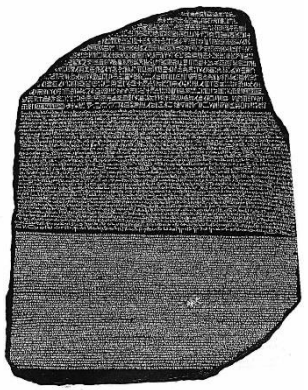
제3장
관용 암호 방식

한국IT 정보보안학부

수업 내용

- 환자 암호
- 전치 암호
- 적 암호(전치+환자)
- 스트림 암호
- 암호 해독
- ***Questions & Answers***



관용 암호 방식

- 암호화와 복호화에 동일한 키를 사용
- 공통키 암호 방식 또는 암호화와 복호화 과정이 대칭적이어서 대칭 암호 방식 이라고도 호칭함
- 수 천년 전부터 사용되어 오고 있는 암호 방식
- 평문의 문자를 다른 문자로 환자(치환)하거나 또는 문자의 위치를 바꾸는 전치과정으로 구성

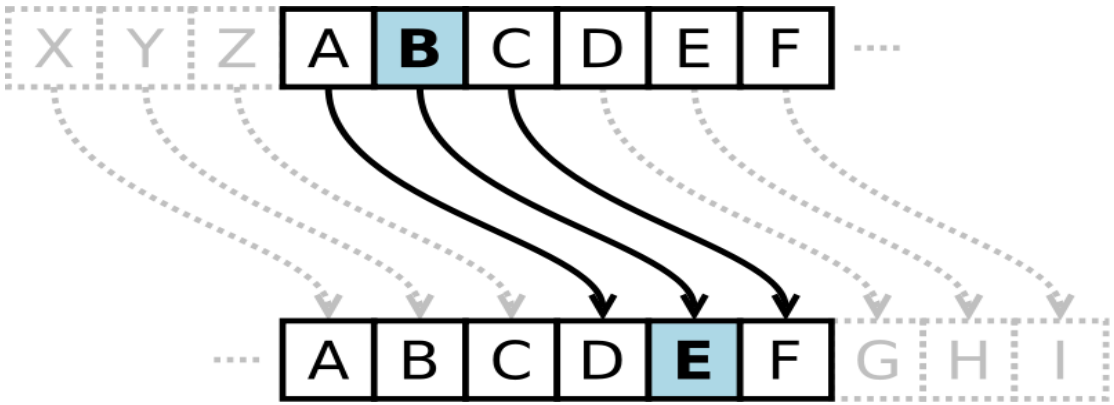
환자 암호

환자 암호

- 시프트 암호
- 단순 환자 암호
- Affine 암호
- 동음이의 환자 암호
- 다표식 환자 암호
- 철자 환자 암호
  - Hill 암호
  - Playfair 암호

시프트 암호(시저암호, 카이사르암호)

- **환자 암호 중에 가장 간단한 방법.**
  - 영문자를 순서대로 나열하고 일정 방향으로 일정 간격 시프트 (shift) 시키는 방법
  - 특히 시프트 간격을 3으로 한 경우를 Caesar 암호라고 한다.



시프트 암호

- Caesar 암호의 예 (k=3)

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
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

평문 M	i	n	f	o	r	m	a	t	i	o	n
암호문 C	L	Q	I	R	U	P	D	W	L	R	Q

시프트 암호

❖ 수식 표현

a	b	c	d	e	f	g	h	i	j	k	…	z
D	E	F	G	H	I	J	K	L	M	N	…	C

$$C = M + K \mod 26$$

$$K = 3$$

a	b	c	d	e	f	g	h	i	j	k	…	z
0	1	2	3	4	5	6	7	8	9	10	…	25

예제

- 시프트 암호의 키가 K=11일 때, 다음의 평문 M을 암호화해 보자.

평문	s	u	b	s	t	i	t	u	t	i	o	n		c	i	p	h	e	r

시프트 암호의 안전성

- 법 26을 이용한 시프트 암호는 안전하지 못하다.
- 침해자가 K에 0부터 25까지 키를 대입해보면 의미 있는 문장을 찾을 수 있음
- 시프트 암호는 이러한 소모적 공격(exhaustive key search)에 매우 취약함

예제

- 시프트 암호에 의한 암호문 C가 다음과 같다. 소모적 공격으로 평문 M을 찾아보자.

암호문	R	Y	G	K	B	O	I	Y	E	Q	O	D	D	S	X	Q	Y	X

단순 환자 암호(simple substitution)

- **평문 문자를 암호문 문자로 치환하는 방식**
  - 알파벳을 임의의 알파벳으로 치환하는 방식
  - 평문과 암호문 알파벳을 일대일로 매핑
  - 알파벳 26자의 순열
  - 키의 개수 : 26

