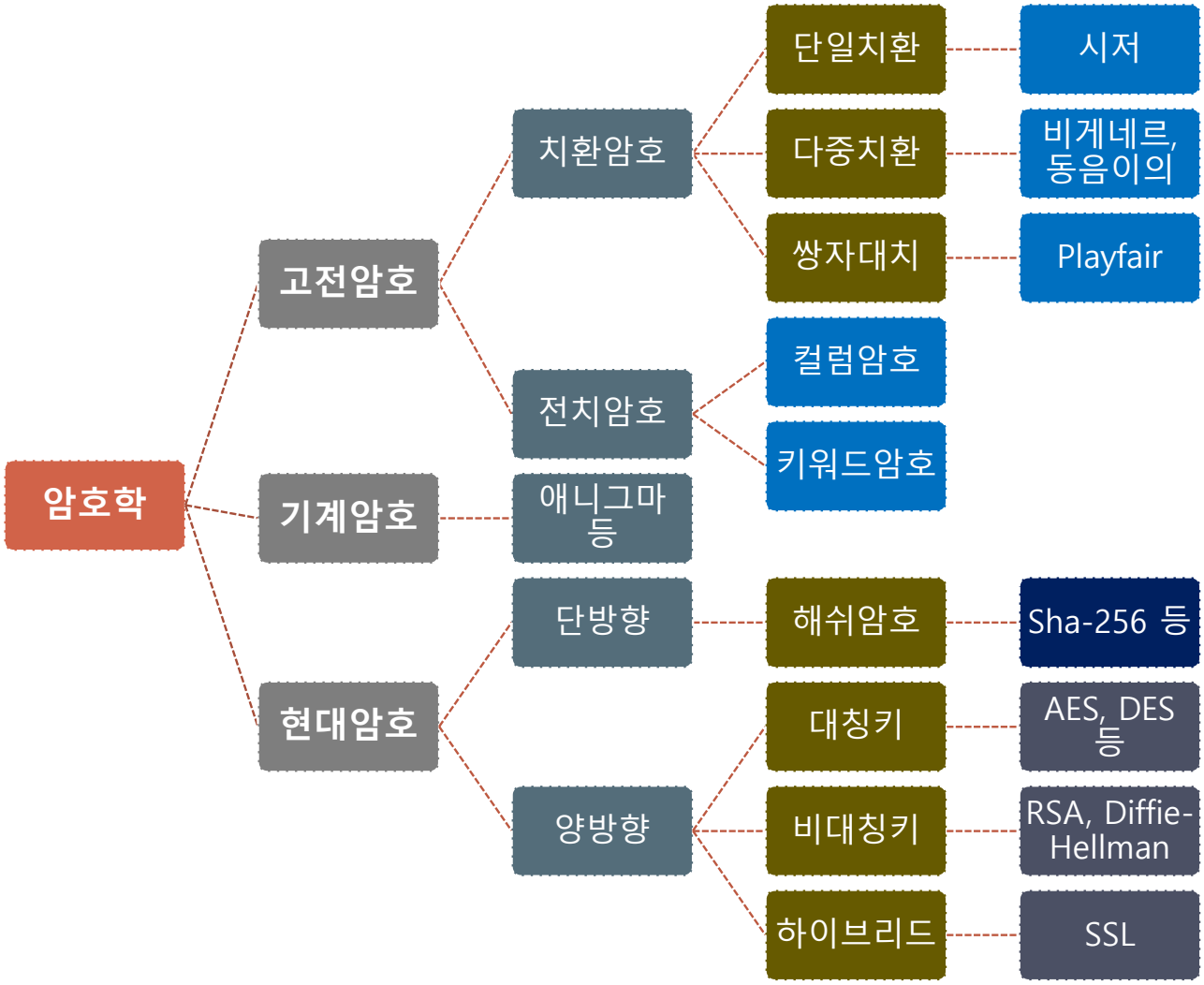
