CR
YP
TO
LO
GY

Cryptography
Cryptology

3장 . 관용암호방식

Korea College of Information & Technology 2020 [김소희]

수업 목표

- 관용암호: 암호화와 복호화에 동일한 키 값을 사용한다.
- 고전 관용 암호 방식을 이해한다.
  - 환자 암호
  - 전치 암호
  - 적 암호
- 현대 암호학의 기초 개념을 이해한다.

3.1 환자 암호

- 대치(substitution) 암호 : 하나의 기호를 다른 기호로 변경.

시프트 암호

› 평문 문자를 암호문 문자로 일대일 대응시켜 암호화
  – 항상 같은 문자로 대응 : 단일 문자 암호

› 예

평문	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
암호문	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

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

Shift 3

평문	i	n	f	o	r	m	a	t	i	o	n	s	e	c	u	r	i	t	y
암호문	L	Q	I	R	U	P	D	W	L	R	Q	V	H	F	X	U	L	W	B

  – 시프트 간격 n = 3 : Caesar 암호, 덧셈 암호 라고도 불린다.

CR
YP
TO
LO
GY

KIM SOHEE

시프트 암호

› 평문문자 M , 암호문자 C, 시프트 간격 K

$$C \equiv M + K \bmod 26$$

– 영문문자를 0~25 까지 값을 순서대로 부여하면 위의 식

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

› 복호화 : $M \equiv C - K \bmod 26$

› 문제 : 1) K=11 , 평문(M) hello 를 암호화 하시오.

› 2) K=15, 암호문(C) WTAAD 를 복호화 하시오.

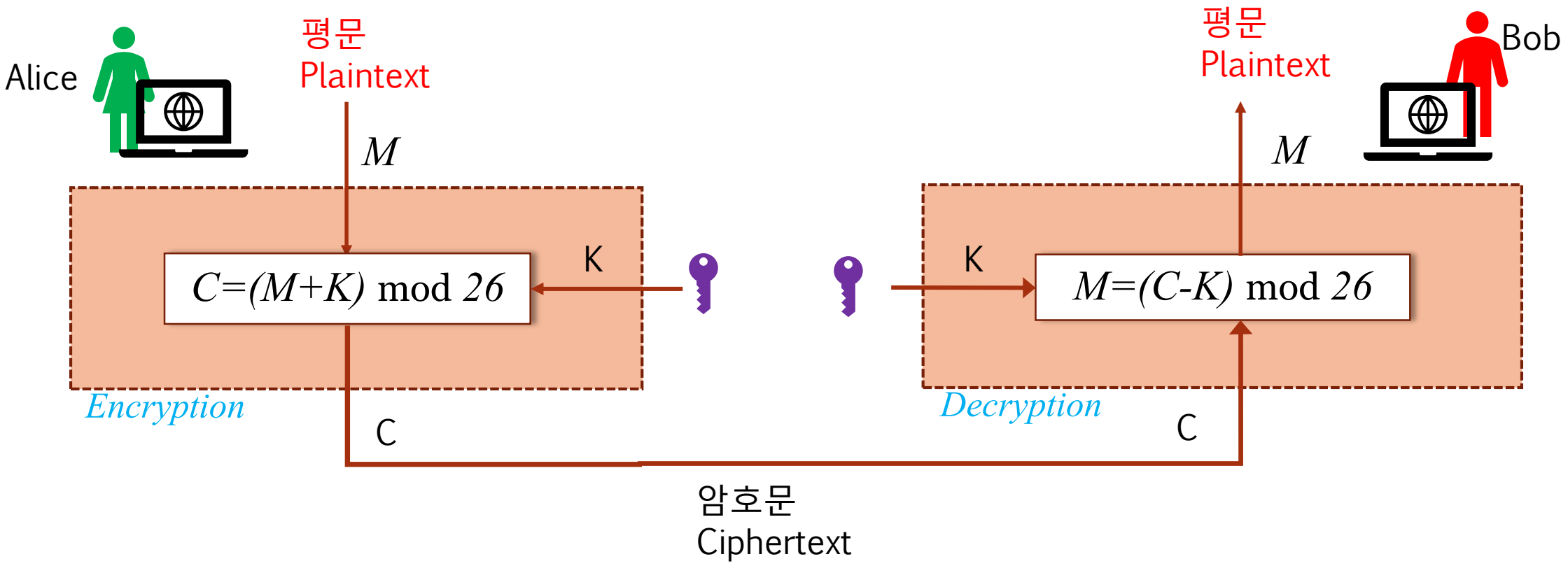
CR YP TO LO GY

KIM SOHEE

(교재)예제3.1

› K=11이다. 평문 M ‘substitution cipher’을 암호화 해보자.