- **평문 영문자를 무작위로 다른 영문자로 치환하여 암호문을 만드는 단순 환자 암호표**
  - p.68 [그림3.3] 참고

- **단순 환자 암호 복호표**
  - p.69 [그림3.4] 참고

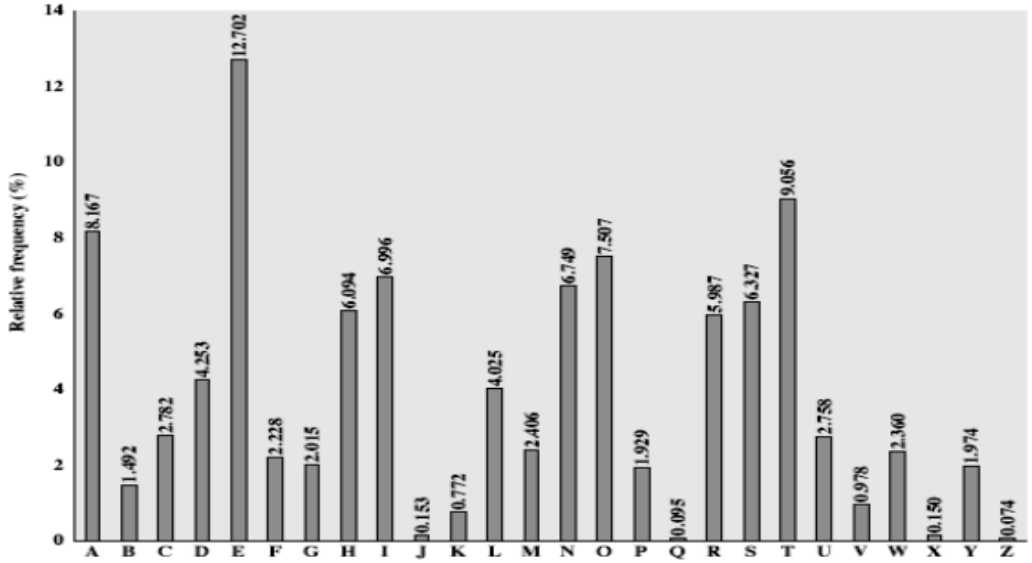
단순 환자 암호의 예

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

평문 M	i	n	f	o	r	m	a	t	i	o	n
암호문 C	P	R	N	X	Y	C	E	D	P	X	R

단순 환자 암호의 안전성

- **시프트 암호보다 전사공격에는 안전**
  - 키의 수 = 26!(약 4 * 10^{26} 개)
- **빈도수에 의한 통계적 분석으로 해독 가능**
  - 충분한 길이의 암호문, 암호문의 양이 많을 수록 통계적 성질이 많이 유지되어 암호문 해독이 용이함
  - p.69 [표3.1], p.70 [표3.2], [표3.3]



Affine 암호

시프트 암호 방식

- $C \equiv M + K \mod 26, \quad K = 3$

Affine 암호

- $C \equiv K_1 M + K_2 \mod 26$
- gcd (K_1, 26) = 1
  - ax = b mod m 에서 gcd(a,m)=1 이면 유일한 해 x 존재함
  - m 과 서로소인 **K1=1,3,5,7,9,11,15,17,19,21,23,25** 12개
- 12개의 K_1 과 26개의 K_2의 조합이 키가 될 수 있으므로 키 숫자는 12*26=312

예제

- $K_1=3$, $K_2=15$ 일 때 information security를 Affine 암호화 하자.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Affine 암호의 예

- K_1 = {1,3,5,7,9,11,15,17,19,21,23,25} 중
- K_1 = 3
- K_2 = 2 일 때

- BAEKS을 암호화 하시오.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

동음이의 환자 암호

- 단순 환자 암호 방식처럼 언어 통계학적 성질을 이용한 해독에 취약한 것을 보완하기 위해 고안된 방식
- 암호문의 문자 빈도가 균등하게 분포되도록 만드는 방식

동음이의 환자 암호

- 미국의 T.J.Beale이 고안한 Beale 암호 방식

평문	빈도%	암 호 문	평문	빈도%	암 호 문
a	8.2	56, 20, 44, 35, 12, 38, 09, 29	n	6.7	89, 84, 73, 78, 68
b	1.5	04	o	7.5	67, 41, 62, 46, 43, 53, 16
c	2.8	11, 95	p	1.9	06
d	4.3	64, 71, 47, 39	q	0.1	10
e	12.7	48, 25, 19, 72, 80, 91, 93, 02, 92, 82, 79, 58	r	6	13, 66, 86, 88, 63, 36
f	2.2	21, 30	s	6.3	77, 94, 09, 87, 45, 22
g	2	81, 18	t	9.1	65, 55, 76, 23, 85, 74, 54, 57, 14
h	6.1	03, 59, 49, 70, 31, 17	u	2.8	08, 15
i	7	27, 42, 07, 83, 90, 60, 32	v	1	24
j	0.2	52	w	2.3	75, 40
k	0.8	96	x	0.1	37
l	4	61, 69, 51, 53	y	0.2	26
m	2.4	50, 34	z	0.1	28

동음이의 환자 암호의 예

- p.73 [최하단]

h	o	m	o	p	h	o	n	i	c	s	u	b	s	t	i
03	67	50	41	06	59	62	89	27	11	77	08	04	94	65	42

- 예)

i	n	f	o	r	m	a	t	i	o	n	s	e	c	u	r	i	t	y
27	89	21	67	13	50	44	65	42	41	84	77	48	11	08	66	07	55	26

다표식 환자 암호 (Vigenere cipher)

- **다중문자치환(polyalphabetic substitution)**
  - **한번에 복수의 문자를 치환하는 암호방식**
  - 19th 세기에 알려져, 현재 "Vigenère cipher" 로 알려짐
  - 일대일 매핑 방식의 암호는 통계적 공격에 안전하지 않기 때문에, 평문과 암호문의 알파벳 빈도수를 다르게 할 필요가 있음
  - **현대 암호는 일대다 매핑 방식임**
    - 암호문의 알파벳 빈도수 분포가 원문의 알파벳 빈도수 분포와 일치하지 않음
  - **시저(카이사르) 암호 방식을 확장**
    - 키를 구성하는 각각의 알파벳 크기 만큼 원문 알파벳을 오른쪽으로 시프트 함

다표식 환자 암호 (Vigenere cipher)

