)

- ➢대칭키 암호 방식(Symmetric Cryptosystem)
- ➢비밀키 암호 방식(Secret-Key Cryptosystem)

❖현대 암호 방식(Modern Cryptosystem)

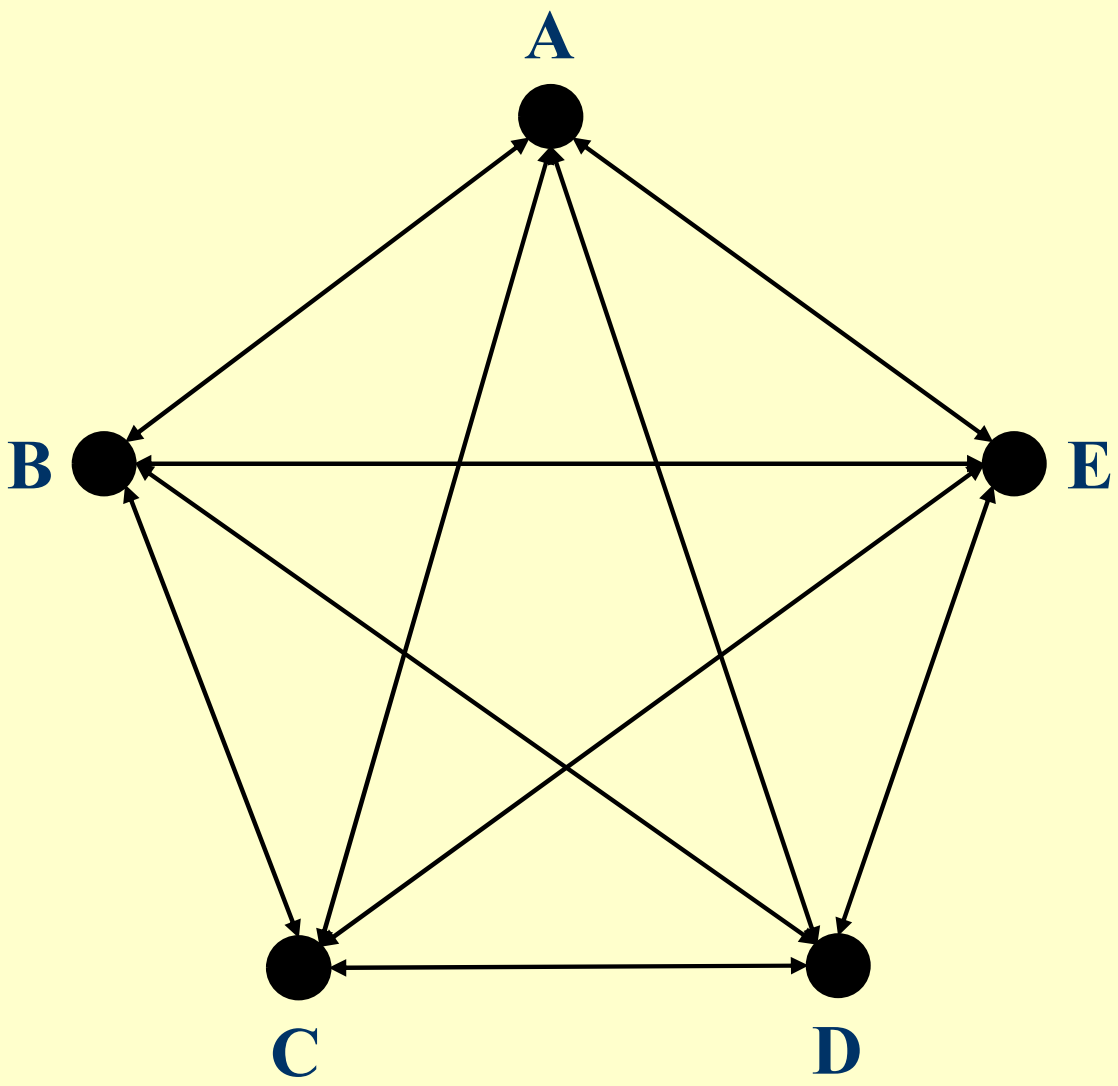
- ➢비대칭키 암호 방식(Asymmetric Cryptosystem)
- ➢공개키 암호 방식(Public-Key Cryptosystem)

관용암호(慣用暗號)

❑ 관용암호방식의 安全性(안전성) 특징

- ❖ 암호 알고리즘은 키 없이 암호문 자체만으로 해독 불가하도록 강도 유지
- ❖ 암호문과 암복호알고리즘이 알려져도 메시지의 해독은 불가하다고 가정
- ❖ 안전성은 알고리즘 자체의 비밀성이 아니라 키의 비밀성에 의존
  - ➢ 5명의 참가자인 경우 키의 가지수는???
- ❖ 암호 알고리즘을 비밀유지 할 필요가 없으므로 저가의 칩으로 개발 유용

- ❖ 장점
  - ➢ DES, RC5, SKIPJACK, IDEA, SEAL, RC4, SEED, AES 등 다양한 알고리즘 개발
  - ➢ 알고리즘 수행속도 빠르다
- ❖ 단점
  - ➢ 키관리 및 키 분배와 디지털 서명의 어려움