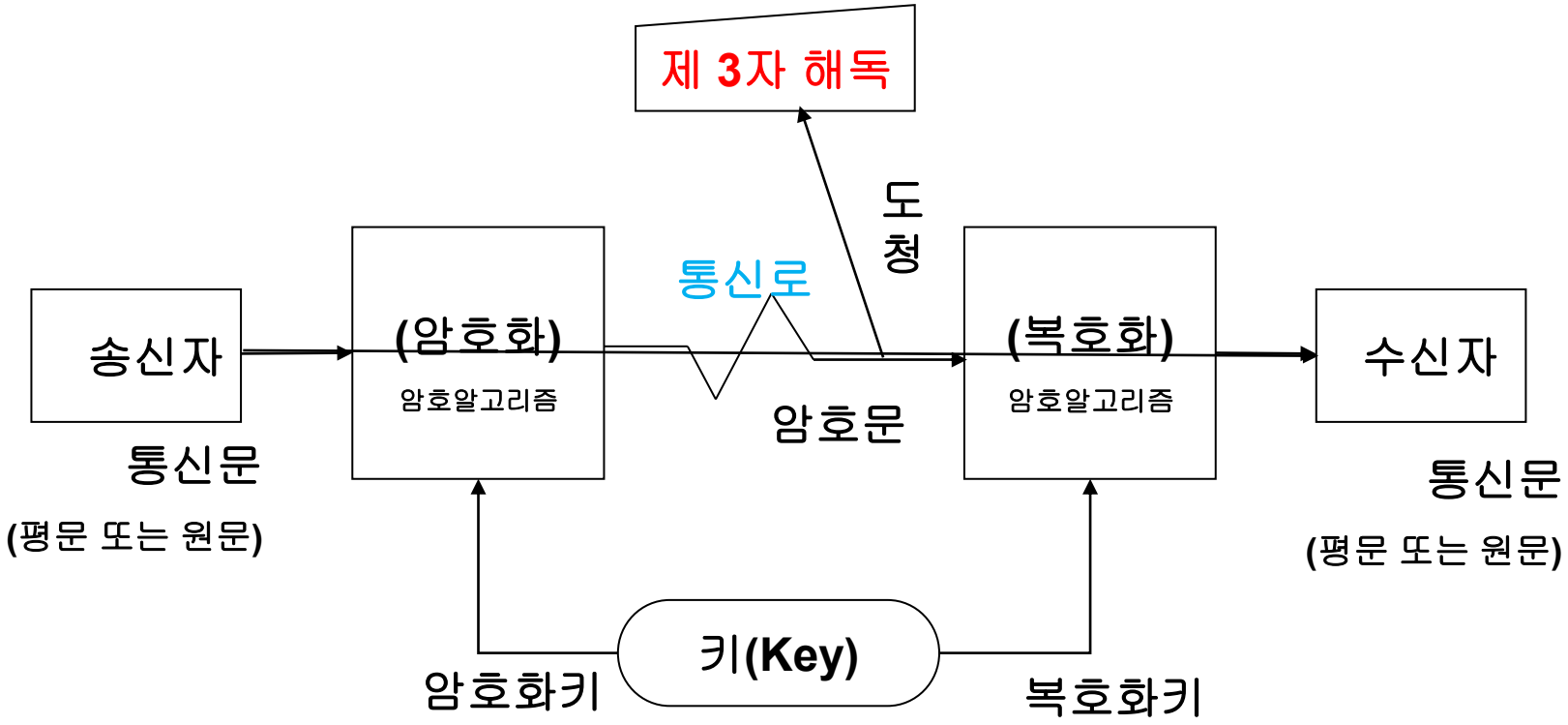