- **비즈네르 암호**(Vigenere cipher)
  - **다표식 암호 중 반복키 암호**
  - 단어나 구조로된 키워드를 필요만큼(평문자 수) 반복해 KEY 로 사용하는 암호방식

ex)

- 키 : apple
- 평문 : hello world
- 암호문 : htaws wdgwh

다표식 환자 암호(Vigenere cipher)표

평문 / 키워드	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

예제

- 키워드 SECURITY로 Vigenere 암호 방식에 따라 다음을 암호화 해 보자

평 문	thiscryptosystemisnotsecure
키워드	SECURITYSECURITYSECURITYSEC
암호문	LLKMTZRNLSUSJBXKAWPIKAXAMVG

철자 환자 암호

- Hill 암호
- Playfair 암호

철자 환자 암호 – Hill 암호

- 다형 환자 암호
- Polygram substitution cipher
- 두 문자 이상을 묶어 이들을 다른 문자나 숫자로 변환
- Invented by Lester S. Hill in 1929

철자 환자 암호 – Hill 암호

- **철자 환자 암호 - Hill 암호**

$$c_1 = k_{11}m_1 + k_{12}m_2 + k_{13}m_3$$
$$c_2 = k_{21}m_1 + k_{22}m_2 + k_{23}m_3$$
$$c_3 = k_{31}m_1 + k_{32}m_2 + k_{33}m_3$$

$$C = KM$$
$$M = K^{-1}C = K^{-1}KM$$

예제

$$A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}, A^{-1}=\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

- 다음 행렬 K로 Hill 암호 및 복호화 하기

$$M = op, K \equiv \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \bmod 26, K^{-1} \equiv \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \bmod 26$$

$C \equiv MK \bmod 26$

$$C \equiv (14 \quad 15)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \bmod 26$$

$$\equiv (154+45, 112+105) \bmod 26$$

$$\equiv (17,9) \bmod 26$$

$$\equiv RJ$$

$M \equiv CK^{-1} \bmod 26$

$$C \equiv (17 \quad 9)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \bmod 26$$

$$\equiv (119+207, 306+99) \bmod 26$$

$$\equiv (14,15) \bmod 26$$

$$\equiv op$$

철자 환자 암호 - Playfair 암호

The Playfair system was invented by Charles Wheatstone, who first described it in 1854.

Lord Playfair, who heavily promoted its use.

철자 환자 암호 - Playfair 암호

❖ Playfair 암호표의 예

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

❖ 암호표 생성 규칙

- 키워드의 문자를 테이블에 좌→우, 위→아래 방향으로 하나씩 채움(단, 중복 문자는 버림)
- 나머지 남는 공간은 알파벳 순서로 채움
- 알파벳의 개수(25)를 맞추기 위해 일반적으로 "J" 를 생략(J=I)
- 또는 많이 사용되지 않는 "Q" 를 생략(Q=Z)

철자 환자 암호 - Playfair 암호

❖ Playfair 암호표의 예2

- Using "playfair example" as the key, the table becomes

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

철자 환자 암호 - Playfair 암호

- **Playfair 암호화 절차**
  - 먼저 평문의 띄어쓰기를 없애면서, 2문자씩 분리하는데
  - 연속되는 문자(예 PP)가 있으면 같은 문자 사이에 X를 삽입(예 PXP)하여 같은 알파벳이 중복되지 않도록 하면서 다시 2문자씩 분리하는 방법을 계속함
  - 전체의 글자 수가 홀수이면 맨 마지막에 X를 추가하여 짝수개로 만듬

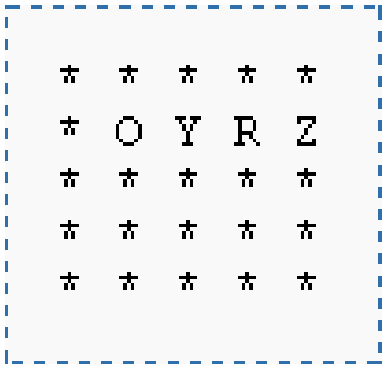
철자 환자 암호 - Playfair 암호

❖ Playfair 암호화 절차

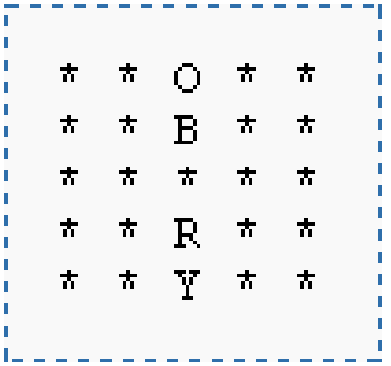
1) 동일 행에 $m_1 m_2$가 있으면 $c_1 c_2$는 우측문자

2) 동일 열에 $m_1 m_2$가 있으면 $c_1 c_2$는 아래문자

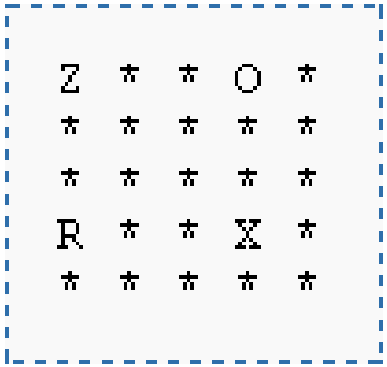
3) 다른 행 열에 $m_1 m_2$가 있으면 $c_1 c_2$는 대각 문자



Hence, OR -> YZ



Hence, OR -> BY



Hence, OR -> ZX

예제

- 아래의 표를 참고하여 평문 informationsecurity를 Playfair암호화 하기

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

rmationsecurityx

- 암호문 – TOHNDUSIAWVFCLZDGIZY

전치 암호

전치 암호(transposition cipher)