A
B
E
C
D

대칭키 암호 방식 모델

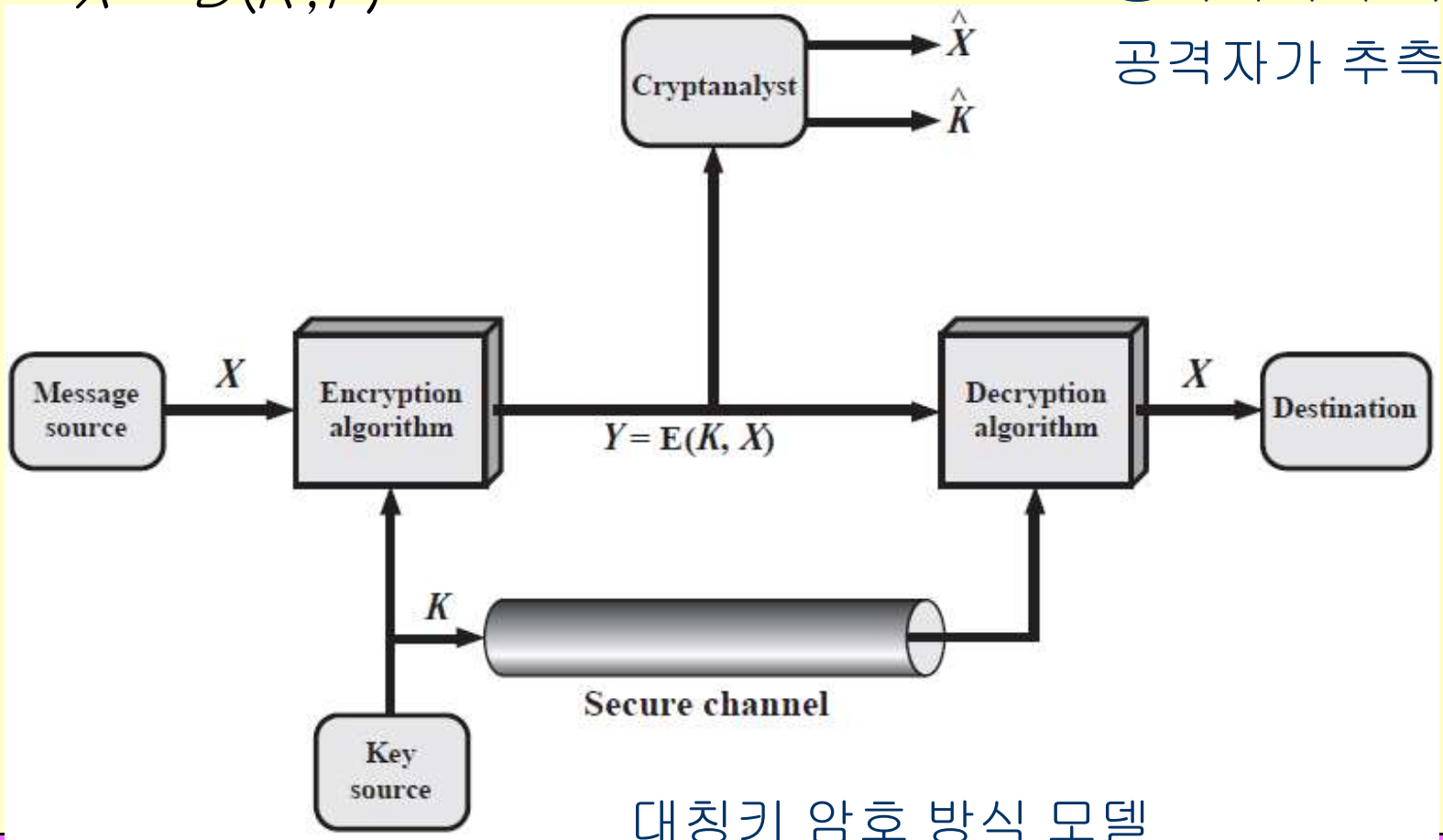
❖**암호문 *Y*, 메시지(평문) *X*, 암호 키 *K*일때:**

$Y = E(K, X)$

$X = D(K, Y)$

공격자가 추측한 평문

공격자가 추측한 암호 키



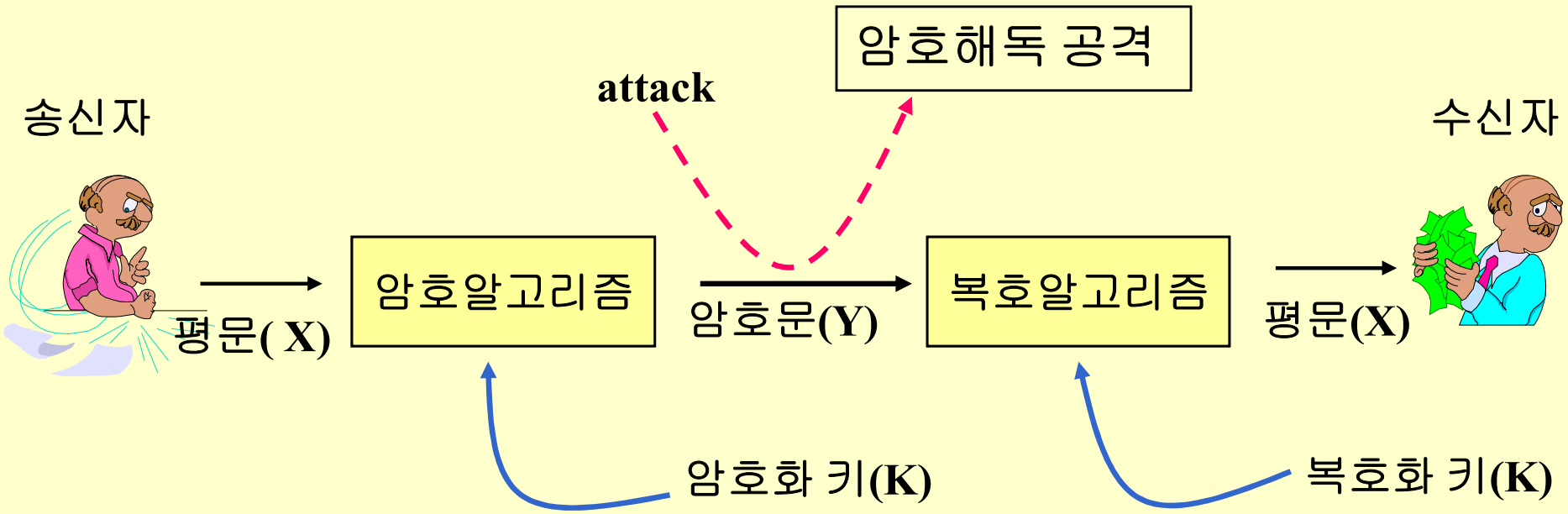
대칭키 암호 방식 모델

관용암호 시스템의 모델

- 평문 메시지: $X = [X_1, X_2, \ldots, X_m]$
- 암복호화 키: $K = [K_1, K_2, \ldots, K_j]$
- 암호문: $Y = [Y_1, Y_2, \ldots, Y_m]$
- 암호화: $Y = E_K(X) = E(K,X)$
- 복호화: $X = D_K(Y) = D(K,Y)$

❖공격자는 암호문에 대응하는 평문을 알기 위하여 예측 평문을 생성하거나 키를 찾아내어 복호를 시도

관용암호 시스템의 모델


암호해독 공격
attack
송신자
수신자
암호알고리즘
복호알고리즘
평문(X)
암호문(Y)
평문(X)
암호화 키(K)
복호화 키(K)

암호학(cryptology)

◆ 암호학 : 암호화/복호화하기 위한 원리, 수단, 방법 등을 취급하는 기술이나 과학의 학문

❖ 암호(cryptography) : 통신 당사자들끼리만 아는 비밀스런 신호나 부호 ; hidden word의 의미

❖ 암호 해독(Cryptanalysis) : 평문이나 키 또는 이 두 가지를 모두 발견하려는 시도 과정

❑ 암호시스템 3가지 영역

❖평문을 암호화하기 위한 연산자의 유형

➢ 전치(轉置, Transposition) : 평문의 각 원소를 재배열

➢ 치환(置換, Substitution) : 평문의 각 원소를 다른 원소로 사상

암호학(cryptology)

❑ 암호시스템 3가지 영역

❖사용된 키의 수

- 관용키(conventional key) : single-key, symmetric, secret-key; 송수신자가 같은 키를 사용
- 공개키(public key) : two-key, asymmetric, public-key; 송수신자가 다른 키를 사용