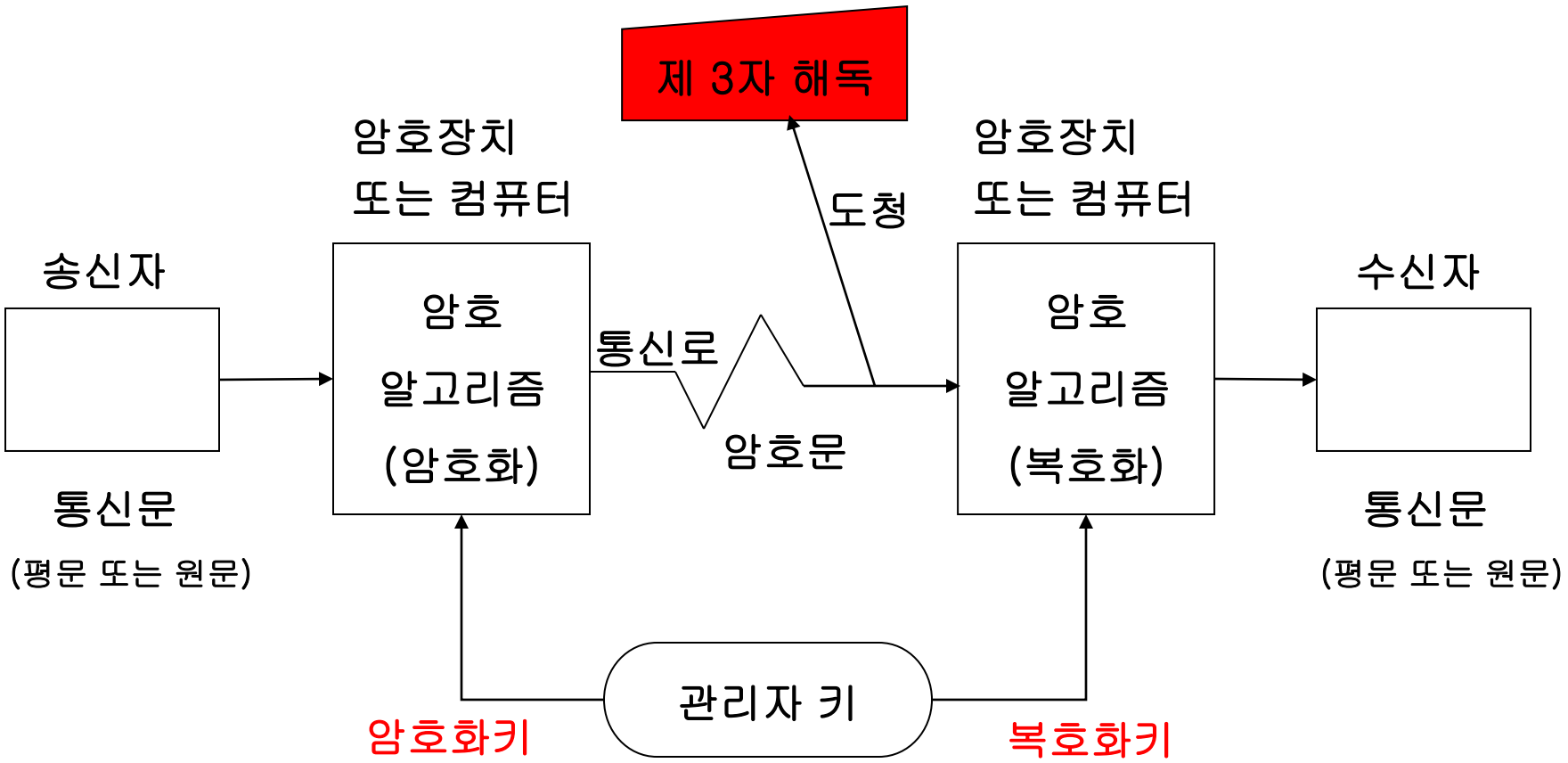
암호학의 분류