시프트 암호



시프트 암호

› 실용적 암호 방식의 조건
  – 1. 암호화 , 복호화 알고리즘은 다항 시간 알고리즘 이어야 한다.
  – 2. 공격자가 암호문 C로 부터 사용된 키 K 또는 평문 M을 알 수 없어야 한다. 암호 해독
  – 소모적 공격 : 키 값 0 ~ 25 26가지를 대입하여 평문 알아내는 방법

› → 소모적 공격은 키 값의 범위(키 공간)를 크게 하여 방지할 수 있다.

CR
YP
TO
LO
GY

KIM SOHEE

(교재)예제3.2

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

RYGKBOIYEQODDSXQYX (rygkboiyeqoddsxqyx

CR
YP
TO
LO
GY

KIM SOHEE

단순 환자 암호

› [그림3.3] 암호화 과정

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

› [그림3.4] 복호화 과정

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

CR
YP
TO
LO
GY

KIM SOHEE

단순 환자 암호

- 평문 문자를 암호 문자로 치환하는 방식이 무작위로 임의의 대응을 한다. 단순 환자 암호표를 사용.
  - 이 때 가능한 경우의 수는 26! => 약 4×10^{26} 개이다.
  - 키 숫자가 많아 소모적 공격에 안전
- 평문문자와 암호문자가 여전히 1대1 대응하므로
- 영문 언어의 통계적 성질을 이용하여 문자 빈도수를 이용 암호문자를 평문 문자로 쉽게 해독될 수 있다. 특히 암호문의 양이 많아지면 해독이 더욱 용이해 진다.

CR
YP
TO
LO
GY

KIM SOHEE

영문자 빈도 확률

p.69 [표3.1], p.70 [표3.2], [표3.3]

평문	빈도	평문	빈도
a	8.2%	n	6.7%
b	1.5%	o	7.5%
c	2.8%	p	1.9%
d	4.3%	q	0.1%
e	12.7%	r	6%
f	2.2%	s	6.3%
g	2%	t	9.1%
h	6.1%	u	2.8%
i	7%	v	1%
j	0.2%	w	2.3%
k	0.8%	x	0.1%
l	4%	y	2.0%
m	2.4%	z	0.1%

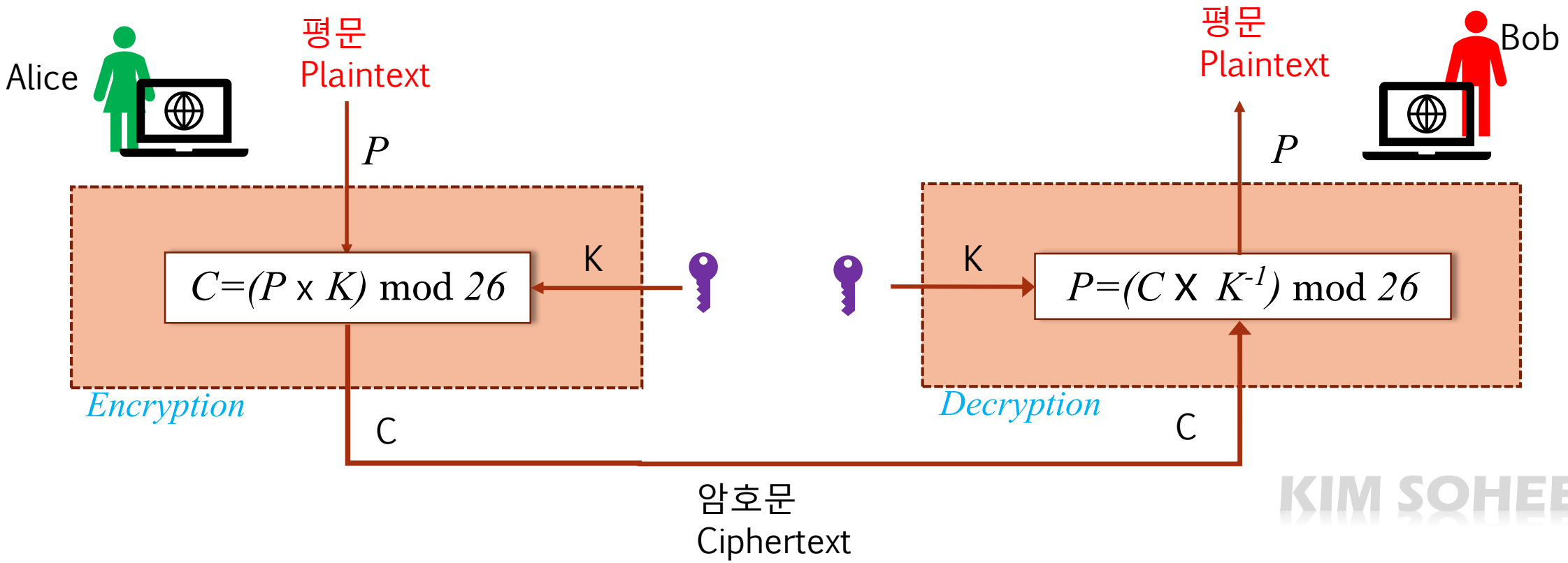
평문	빈도	평문	빈도
th	3.88%	to	1.17%
he	3.68%	or	1.15%
in	2.28%	it	1.13%
er	2.18%	is	1.11%
an	2.14%	hi	1.10%
re	1.75%	es	1.10%
nd	1.56%	ng	1.05%
on	1.42%	the	3.50%
en	1.38%	and	1.59%
at	1.34%	ing	1.15%
ou	1.29%	her	0.82%
ed	1.26%	hat	0.65%
ha	1.25%	his	0.60%