❖평문 처리 방법

- 블록 암호 (Block cipher) : 연산을 블록 단위로 처리
- 스트림 암호 (Stream cipher) : 입력을 연속적으로 처리

암호 해독

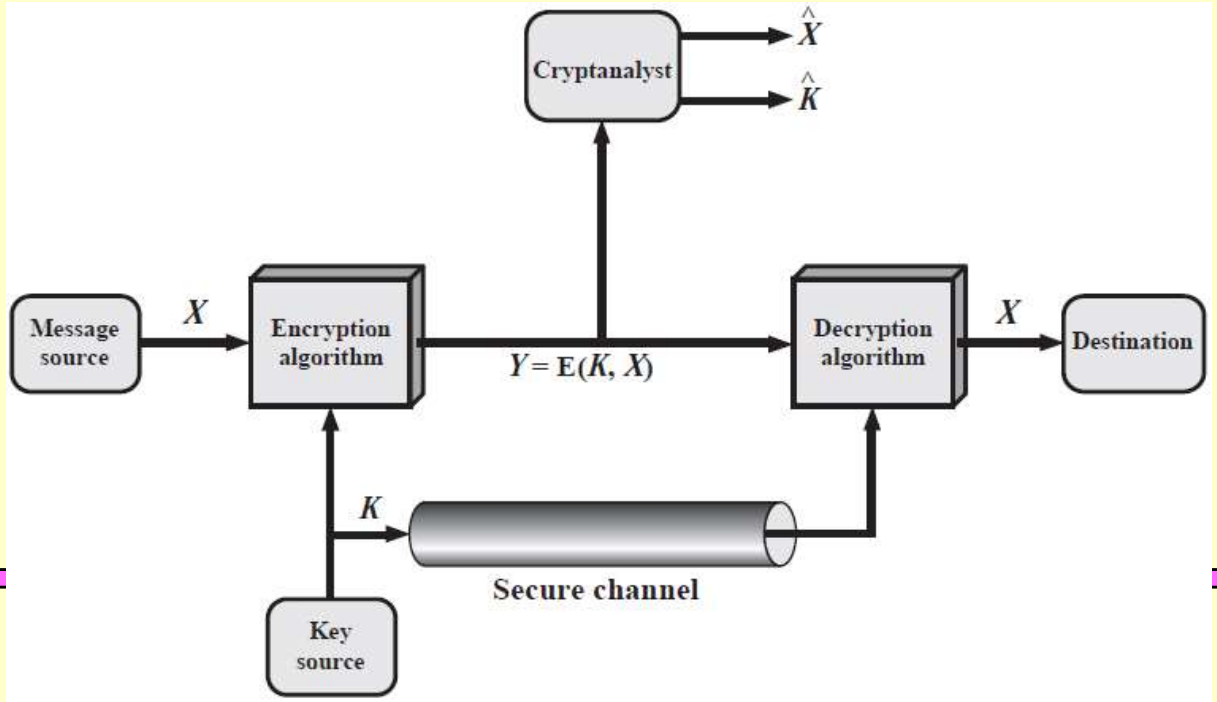
❑ 암호 해독(Cryptanalysis)

❖ 평문이나 키 또는 이 두 가지를 모두 발견하려는 시도 과정

❑ Brute-Force Attack (Exhaustive Attack)

❖ 가능한 모든 경우의 수를 시도(전사적 탐색, 전사 공격)

❖ Probable-Word Attack(추정단어공격)



암호 해독

❑ 안전성

❖무조건 안전성(Unconditionally Secure)

- ➢비용과 시간이 충분하여도 복호하기가 불가능
- ➢해당 암호 기법으로 생성된 암호문을 아무리 많이 사용하더라도 해당 암호문에 평문을 알아낼 수 있는 충분한 정보를 포함하지 않을 경우
- ➢One-time Pad

❖계산상 안전성(Computationally Secure)

- ➢해독 비용이 복호된 정보의 가치를 초과
- ➢해독시간이 정보의 유효 기간을 초과

❑ 암호 메시지에 대한 공격의 유형

- ❖ 암호문 단독 공격 (Ciphertext only Attack)
  - ➢ 암호 알고리즘, 해독할 암호문
- ❖ 기지 평문 공격 (Known plaintext Attack)
  - ➢ 하나 또는 그 이상의 알고 있는 평문에 대한 암호문을 인지
- ❖ 선택 평문 공격 (Chosen plaintext Attack)
  - ➢ 해독자가 선택한 평문 메시지와 해당 암호문을 인지
- ❖ 선택 암호문 공격 (Chosen ciphertext Attack)
  - ➢ 해독자가 선택한 암호문과 해독된 평문을 인지
- ❖ 선택 원문 공격 (Chosen text Attack)
  - ➢ 해독자가 선택한 평문 메시지와 해당 암호문을 인지
  - ➢ 해독자가 선택한 암호문과 해독된 평문을 인지

❑ 전사공격 시 모든 키 탐색을 위해 필요로 하는 평균 시간

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

처리 속도 단위

- 1ms = 1밀리초(millisecond) = 10^{-3}초
- 1μs = 1마이크로초(microsecond) = 10^{-6}초
- 1ns = 1나노초(nanosecond) = 10^{-9}초
- 1ps = 1피코초(picosecond) = 10^{-12}초
- 1fs = 1펨토초(femtosecond) = 10^{-15}초

고전적 암호기법

❑ 암호의 시초

- 이집트 나일강 변에 '미네쿠프'란 마을에서 시작
- 4000여년 전 한 문필가가 통치자의 일생을 기록하기 위해 석판에 상형 문자를 남긴 것
- 위엄과 권위를 담기 위해 상형문자 속에 환자(煥子)를 사용
  -> 결과적으로 내용을 숨긴 것이므로 암호의 효시

❑ 최초의 암호장치

- 스키테일(Scytale)
- 기원전 450년경 첩자의 비밀보고서로 사용
- 스파르타(라이산더 장군) 사용
  - ➢ 페르시아와 동맹, 아테네와 교전중 사용

❑ 암호시스템 3가지 영역

❖평문을 암호화하기 위한 연산자의 유형

- ➢치환(置換, Substitution) : 평문의 각 원소를 다른 원소로 사상
- ➢전치(轉置, Transposition) : 평문의 각 원소를 재배열

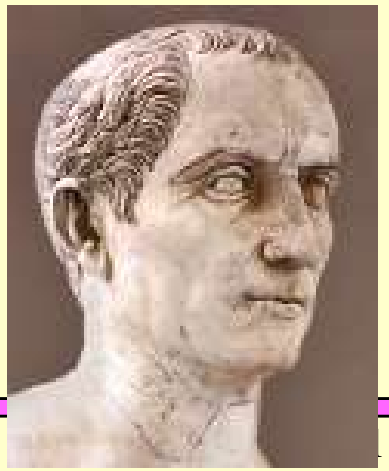
고전적 암호기법(시이저 암호)

❖ 치환(Substitution)기법

- ❑ 평문의 문자를 다른 문자나 숫자 또는 기호로 대체 시키는 방법
- ❑ 간단한 치환 암호기법
  - ❖ 쥴리어스 시저에 의해 개발(Ceaser Cipher, 시이저 암호법)
  - ❖ 예제 (Key: 3)

    평문 : MEET ME AFTER THE TOGA PARTY

    암호문 : PHHW PH DIWHU WKH WRJD SDUWB
  - ❖ 암호화 (문자 p를 암호화)
    - ➢ 문자 P를 C로 암호화
    - ➢ C = E (P) = (P + 3) mod (26)
    - ➢ P = D (C) = (C – 3) mod (26)



고전적 암호기법(시이저 암호)