- **평문 문자의 순서를 어떤 특별한 절차에 따라 재배치하여 평문을 암호화하는 방식**
  - 평문의 알파벳 위치를 변경
  - 평문의 알바펫들은 손실없이 유지됨
  - 평문의 알파벳 빈도수 분포가 암호문에 그대로 유지됨

  예1)레일펜스암호
    - 열단위로 매핑하고 행단위로 읽기

  예2) Row Transposition
    - 평문을 행렬테이블에 행단위로 입력. 남는부분은 임의의문자
    - 암호문은 키의 열 번호 순으로 읽기
- **scytale 암호**
- **단순전치 암호**
- **Nihilist 암호**

scytale 암호

	a	b	c	d	e	f	g
	s	c	y	t	a	l	e

as	bc	cy	dt	ea	fl	ge

단순 전치 암호

- simple transposition cipher
- 정상적인 평문 배열을 특정한 키의 순서에 따라 평문 배열을 재조정하여 암호화하는 방식

예제

- 단순 전치 암호의 키가 다음과 같을 때 information security를 암호화 하자

암호화

1	2	3	4	5	6
3	5	1	6	4	2

복호화

1	2	3	4	5	6
3	6	1	5	2	4

평문 i n f o r m a t i o n s e c u r i t y x y z a b

암호문 F R I M O N I N A S O T U I E T R C Y A Y B Z X

Nihilist 암호

- 단순 전치 암호의 암호 강도를 높이기 위해 행은 물론 열에 대해서도 전치를 적용한 암호
- 키워드에 따라 먼저 행을 일정 간격으로 전치시키고 다시 키워드의 순서에 따라 열을 일정 간격으로 전치시킨다.
- 때로는, 전치를 대각선 방향으로 하는 경우도 있다.

예제

- LEMON이라는 키워드를 이용한 Nihilist 암호를 구성해 보자

		L	E	M	O	N
		2	1	3	5	4
L	2	h	t	i	i	s
E	1	g	s	o	d	o
M	3	o	f	r	e	s
O	5	u	c	r	c	e
N	4	p	i	h	r	e

평문 t h i s i s g o o d f o r s e c u r e c i p h e r

암호문 GSODOHT I I SOFRE SP I HREUCRCE

적 암호

적 암호(product cipher)

- 암호 강도를 향상시키기 위해 전치와 환자를 혼합한 암호 방식
- 대표적인 예
  - 제 1차 세계 대전 때 독일군이 사용하던 ADFGVX 암호
- 대부분의 현대 관용 암호 방식은 적 암호 방식을 이용하고 있음

적 암호

- ADFGVX 암호
- Feistel
- DES
- Rijndael(AES)
- SEED

ADFGVX 암호

- ADFGVX의 여섯 개의 문자를 행과 열로 나열한 다음 36개의 열과 행이 직교하는 위치에 26개의 문자와 10개의 숫자를 무작위로 대입하여 암호화

ADFGVX 암호

❖ ADFGVX 암호 환자표

	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

예제

- **평문 conventional cryptography를 앞의 표에 따라 전치 키워드 CIPHER로 ADFGVX 암호화해 보자.**
  - 중간 암호문 작성(환자)

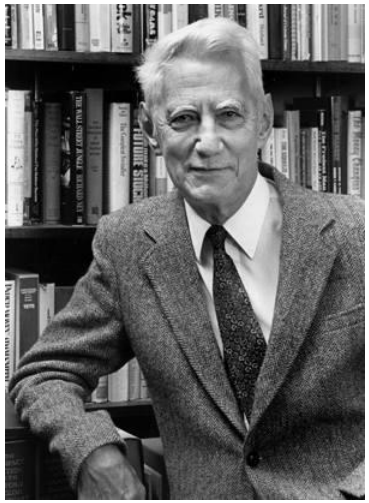
c	o	n	v	e	n	t	i	o	n	a	l
XA	DX	DA	GX	VG	DA	GV	VX	DX	DA	AF	DG

c	r	y	p	t	o	g	r	a	p	h	y
XA	XV	GG	XX	GV	DX	DD	XV	AF	XX	FV	GG

[참고] Claude Shannon

- Claude Elwood Shannon
- April 30, 1916 – February 24, 2001
- an American electronic engineer and mathematician, is known as "the father of information theory".
- 정보이론의 아버지

Claude Elwood Shannon
(1916-2001)