평문	빈도
tha	0.59%
ere	0.56%
for	0.55%
ent	0.53%
ion	0.50%
ter	0.46%
was	0.46%
you	0.43%
ith	0.43%
ver	0.43%
all	0.42%
wit	0.39%
thi	0.39%

CR YP TO LO GY

곱셈 암호

- 암호 알고리즘 : 평문에 키를 곱함.
- 복호 알고리즘 : 암호문을 키로 나눔. 즉 키의 역원을 곱함
  - 역원이 존재하려면 키는 Z_{26}^* 의 원소. 키 공간이 작음.



Affine 암호

› 시프트 암호 방식의 K를 더하는 수식을 곱셈으로 한다면

$C \equiv M \times K \bmod 26$

$M \equiv C \times K^{-1} \bmod 26$

– 이 때 암호 문자 M 이 평문 문자 C로 유일하게 복원되어야 하므로

$gcd(K, 26) = 1$ ※ $gcd(a,m)=1$ 이면 modulus m 에 대한 a의 역원이 존재함.

K = 1,3,5,7,9,11,15,17,19,21,23,25 12개 → 키공간이 적어 취약함

› 키를 추가하여 개선 : $C \equiv K_1 M + K_2 \bmod 26$, $K_1, K_2 \in Z_{26}$

(K_1 =1 이면 단순 시프트 암호)

$K_1 M \equiv C - K_2 \bmod 26$ ※ $ax = b \bmod m$ 에서 $gcd(a,m)=1$ 이면 유일한 해 x 존재함

– Affine 암호방식도 암호문이 유일한 평문으로 복원되어야 하므로 $gcd(K_1, 26) = 1$

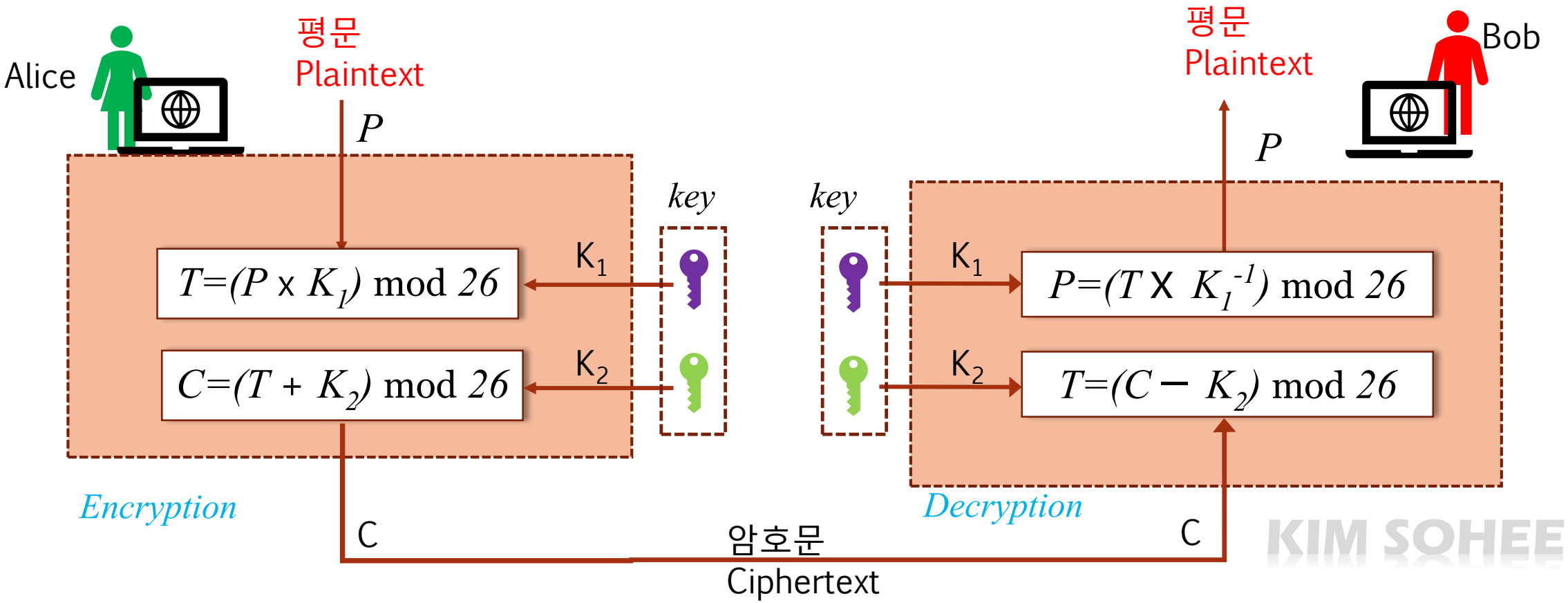
– 12개의 K_1 과 26개의 K_2의 조합이 키가 될 수 있으므로 키 숫자는 12*26=312