❑ 일반화

- ❖ 암호화 ; C = E(P) = (P + k) mod 26
- ❖ 복호화 ; P = D(C) = (C - k) mod 26

❑ 단점

- ❖ 암호화 및 해독 알고리즘이 단순하다.
- ❖ 단순 대치이므로 문자 출현 빈도수에 의한 복호가 용이하다.
- ❖ 한 키가 25개 뿐이다.
  - ➢ Brute-force attack이 가능
  - ➢ 시도해야 할 키의 개수가 많도록 응용 필요
- ❖ 평문의 언어를 알고 있으며 쉽게 인식할 수 있다.
  - ➢ (평문 유형을 알 수 없도록 암호화 이전에 압축하여 인식을 어렵게 변환)

고전적 암호기법(시이저 암호)

❑ Caesar 암호

- ❖ 암호화 및 복호화 알고리즘을 알고 있음
- ❖ 가능한 키는 25개뿐임
- ❖ 평문의 언어를 알고 있으며 쉽게 인식 가능

→전사적 키 해독 기법에 취약

➢ 참고) 많은 키를 사용하는 경우, 전사적 공격은 비실용적임

- ❖ 예: 3DES의 키 공간: 2^{128}

➢ 참고) 평문의 언어나 유형을 알지 못할 경우 공격은 더 어려움

- ❖ 예: 원문이 ZIP으로 압축될 경우

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Q) 평문 SOONCHUNHYANG에 대하여 키 +5를 사용한 경우 암호문은?

평문 : SOON CHUN HYANG

암호문 :

귀족들에게 암살당하는 카이사르

❑ Q) 시저에게의 다음 편지에서 암호문의 내용은 무엇인가?

“EH FDUHIXO IRU DVVDVVLQDWRU”

고전적 암호기법(단일 문자 치환)

- **단일문자 치환 암호기법(Monoalphabetic Ciphers)의 단점**
  - ❖문자 출현 빈도수를 이용해 평문 유추가능
  - ❖사례 암호문:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWTMXUZUHSX

EPTEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

  - ➢암호문 문자의 출현 100분율

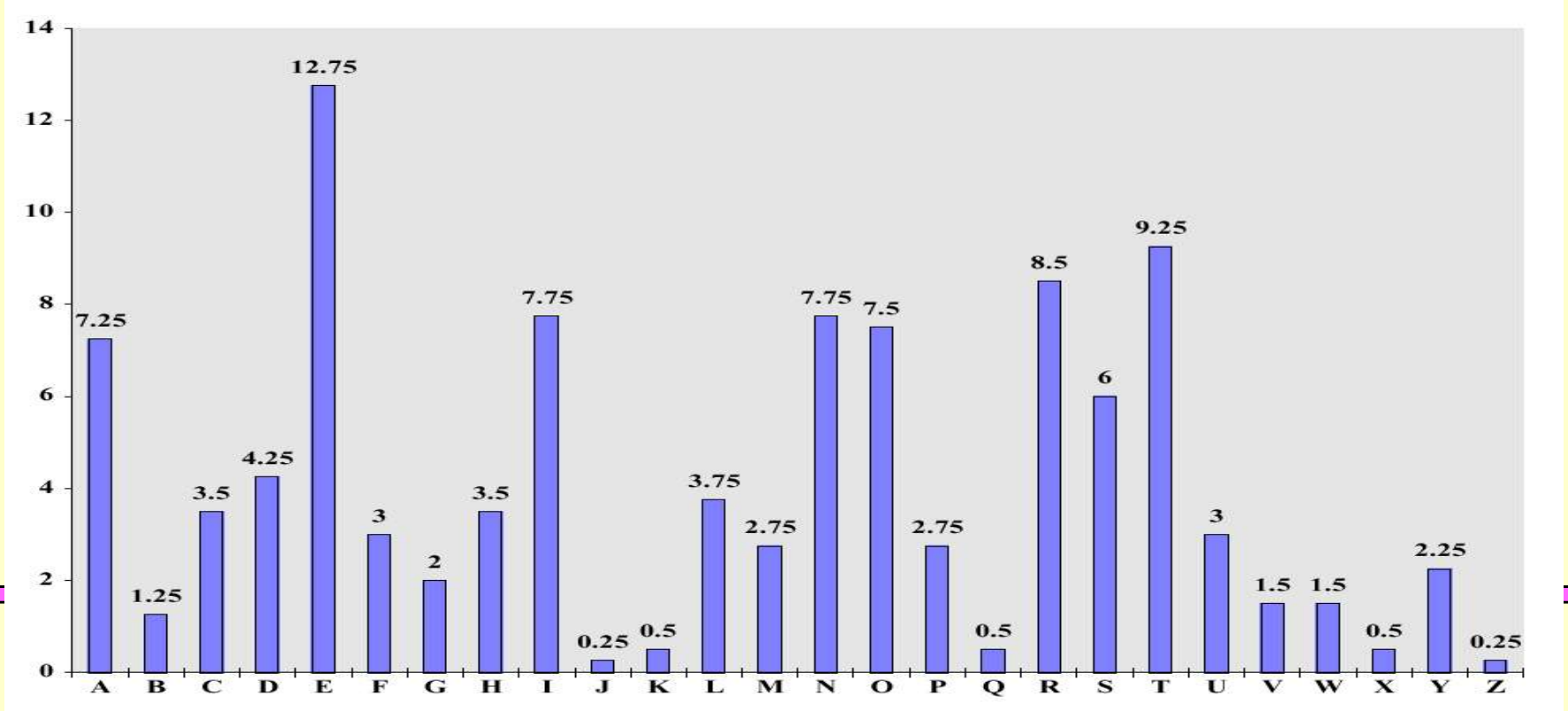
P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

고전적 암호기법(단일 문자 치환)

❖일반적 평문의 출현율

- ➢1 문자 출현율: { e, t, r, n, i, o, a, s }
- ➢ 2문자 출현율: th 등이 많이 나타남

❖암호문에서도 일반적 평문에 대응하는 문자가 같은 빈도로 나타남



고전적 암호기법(단일 문자 치환)

❑ 1문자 대응

- ❖ 암호문자 P, Z, S, U, O, M 및 H가 모두 상대적으로 높은 빈도 수를 갖으며 아마도 평문자 집합 e, t, r, n, i, o, a, s 중의 하나에 각각 해당 가정
- ❖ 최저 빈도 수를 갖는 문자 A, B, G, Y, I, J는 아마도 평문자 집합 w, v, b, k, x, q, j ,z 에 포함 가정

❑ 2문자 대응

- ❖ 암호문에서 가장 빈도 높은 2중자는 ZW로서 3번 출현
- ❖ 평문에서 가장 빈도 높은 2중자는 th
- ❖ 암호문 2중자 ZW 를 th에 대응

❑ 암호문에 ZWP에 평문 3중자 "the"로 해독

- ❖ 1문자 빈도율에서 P는 e에 해당
- ❖ 3중자 빈도율에서 the와 대응

고전적 암호기법(단일 문자 치환)

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

t a e e te a t h at e e a a

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

e t ta t ha e ee a e th t a

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

e e e tat e the t

- 지금까지 4문자만 확인됐지만, 메시지를 조금은 찾아냄.
- 빈도수를 계속 분석하고 시행착오를 거듭하면 해답 획득 가능.
- 단어 사이의 공백을 추가한 완전한 평문은 다음과 같다.