암호학
고전암호
치환암호
단일치환
시저
다중치환
비게네르, 동음이의
쌍자대치
Playfair
전치암호
컬럼암호
키워드암호
기계암호
애니그마 등
현대암호
단방향
해쉬암호
Sha-256 등
양방향
대칭키
AES, DES 등
비대칭키
RSA, Diffie-Hellman
하이브리드
SSL


제 3자 해독
도청
통신로
송신자
(암호화)
암호알고리즘
암호문
(복호화)
암호알고리즘
수신자
통신문
(평문 또는 원문)
통신문
(평문 또는 원문)
키(Key)
암호화키
복호화키


제 3자 해독
암호장치
또는 컴퓨터
도청
암호장치
또는 컴퓨터
송신자
암호
알고리즘
(암호화)
통신로
암호문
암호
알고리즘
(복호화)
수신자
통신문
(평문 또는 원문)
통신문
(평문 또는 원문)
관리자 키
암호화키
복호화키

[개괄적 비밀 통신 절차]

암 호 학 I

- 고 전 암 호 -

1. 암호용어 정리

- **암호(cryptography) :** 평문을 해독 불가능한 형태로 변형하거나
  또는 암호화된 통신문을 해독 가능한 형태로 변환하기 위
  한 원리, 수단, 방법 등을 취급하는 기술 또는 과학
- **평문(plain text,원문) :** 송신자가 수신자에게 보내고 싶은 보통의 통신문

- **암호화(encryption) :** 평문을 암호문(cipher text)으로 변환하는 조작.
  - Encoding
- **복호화(decryption) :** 암호문을 본래의 평문으로 바꾸는 조작
  - 정당한 수신자가 정당한 절차를 통해 평문을 복원하는 과정. Decoding

- **암호 해독 :** 부당한 제 3자(도청자)가 다른 수단을 통해 추정하는 것
- **키(key) : 암호 알고리즘에 의한 변환을 제어하는 요소**

2. 암호학의 발달과정

- 제 1단계(고대~19세기 말)
  - 단순한 문자 대입방법
  - 암호문의 통계적 특성을 분석하여 해독가능
  - 예) 시저 암호(Caesar cipher), 비게네르 암호(Vigenere cipher), 뷰포트 암호(Beaufort cipher) 등

- 제 2단계(20세기 초~1940년대 말)
  - 복잡한 기계(로터기기:Rotor Machine)를 이용하여 암호 알고리즘 실현
  - 암호문 해독에 계산량이 증가, 해독을 위해 컴퓨터 발달
  - Enigma(독일, 앨런튜링에 의해 해독됨), M-209(미국) 등

- 제 3단계(1940년대 말~현재: 현대 암호학의 시대)
  - C.E. Shannon의 논문 발표시점으로부터 시작
  - 1970년대 초 전자 산업의 발달로 복잡도가 높은 암호 알고리즘 실현 가능.
  - 암호문 : 문자가 아닌 대단히 긴 이진코드(비트열)

3. 고전암호 시스템

1) 치환 암호 (substitution cipher; 대치 암호)

① 단순 대치 암호(simple substitution cipher)
② 동음이의 대치 암호 (homophonic substitution cipher)
③ 쌍자 대치 암호(polygram substitution cipher)
④ 모든 암호알고리즘의 기본

2) 전치암호 (transposition cipher;)

① 문자열의 순서를 바꿈
② 엄밀히 따지면 치환암호의 한 종류

3-1. 단순 대치 암호

- 평문과 암호문의 각 문자가 일대일 대응되는 암호
  - S를 26개의 영문 알파벳들의 집합이라 하고
  - S 위에서의 일대일 대응함수 $f: S \rightarrow S$ 는 단순 대치 암호의 키가 됨.