CR YP TO LO GY

KIM SOHEE

Affine 암호

› K_1의 키는 Z_{26}^* 의 원소, K_2의 키는 Z_{26} 의 원소. 키 공간은 12x26



(교재)예제3.3

› 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

› i : 8 x 3 + 15 => 39 ≡ 13 mod 26

› n : 13 x 3 + 15 => 54 ≡ 2 mod 26

› f :

CR
YP
TO
LO
GY

KIM SOHEE

동음이의 환자 암호(단성 암호화)

- 평문 문자를 여러 개의 다른 암호문 문자로 암호화
  - 암호문 부호(문자개수보다 많은 부호가 생성)의 빈도 통계를 혼동시킴
  - 암호문 부호의 빈도수를 균일하게 하는 것이 목적. 일-대-다 대응
- 영문자 26개를 1000개의 부호 중 하나로 암호화 할 때
  - 문자 A는 8.2% 빈도 → A를 암호화 하는데 82개를 할당
  - 문자 B는 1.5% 빈도 → B를 암호화 하는데 15개를 할당
  - 문자 C는 2.8% 빈도 → C를 암호화 하는데 28개를 할당
- 암호화 할 때 해당 문자와 대응되는 그룹의 암호문 부호를 무작위로 선택.
- 문제점 : 2문자 , 3문자 연속의 빈도 분석은 가능.

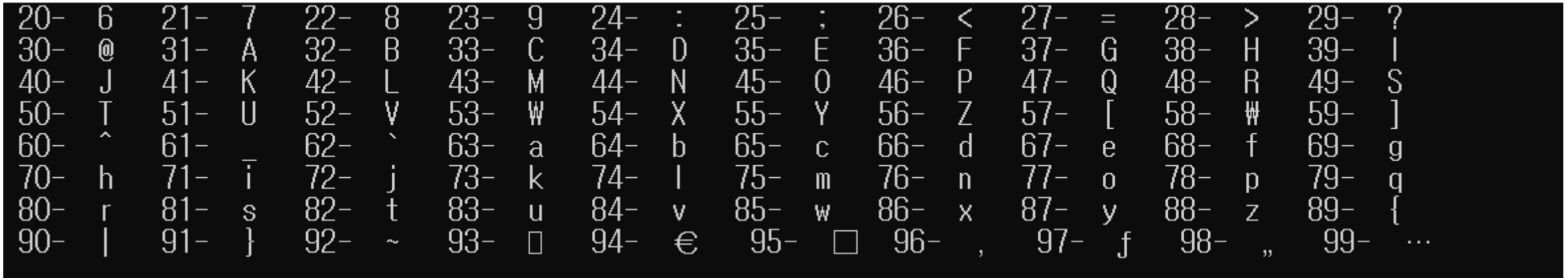
(교재)예제3.4 - 동음이의 환자 암호표

평문	빈도	암호문 부호(할당 숫자)
a	8.2%	44,35,12,38,01,29,56,20
b	1.5%	04
c	2.8%	11,95
d	4.3%	64,71,47,39
e	12.7%	48,25,19,72,80,91,93,02,92,82,79,58,97
f	2.2%	21,30
g	2%	81,18
h	6.1%	03,59,49,70,31,17
i	7%	27,42,07,83,90,60,32
j	0.2%	52
k	0.8%	96
l	4%	61,69,51,53
m	2.4%	50,34