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

다중 문자 치환 암호 기법

(Multiple-letter encryption, Polygram substitution)

- 2자씩 암호화
- Playfair 알고리즘은 5 * 5 행렬에 기초
- 영국 Wheatstone 개발(1854년) 친구인 Playfair가 발표
- 키워드가 monarchy인 행렬

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

- I & J are treated as the same
- B,C,D,E,F...

C was already used in the keyword "MONARCHY"

- ❖ 해당 키워드를 사용하여 matrix를 채우고 해당 키워드를 구성하는 문자가 아닌 다른 문자로 나머지 matrix 공간을 채움
- ❖ 키워드 중복 문자를 제외하고 좌에서 우로, 상에서 하로 문자채움
- ❖ I와 J는 한 문자로 취급

다중 문자 치환 암호 기법

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

❑ 암호화 방법

1. 반복되는 평문은 X와 같은 채움문자로 분리
   - balloon : ba lx lo on
2. 같은 행에 두문자가 있을 경우 우측에 있는 문자와 치환
   - ar은 RM으로 치환
3. 같은 열에 두문자가 있을 경우 바로 밑에 문자와 치환
   - mu는 CM으로 치환
4. 그 외에 평문자 쌍은 대각선에 위치한 문자와 치환
   - hs는 BP로, ea는 IM(또는 JM)

다중 문자 치환 암호 기법

그 외에 평문자 쌍은 대각선에 위치한 문자와 치환

- hs는 BP로, ea는 IM(또는 JM)

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

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

Quiz

1. CORONA

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

2. SMART

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

Report 1

Q) 평문 DEPARTMENT OF COMPUTER SOFTWARE ENGINEERING 을 PALYFAIR에 의하여 암호문을 작성하시오. 키 값은 SECURITY

다중 문자 치환 암호 기법

❑ 특징

❖monoalphabetic 암호기법의 진보된 방법

➢알파벳은 26 가지

➢2중자는 26 * 26 = 676 가지

❖2중자의 빈도수 분석은 1중자보다 어려움

❖1차대전 중 영국 육군 야전 표준 시스템 사용

❖2차 대전 중 미국 육군 및 연합군에서 사용

❑ 단점

❖평문의 원래 구조가 많이 드러남

❖수백자의 암호문자로 구조를 알 수 있다.

❖암호기법은 평문과 같은 일정한 분포를 갖으므로 해독이 용이함.

다중 문자 치환 암호 기법

❑ Hill 암호

- ❖1929년 미국 수학교수 Laster Hill 제안
- ❖n-gram 치환 암호방식
  - ➢m개의 연속적인 평문자를 m개의 암호문자로 치환
- ❖M = 3일 경우 암호문 치환

$$C1 = (k11\ P1 + k12\ P2 + k13\ P3)\ mod\ 26$$
$$C2 = (k21\ P1 + k22\ P2 + k23\ P3)\ mod\ 26$$
$$C3 = (k31\ P1 + k32\ P2 + k33\ P3)\ mod\ 26$$

C: 암호문
P: 평문
k: 키

다중 문자 치환 암호 기법

❑ 암호문 형식을 열 벡터와 행렬로 표현

$$\begin{vmatrix} C1 \\ C2 \\ C3 \end{vmatrix} = \begin{vmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{vmatrix} \begin{vmatrix} P1 \\ P2 \\ P3 \end{vmatrix}$$

❑ 암호화 사례

❖평문: PAYMOREMONEY ➔ P, A, Y : 15, 0, 24

❖암호 키

$$K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

다중 문자 치환 암호 기법

❑ 암호문 계산

$$\begin{vmatrix} C1 \\ C2 \\ C3 \end{vmatrix} = \begin{vmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{vmatrix} \begin{vmatrix} P1 \\ P2 \\ P3 \end{vmatrix}$$

❖평문을 숫자변환➔ PAYMOREMONEY:

❖ P ➔15, A ➔ 0, Y ➔ 24, … …

❑ 숫자 대입 암호문 치환

$$\begin{vmatrix} C1 \\ C2 \\ C3 \end{vmatrix} = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \begin{vmatrix} 15 \\ 0 \\ 24 \end{vmatrix} \quad \text{mod } 26$$

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

❑ 숫자 대입 암호문 치환

	C1		17	17	5		15		11		L
	C2	=	21	18	21		0	mod 26 →	13		N
	C3		2	2	19		24		18		S

❑ K*(15, 0, 24) => (375, 819, 486) mod 26 = (11 13 18) = LNS

- ❖ C1 = 17 x 15 + 17 x 0 + 5 x 24 = 375 mod 26 = 14 … …11
- ❖ C2 = 21 x 15 + 18 x 0 + 21 x 24 = 819 mod 26 = 31 … …13
- ❖ C3 = 2 x 15 + 2 x 0 + 19 x 24 = 486 mod 26 = 18 … …18

❑ 복호화하기 위해서는 K^{-1}를 사용함

- ❖ $C=E(K,P)=PK \bmod 26$
- ❖ $P=D(K,C)=CK^{-1} \bmod 26 = PKK^{-1}=P$

다중 문자 치환 암호 기법

❑ 복호문 계산

❖암호문 계산 형식 C = E(K,P) = KP에서

❖평문 P = D(K,C) = $K^{-1}C = K^{-1}KP$ = P;

여기서, K^{-1}는 역행열:; $K^{-1}K = I$

$$\begin{vmatrix} P1 \\ P2 \\ P3 \end{vmatrix} = \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 7 \end{vmatrix} \begin{vmatrix} 11 \\ 13 \\ 18 \end{vmatrix} \quad \text{mod } 26 \rightarrow \begin{vmatrix} 15 \\ 0 \\ 24 \end{vmatrix} \begin{vmatrix} P \\ A \\ Y \end{vmatrix}$$

➢역행렬 계산

$$\begin{vmatrix} 17 & 17 & 15 \\ 21 & 18 & 2 \\ 2 & 2 & 19 \end{vmatrix} \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{vmatrix} \quad \text{mod } 26 \rightarrow \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

Report

- SCH의 암호문은??

	C1		7	2	5		?
	C2	=	3	8	1		?
	C3		4	5	9		?

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- **9월5일(화) 수업전까지 교탁위에 올리세요.**

다중 단일 문자 치환 암호화(Polyalphabetic cipher, 다표식 대치 암호)

- 다중대치를 통하여 고정키 단일 문자 치환 방법을 개량
- 다중 단일 문자 치환 암호방법의 공통점
  - ❖하나의 단일 문자 치환 규칙 집합을 사용
  - ❖주어진 변환에 사용될 규칙은 키에 의해 결정

- Vigenere 방법(1523-1596, 프랑스)
  - ❖키워드 : deceptive
  - ❖평문 : We are discovered save yourself"