  평문 $M = m_1 m_2 \cdots$

  암호문 $C = f(m_1) f(m_2) \cdots$

- 예)

알파벳문자열	ABCDEFGHIJKLMNOPQRSTUVWXYZ
f:	⇩
암호화문자열	HARPSICODBEFGJKLMNQTUVWXYZ

M = RENAISSANCE

C = NSJHDQQHJRS

시저암호

- 영문자 알파벳 각각을 k 자리 뒤의 다른 알파벳으로 대치하는 것.
- 각 문자를 0부터 25까지의 정수로 대응시켰을 때, 시저 암호는 0부터 25까지의 정수들의 집합 A에서 A로 가는 함수로 표현.

  $f(a) \equiv (a+k) \bmod 26$

- 예) k=3 일 때,
  - M = RENAISSANCE

  - C = UHQDLVVDQFH
  - M = NEVER TRUST BRUTUS
  - C = QHYHU WUXVW EUXWXV

시저암호의 해독

- VLA SP를 해독해보자
- 키값은 1~25뿐이다(Why?)

암호문	VLA SP
+1	WMB TQ
+2	XNC UR
+3	YOD VS
+4	ZPE WT
⋮	⋮
+20	PFU MJ
+21	QGV NK
+22	RHW OL
+23	SIX PM
+24	TJY QN
+25	UKZ RO

- 해독을 막을 수 있는가?
- 암호를 어렵게 만들자!
  - 어느정도?
  - 6시 이후에 해독이 될 수 있도록

시저암호의 개선

- 사용할 단어 : JEJUEDUCATION
  암호화할 문장 : NEVER TRUST BRUTUS
- 단어 JEJUEDUCATION에서 반복되는 문자가 있으면 처음 나오는 문자 외에는 모두 삭제
- JEUDCATION
- 윗줄에 평문 문자인 알파벳을 순서대로 쓰고, 아랫줄에 키를 첫 번째 위치부터 쓴다

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
J E U D C A T I O N

- 키에 속하는 문자를 제외한 알파벳의 나머지 문자를 순서대로 쓴다.

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

- HCVCP RPSQR EPSRSQ
- 문제점 : 뒷부분은 평문과 암호문이 동일

시저암호의 개선

- 어느 부분부터 평문 문자와 암호 문자가 같아지는 문제점을 없애고, 좀더 복잡하게 하려면 단어와 숫자 키를 동시에 사용
- 숫자 키 7과 단어 LINUXANDWINDOWS를 동시에 사용해서 암호화해 보자
- 윗줄에 평문 문자인 알파벳을 쓰고, 아랫줄에 숫자 키인 7만큼 오른쪽으로 이동하여 단어 키를 쓴다.

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
L I N U X A D W O S

- 단어 키에서 사용된 문자를 제외한 알파벳의 나머지 문자를 순서대로 쓴다. 평문 문자 Z까지 채워 넣었으면 다시 A부터 시작한다. 모두 채우면 암호화 표가 완성된다

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

- NEVER TRUST BRUTUS → DVGVB EBFCE QBFEFC

비게네르(Vigenere;비즈네르) 암호

- 7, 1, 11, 19의 키로 C PROGRAMMING을 암호화해보자.

C	P	R	O	G	R	A	M	M	I	N	G
7	1	11	19	7	1	11	19	7	1	11	19

비게네르표

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

I PBGMRKESIXY

비게네르(Vigenere;비즈네르) 복호

I	P	B	G	M	R	K	E	S	I	X	Y
7	1	11	19	7	1	11	19	7	1	11	19
C	P	R	O	G	R	A	M	M	I	N	G

비게네르표

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

비게네르암호의 확장

- 일반적으로 다음과 같은 베게네르표를 사용한다

	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

- 평문 : DOGS
- 키 : PLUG
- 암호문 : SZAY

3-2. 동음이의 대치 암호

- 평문 각 문자에 여러 개의 문자가 대응하는 암호
- 평문 각 문자의 빈도 분포가 대치된 암호문의 빈도 분포와 동일하게 되는 단순 대치 암호의 단점을 보완
- 통계적 특성이 줄어들긴 했으나 암호해독이 가능
- 예) 26개 영문자를 0부터 99까지 정수로 대치하여 암호화하는 경우