평문	빈도	암호문 부호(할당 숫자)
n	6.7%	89,84,73,78,68,98
o	7.5%	67,41,62,46,43,33,16
p	1.9%	06,43
q	0.1%	10
r	6%	13,66,86,88,63,36
s	6.3%	77,94,09,87,45,22
t	9.1%	65,55,76,23,85,74,54,57,14
u	2.8%	08,15,99
v	1%	24
w	2.3%	75,40
x	0.1%	37
y	2.0%	26,05
z	0.1%	28

[문제]

› hello elle high 를 암호화 해보자.



20-	6	21-	7	22-	8	23-	9	24-	:	25-	;	26-	<	27-	=	28-	>	29-	?
30-	@	31-	A	32-	B	33-	C	34-	D	35-	E	36-	F	37-	G	38-	H	39-	I
40-	J	41-	K	42-	L	43-	M	44-	N	45-	O	46-	P	47-	Q	48-	R	49-	S
50-	T	51-	U	52-	V	53-	W	54-	X	55-	Y	56-	Z	57-	[	58-	₩	59-	]
60-	^	61-	_	62-	`	63-	a	64-	b	65-	c	66-	d	67-	e	68-	f	69-	g
70-	h	71-	i	72-	j	73-	k	74-	l	75-	m	76-	n	77-	o	78-	p	79-	q
80-	r	81-	s	82-	t	83-	u	84-	v	85-	w	86-	x	87-	y	88-	z	89-	{
90-	|	91-	}	92-	~	93-	□	94-	€	95-	□	96-	‚	97-	ƒ	98-	„	99-	…

CR
YP
TO
LO
GY

KIM SOHEE

다표식 환자 암호

› 언어의 통계학적 성질을 없애기 위한 방식.

› Vigenere (비즈네르) 암호 : 위치 의존성을 이용

– (교재)예제3.5 : 평문 this crypto system 를 key 단어 security로 암호화

평문	t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m
키워드	s	e	c	u	r	i	t	y	s	e	c	u	r	i	t	Y
암호문	L	L	K	M	T	Z										

– 참고

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

Vignere 암호 방식

› 키워드 길이가 d 일 때 , 키 공간의 크기 : 26^d

- d = 5 일 때, 26^5 → 약 10^7
- d = 13 일 때, 26^{13} → 약 4.2×10^{39}

› 키워드의 길이를 알게 되면 소모적 공격이 가능하다.

CR
YP
TO
LO
GY

KIM SOHEE

Playfair 플레이페어 암호

- 5 x 5 의 25자 영문자(J는 제외)를 임의로 나열하여 전처리후 암호화 한다.
- 평문 문자를 두 문자씩(바이그램) 작동시킨다.
- 예 : 평문 NATTERJACK TOAD 에 대한 전처리
  - 1. J를 I로 대체한다. → NATTERIACKTOAD
  - 2. 문자를 2개씩 나눈다. → NA TT ER IA CK TO AD
  - 3. 같은 문자가 있는 짝은 사이에 'Z'(임의 문자)를 삽입하고 짝을 재구성한다. → NA TZ TE RI AC KT OA D
  - 4. 홀수 문자 개수이므로 마지막에 'Z' '(임의 문자) 를 추가 한다.

    → NA TZ TE RI AC KT OA DZ

CR YP TO LO GY

KIM SOHEE

Playfair 플레이페어 암호

› 전처리 결과 암호화 하기
› 플레이페어 암호표-예

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

플레이페어 스퀘어

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

– 같은 행이면 오른쪽 문자, 같은 열이면 아래 문자로 대체한다.

– NA TZ TE RI AC KT OA DZ → DN DW SR HF CG FS PT BD

KIM SOHEE

CR YP TO LO GY

(교재)예제3.7

› 평문 INFORMATION SECURITY 를 아래 플레이페어 암호표로 암호화 하자.

(단, J → X , 기수문자 짝 X로 한다.)

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

› IN FO RM AT IO NS EC UR IT YX

› → TO HN DU SI AW VF CL GI ZY

› 플레이페어 암호 특징

- 키공간의 크기 25!
- 문자의 빈도수를 숨길 수 있으나 두문자의 빈도를 테스트하는 공격은 가능하다.

CR YP TO LO GY

KIM SOHEE