키 : d e c e p t i v e d e c e p t i v e d e c e p t i v e

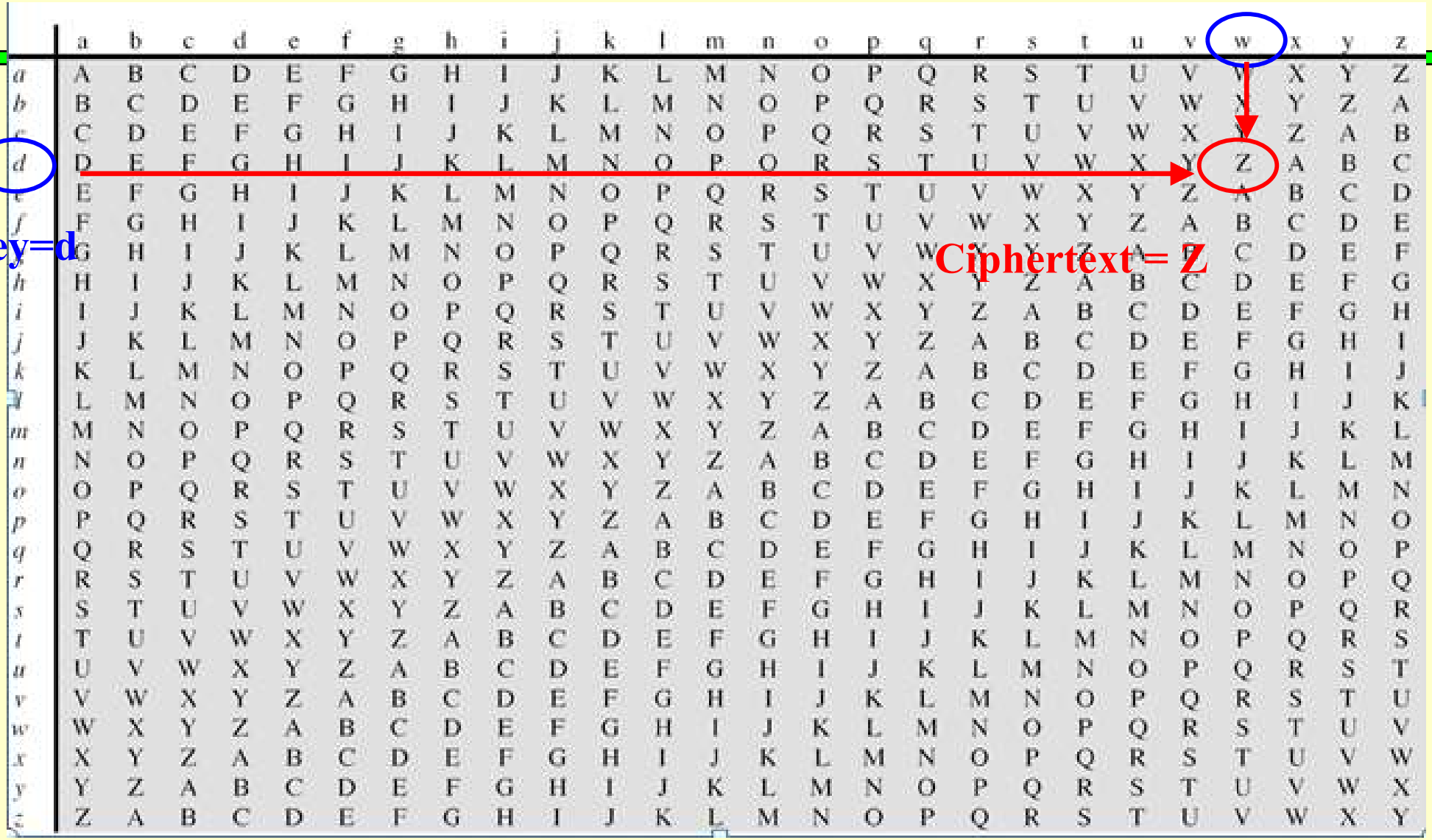
평문 : w e a r e d i s c o v e r e d s a v e y o u r s e l f

암 호 문 : Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext = w



Key=d

Ciphertext = Z

키 : d e c e p t i v e d e c e p t i v e d e c e p t i v e

평문 : w e a r e d i s c o v e r e d s a v e y o u r s e l f

암 호 문 : Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

다중 문자 치환 암호 기법

❑ 일반화

- ❖ 암호화 : $C_i = P_i + k_i \mod 26$
- ❖ 복호화 : $P_i = C_i - k_i \mod 26$
- ➢ 시저 암호 $C_i = E(P_i) = (P_i + k) \mod 26$

❑ 특징

- ❖ 평문자에 대한 암호문자가 유일한 키워드의 각 문자에 대하여 여러 개 존재
- ❖ 문자 빈도수에 대한 정보가 불분명해진다

❑ 단점

- ❖ 평문 구조에 대한 정보가 모두 은폐되지는 않는다.
- ❖ 단일 문자나 Vigenere로 암호화 되었는지 아는 것은 쉽다.
- ❖ 키워드 deceptive의 길이에 따른 암호문 주기발견 (키워드를 3이나 9로 유추가능)
  - ➢ 암호문에서 "VTW"이 나타남

다중 문자 치환 암호 기법

❑ 시저 암호

평문 : MEET ME AFTER THE TOGA PART

암호문 : PHHW PH DIWHU WKH WRJD SDUW

❑ Vigenere 암호

❖키워드 : deceptive

❖평문 : We are discovered save yourself”

키 : d e c e p t i v e d e c e p t i v e

평문 : w e a r e d i s c o v e r e d s

암호문 : Z I C V T W Q N G R Z G V T W A

다중 문자 치환 암호 기법

- 키워드의 변형 사용
- 키워드와 평문을 연결하여 키로 사용

키 : d e c e p t i v e w e a r e d i s c o v e r e d s a v
평문 : w e a r e d i s c o v e r e d s a v e y o u r s e l f
암 호 문 : Z I C *V T W* Q N G K Z E I I G A S X S T S L V V W L A

❖암호 해독상 취약점

➢ 키와 평문이 동일한 문자 빈도분포를 갖기 때문에 통계적 기법을 해독에 사용 가능

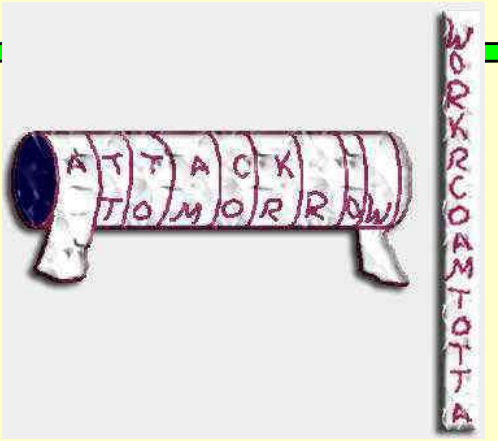
암호학(cryptology)

- 암호시스템 3가지 영역
  - ❖평문을 암호화하기 위한 연산자의 유형

    치환(置換, Substitution) : 평문의 각 원소를 다른 원소로 사상

    전치(轉置, Transposition) : 평문의 각 원소를 재배열

전치기법(Transposition Techniques)



- Scytale(스키테일)
  - ❖기원전 450년 경 그리스인들
  - ❖길이와 굵기가 같은 2개의 나무봉 사용
- 평문자나 비트의 순서를 절차에 따라 위치를 재조정
- rail fence 기법(단순한 전치 암호방식)
  - ❖깊이 : 2
  - ❖평문 : meet me after the toga party

    m e m a t r h t g p r y

    e t e f e t e o a a t
  - ❖암호문 : mematrhtgpryetefeteoaat
- 동일한 문자의 출현주기 문제점

❑ 복잡한 전치기법

❖메시지를 행렬의 행 순서로 쓰고 열 순서로 판독

- ➢row by row write / column by column read (key order)