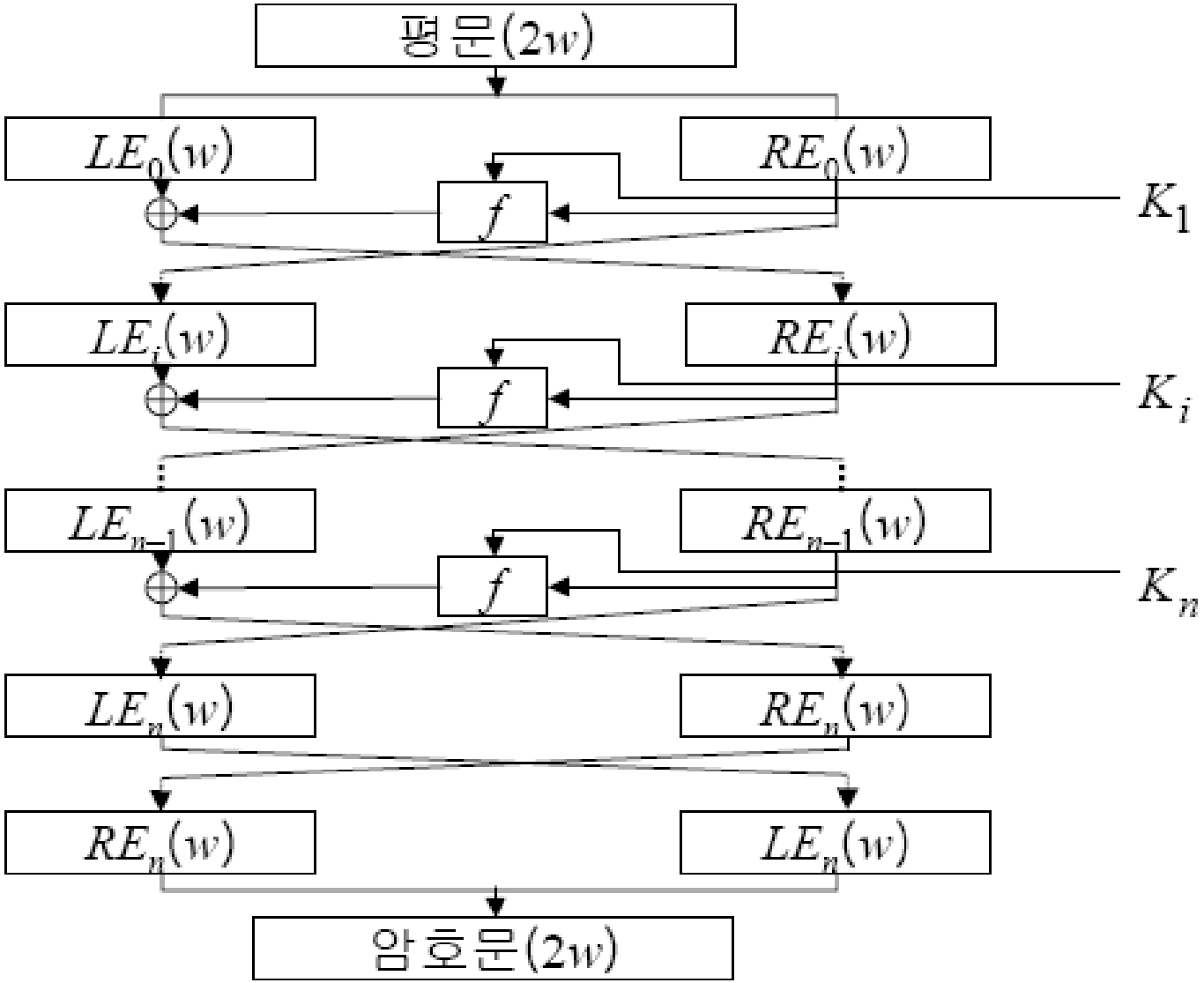


Feistel 암호

- Shannon의 암호 이론을 근거로 전치와 환자를 반복 적용한 적 암호를 구성함

- 간편한 방식과 암호의 안전성이 높아 대부분의 현대 관용 암호 방식 설계에 Feistel 암호 방식이 이용되고 있음

Feistel 암호 방식



Feistel 암호 방식

- **관계식**

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus f(RE_{15}, K_{16})$$

Feistel 암호 방식의 복호화 과정

- **복호화 과정**

$LD_1 = RD_0 = LE_{16} = RE_{15}$

$RD_1 = LD_0 \oplus \mathrm{f}(RD_0, K_{16})$

$= RE_{16} \oplus \mathrm{f}(RD_0, K_{16})$

$= [LE_{15} \oplus \mathrm{f}(RE_{15}, K_{16})] \oplus \mathrm{f}(RE_{15}, K_{16})$