❖n x m 행렬로 평문구성

- ➢Attack postponed until two am

키 : 4 3 1 2 5 6 7

평문 : a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

암호문 : TTNA APTM TSUO AODW COIX KNIY PETZ

❑ 문자가 바뀌는 일정한 주기 발견

❖n x m 행렬로 평문 재구성

TTNA APTM TSUO AODW COIX KNIY PETZ

키 : 4 3 1 2 5 6 7

평문 : T T N A A P T

M T S U O A O

D W C O I X K

N I Y P E T Z

암호문 : NSCY AUOP TTWI TMDN AOIE PAXT

TOKZ

❑ 평문 메시지의 문자들을 그 위치를 나타내는 숫자로 표시하면;

❖ a t t a c k p o s t p o n e d u n t i l t w o a m x y z

❖ 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

키 : 4 3 1 2 5 6 7

평문 : a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

❑ 첫 번째 전치 후의 결과

: TTNA APTM TSUO AODW COIX KNIY PETZ

❖ 03 10 17 24 04 11 18 25 02 09 16 23 01 08 15 22 05 12 19 26 06 13 20 27 07 14 21 28

❑ 규칙적인 구조 발견 (7문자씩 증가순서)

키 : 4 3 1 2 5 6 7

평문 : T T N A A P T

M T S U O A O

D W C O I X K

N I Y P E T Z

❑ 2차적 전치후의 결과

: NSCY AUOP TTWI TMDN AOIE PAXT TOKZ

❖ 17 09 05 27 24 16 12 07 10 02 22 20 03 25 15 13 04 23 19 14 11 01 26 21 18 08 06 28

❑ 다중단계 재 암호화

❖두 단계 이상의 다중전치와 치환을 하는 것은 일정한 주기를 회피하고 암호문 해독을 더욱 어렵게 만드는 효과

회전자 기계(Rotor Machine)

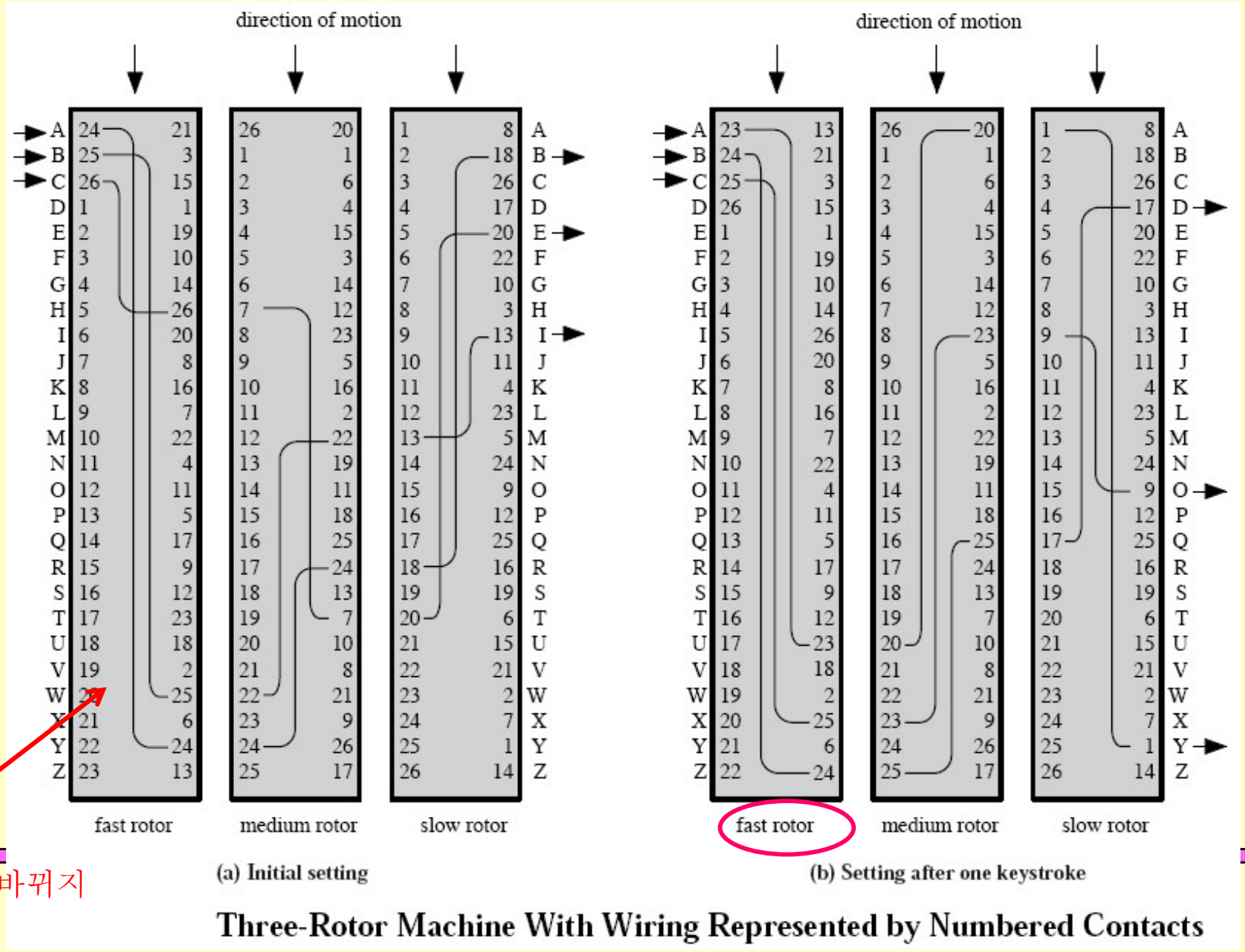
❑ 특징

- ❖독립적으로 회전 순환하는 실린더 집합으로 사용
- ❖다수의 실린더로 구성되며 각 실린더는 한 문자에 대한 치환을 수행함
  - ➢각 실린더는 26개의 입력핀과 출력핀 보유
  - ➢주기가 26인 다중 단일문자 치환
    - (26주기 polyalphabetic substitution)
  - ➢ 저/ 중/ 고속의 3단계 실린더로 구성하여 다중 치환 방식을 수행
- ❖2차 세계 대전 때 사용됨
- ❖세개의 실린더를 사용할 경우: 26^3 = 17,576개의 다른 알파벳 치환이 가능함

Rotor Machine(회전자 기계)