$= LE_{15}$

$LD_{16} = RE_0$

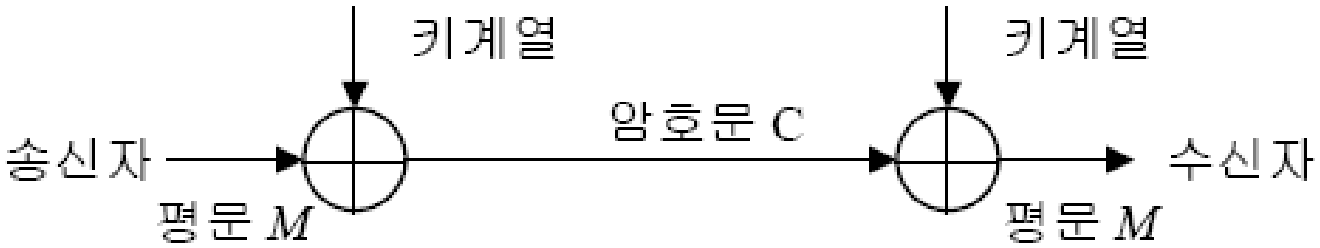
$RD_{16} = LE_0$

- $\boldsymbol{A \oplus B \oplus B = A}$

스트림 암호

스트림 암호

- 비트 단위의 암호화를 수행
- 메시지열과 키계열을 이진합하여 암호화하는 방식

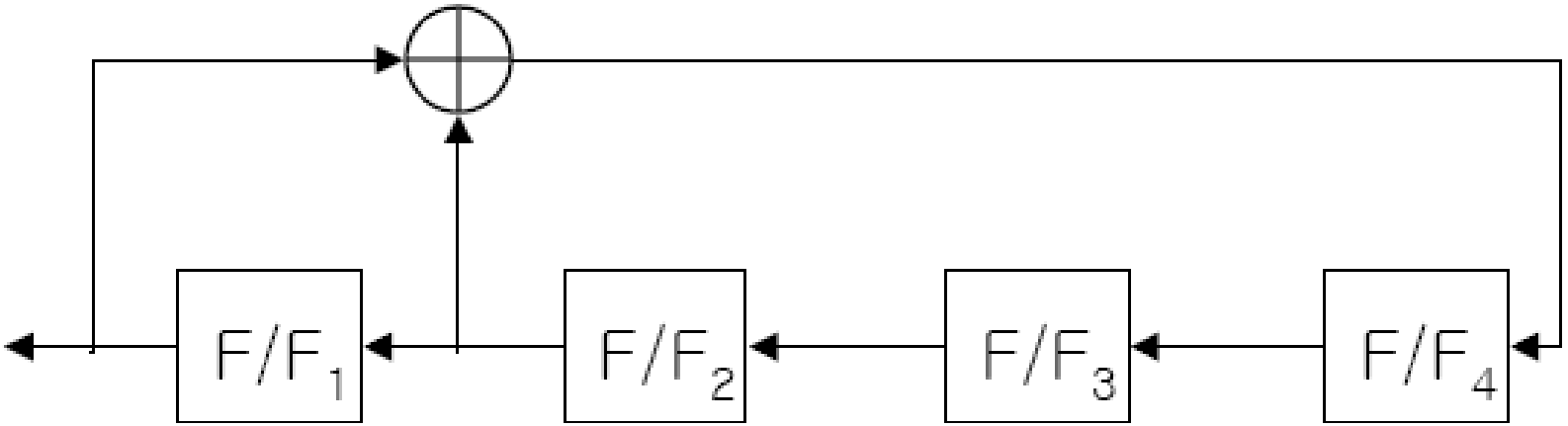


평문	10111011	암호문	01111110
키계열	11000101	키계열	11000101
암호문	01111110	평문	10111011

스트림 암호

- 스트림 암호 방식의 암호 강도는 키 계열의 무작위성이 결정한다.
- 키스트림의 비예측성(unpredictability)을 충족하기 위해서 최대주기, 선형복잡도, 난수성 필요
- 일반적으로 키 계열은 선형 궤환 시프트 레지스터(linear feedback shift register, LFSR)를 이용하여 생성함

4단 선형 궤환 시프트 레지스터



- **플립플롭의 초기값은 모두 0이어서는 안됨**
  - 왜냐하면, 출력 키 계열은 계속해서 0만 출력함
  - 스트림 암호는 암호문과 평문이 동일하게 됨

예제

- [그림3.8]의 선형 궤환 시프트 레지스터의 플립플롭 F/F_i의 초기값이 1010일 때 키 계열을 구해 보자.