❖다중단계 재암호화의 원리를 적용

A → B
B → I
C → E



Three-Rotor Machine With Wiring Represented by Numbered Contacts

A → Y
B → D
C → O

내부연결은 바뀌지 않음

Vernam 암호

- 암호학적 공격에 안전하기 위해선 평문과 동일한 길이의 키를 가져야 하며, 평문과 통계적 연관성이 없어야 함
- Vernam 암/복호화 스킴

$$c_i = p_i \oplus k_i$$

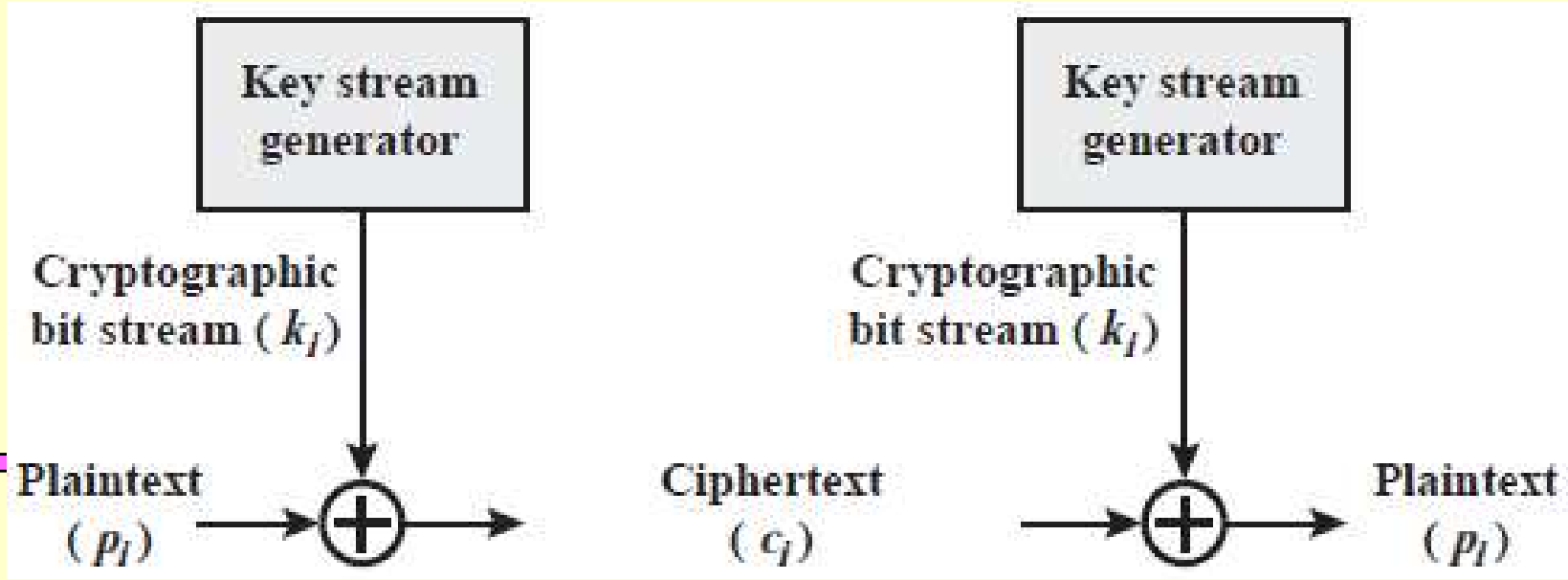
$$p_i = c_i \oplus k_i$$

p_i : ith binary digit of plaintext

k_i : ith binary digit of key

c_i : ith binary digit of ciphertext

$\oplus$: exclusive-or (XOR) operation



❑ 예) 평문 m=01011 10111 이라 하고,

비밀키 k=11011 10010 이라 하면 암호문은?

$c = m \oplus k$ =

암호문으로 부터 평문은???

Vernam 암호

- 스트림 암호
- 문자 대신 2진 자료로 작동
- 암호문은 평문과 키를 비트 방식의 XOR 연산을 수행하여 생성
- 복호문은 XOR의 속성상 해독(복호) 역시 같은 비트 방식으로 연산
- J. Mauborgne는 random한 key 값(반복없음)을 사용하면서 메시지 길이와 동일한 key를 가정함 → Perfect secrecy
- One Time Pad는 perfect security를 제공하지만 다음과 같은 문제점 가짐
  - ❖대용량의 random한 key를 다루기 어려움
  - ❖Key 분배 및 보호의 문제가 발생함

- 1917년 Gilbert Vernam이라는 AT&T기술자에 의해 소개
- 메시지와 정확히 같은 길이이고 반복되지 않는 랜덤 키 사용을 제안 ; 일회용 키(one-time pad)
- 랜덤 키를 무작위성을 가지도록 선택(생성)
  - ❖어떠한 수학적인 통계적 특성을 가지지 않음
  - ❖암호문으로 부터 키를 추론 할 단서를 발견할 수 없음
  - ❖Perfect secrecy
- 송수신자가 모두 이 랜덤 키를 보유하고 보호, 분배
- Vernam 암호 기법은 다른 기법보다 탁월한 아이디어지만 거의 사용하기 어려움.
  - ❖Unconditionally Secure
- 안전성
  - ❖무조건 안전성(Unconditionally Secure)
  - ❖계산상 안전성(Computationally Secure)

Steganograhpy

❑ 보안기술의 범주

- ❖ 보안(Security): 정보를 보호하는 방법
- ❖ 첩보(Intelligence): 정보를 탐지하는 방법

❑ 평문 메시지의 은닉 방법

- ❖ Steganograhpy 방법 ; 메시지의 존재 자체를 은폐
- ❖ cryptography 방법 ; 다양한 원문의 변환에 의해 외부인이 그 의미를 알지 못하도록 메시지를 변형

❑ 특징

- ❖ 메시지의 존재 자체를 은폐
- ❖ 원문내의 단어나 문자를 적절히 발췌하여 조합배열 함으로써 실제 메시지를 나타냄
- ❖ 스테가노그라피 또는 스테고(Stego : 스테고는 덮여있거나 비밀이라는 그리스어원 '스타가노스'에서 유래)는 잘 보이지 않게 데이터를 은닉하는 기술
- ❖ 스테가노그라피는 9.11 테러 이후, 테러리스트들이 그들의 대화를 은폐하기 위해

사용 예

- 노예의 머리
- 추노(推奴)
- 문자 마킹 (Character marking)
  - 원문의 문자에 연필로 덧써서 표시를 빛을 적당한 각도로 비추어야만 보임
- 보이지 않는 잉크 (Invisible ink)
  - 종이에 열이나 화학 처리를 해야만 보이는 잉크를 사용
- 핀 구멍 (Pin punctures)
  - 빛을 비춰야만 보이는 작은 구멍을 원문에 넣는 방법
- 타자 수정 리본 (Typewriter correction ribbon)
  - 흑색 리본으로 타자된 줄 사이에 강한 빛에서만 보이는 수정리본을 이용하여 타자하는 방법
- 악보암호
  - 1차대전(1914-1918)의 전설적인 독일 여첩보원 마타하리

❑ Steganography의 장점

- ❖ 비밀통신에 대한 사실이 발견되면 안 되는 사용자들에 의해 이용
- ❖ 암호화의 경우의 문제점
  - ➢ 암호화 한다는 사실이 통신 메시지가 중요하거나 비밀임을 암시
  - ➢ 즉, 암호화는 송수신자간에 무언가 감출게 있다고 생각하게 함

❑ Steganography의 단점

- ❖ 상대적으로 적은 정보비트를 은닉하는데 많은 오버헤드 요구
- ❖ 방법 노출시 재사용 불가

❑ 최근의 방법

- ❖ 키를 적용하는 기법을 추가하여 단점 극복
- ❖ 메시지를 먼저 암호화 한 후에 Steganography을 이용하여 은닉가능