암호 해독

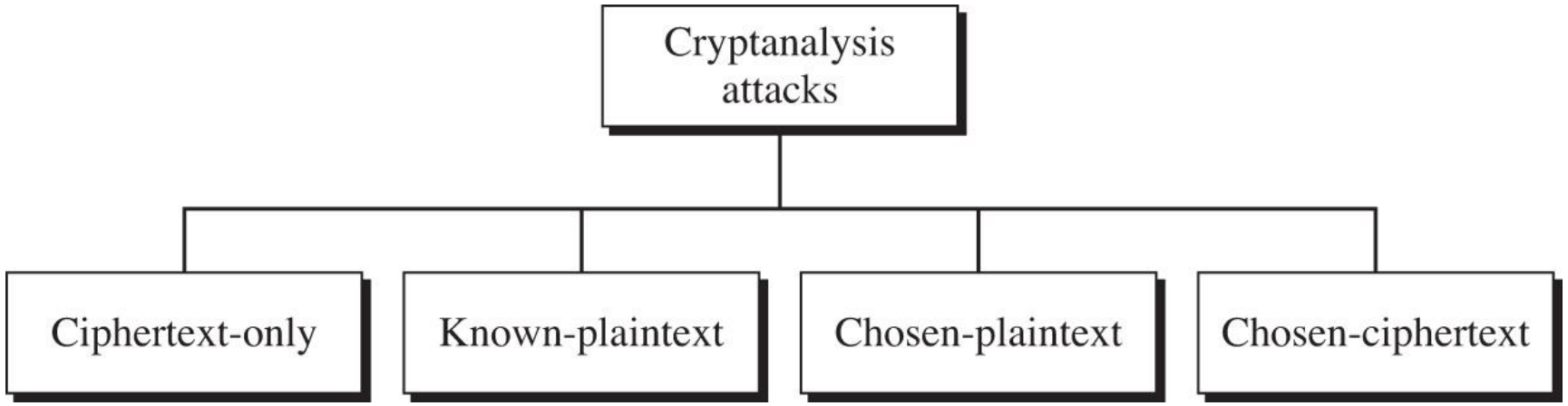
환자 암호의 해독

암호 해독

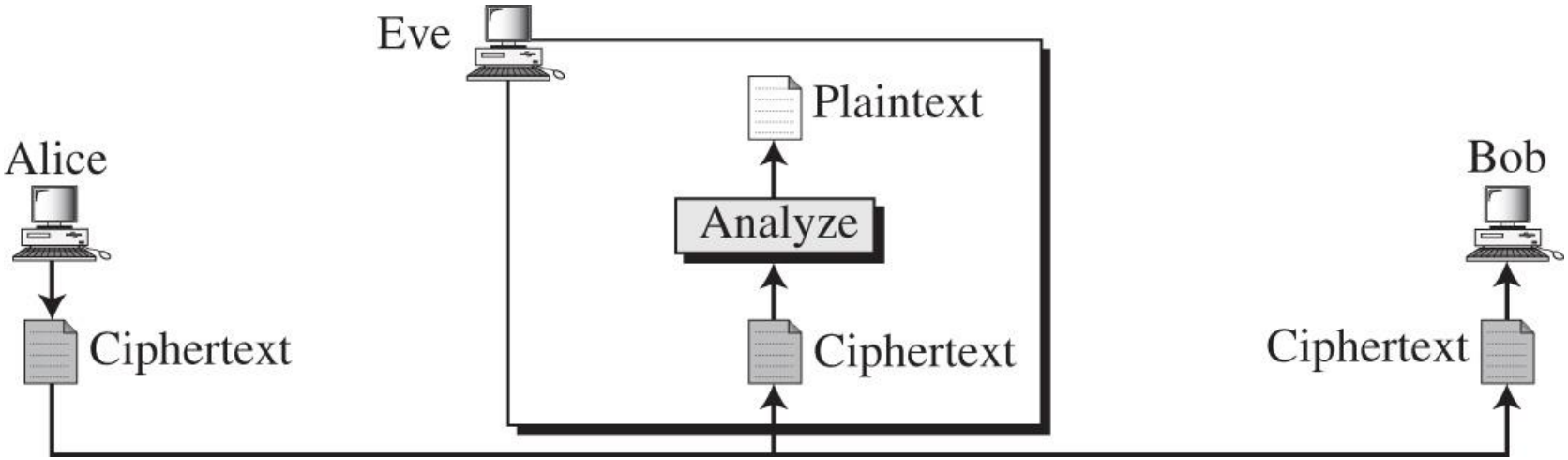
- 암호 방식의 정규 참여자가 아닌 제삼자로 암호문으로부터 평문을 찾으려는 시도를 암호 해독 또는 공격이라 함
- 암호 해독자, 제삼자, 침해자
  - **eavesdropper** (사적인 대화를) 엿듣는 사람.

암호 해독 방법

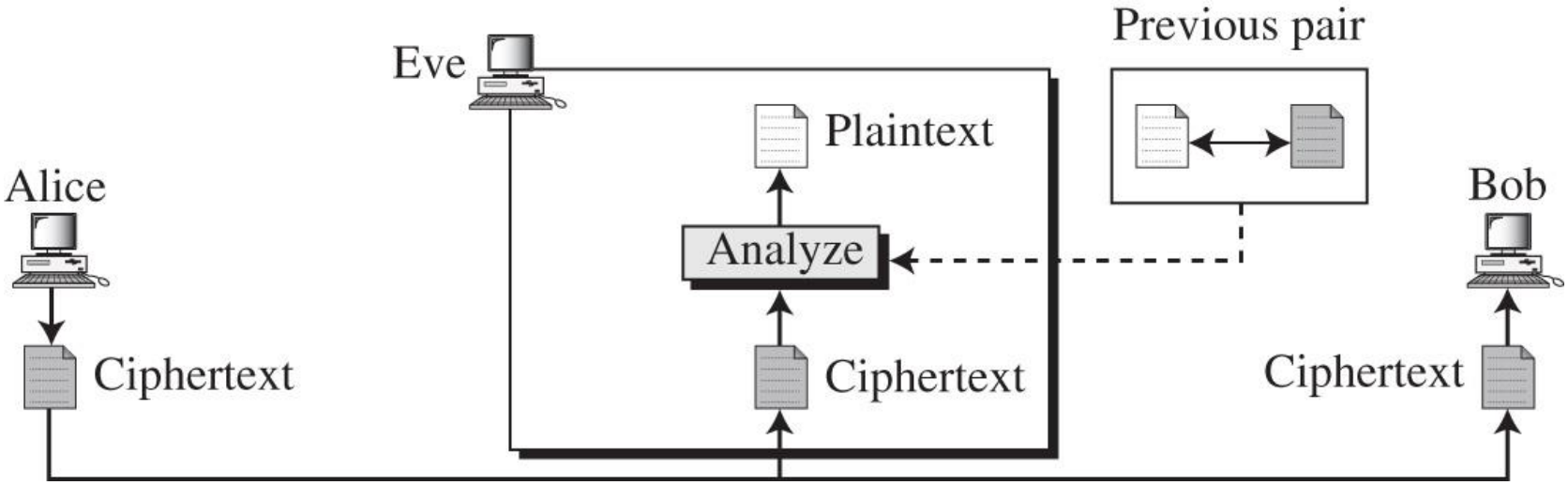
- 암호문 단독 공격 (Ciphertext-only Attack)
- 기지 평문 공격 (Known-plaintext Attack)
- 선택 평문 공격 (Chosen-plaintext Attack)
- 선택 암호문 공격 (Chosen-ciphertext Attack)



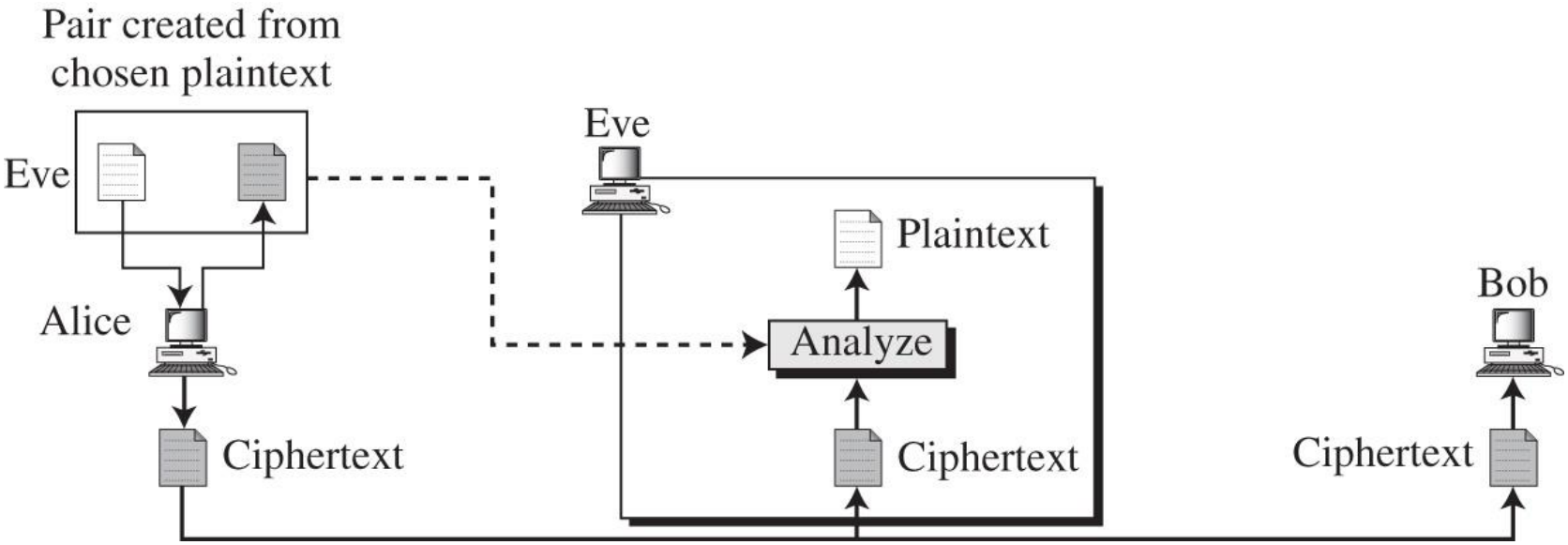
암호문 단독 공격 (Ciphertext-only)



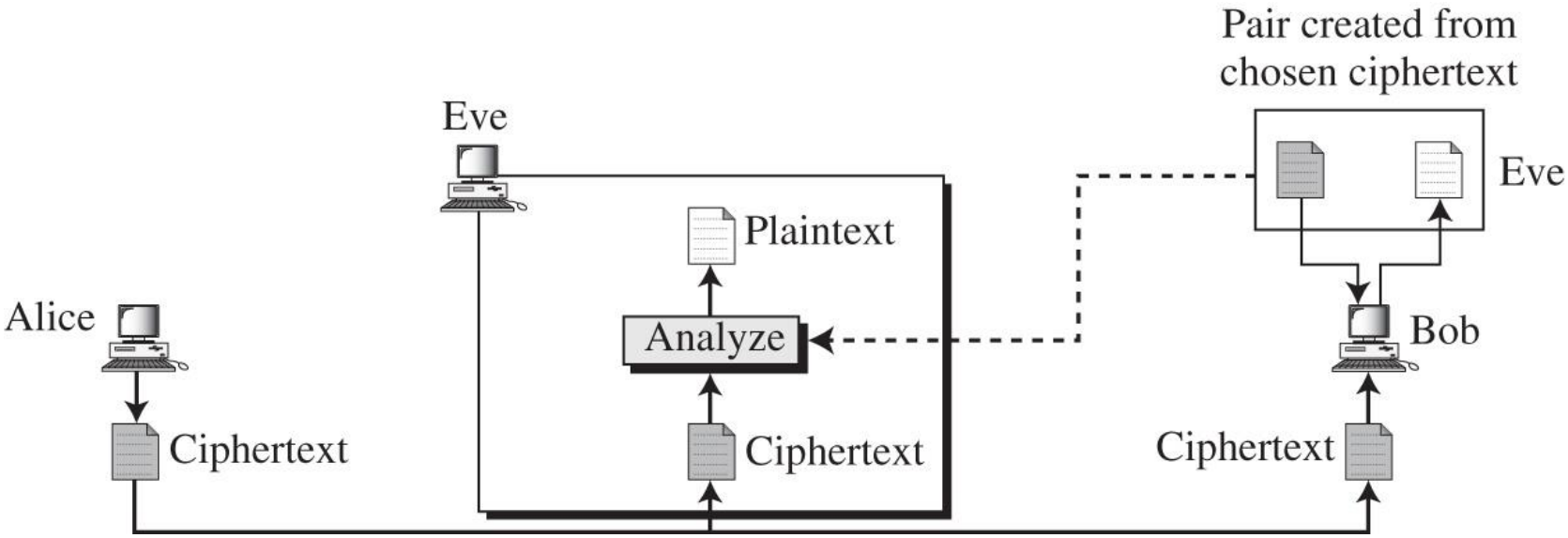
기지 평문 공격 (Known-plaintext)



선택 평문 공격 (Chosen-plaintext)



선택 암호문 공격 (Chosen-ciphertext)



[참고] 환자 암호의 해독

- 교재 p.94

연습문제

1. 환자 암호방식, 전치 암호방식, 적 암호 방식에 대해 각각 설명하고 간단히 예를 들어 보라.
2. 시프트암호의 키가 9 일때 다음의 암호문을 복호화 하라.

   암호문 : yujrwcngc
3. CIPHER 라는 키워드를 사용하여 Nihilist 암호를 구성하라.

   평문 : The name of the book is modern cryptography
4. 평문 modern cryptography를 다음의 표에 따라 ADFGVX 암호화 하라. (단,전치키워드는 cryoto이다)

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