  A 17 19 34 41 56 60 67
  I 08 22 53 65 88 90
  L 03 44 76
  N 02 09 15 27 32 40 59
  O 01 11 23 28 42 54 70
  P 33 91
  T 05 10 20 29 45 58 64

  이때 영문자 각각에 할당된 정수 개수는 평문 각 문자의 빈도에 비례하며, 모든 정수는 하나의 영문자에만 할당됨.

  M = P L A I N P I L O T

  C = 91 44 56 65 59 33 08 76 28 78

3-2. 동음이의 대치 암호사례(정리필요)

- **일본이 쩔쩔맨 K암호**
- 비밀결사 조직 고려공산청년회 책임비서 김재명
- 가로세로 10행씩의 바둑판 모양을 만들고, 맨 윗줄과 맨 왼쪽줄에 1부터 9까지 숫자를. 가로줄은 올림 순서로, 세로줄은 내림 순서로 적었다.
- 둘째, 열쇳말을 만들었다. 세 음절로 이뤄진 열쇳말을 정해, 교신 당사자끼리 공유했다. 예컨대 공청 중앙부와 함남도위원회 사이의 교신 열쇳말은 '금강산'이었다. 이 열쇳말에서 중요한 것은 음절이 아니라 '음소'였다.
  - '금강산'은 ㄱㅡㅁㄱㅏㅇㅅㅏㄴ이라는 9개 음소로 분해되고, 각 음소는 숫자판의 첫 번째 세로줄에 차례대로 배치됐다.
- 자음은 ㄱㄴㄷㄹㅁㅂㅅㅇㅈㅊㅋㅌㅍㅎ 순으로, 모음은 ㅏㅑㅓㅕㅗㅛㅜㅠㅡㅣ 순으로 1열의 문자에 이어 순서대로 여백을 채운다
- '금강산'은 강원도, 전라북도, 함경남도 '백두산'(전라남도·충청남북도·함경북도), '남극성'(황해도·경기도·경상남도), '대동강'(평안남북도·경상북도·만주총국)이라는 열쇳말을 사용했다.
- 셋째, 말하려는 문장의 음소를 숫자판에서 추출한다. 하나의 음소는 둘 이상 될 수 있다. 예를 들어 'ㅅ'은 여섯 곳에 분포했다. 세로 9행과 가로 7행, 세로 8행과 가로 9행, 세로 7행과 가로 3행, 세로 6행과 가로 7행, 세로 3행과 가로 1행, 세로 1행과 가로 6행에 있다. 이 중에서 아무것이나 임의로 선택해도 무방함.

	1	2	3	4	5	6	7	8	9
9	ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ
8	ㅡ	ㅣ	ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ
7	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ	ㅊ	ㅋ	ㅌ	ㅍ
6	ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ
5	ㅏ	ㅑ	ㅓ	ㅕ	ㅗ	ㅛ	ㅜ	ㅠ	ㅡ
4	ㅇ	ㅈ	ㅊ	ㅋ	ㅌ	ㅍ	ㅎ	ㅏ	ㅑ
3	ㅅ	ㅇ	ㅈ	ㅊ	ㅋ	ㅌ	ㅍ	ㅎ	ㅏ
2	ㅏ	ㅑ	ㅓ	ㅕ	ㅗ	ㅛ	ㅜ	ㅠ	ㅡ
1	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ	ㅊ

"73556 14782 97486861544147516448"

ㅅㅗㄱ

"속히 상경하라"

3-3.쌍자 대치 암호

- 한문자 씩 변환하는 방법의 문제점
  - 알파벳 빈도수 분석에 의해 쉽게 해독 됨
- 한번에 여러 개의 문자를 암호화함으로써 각 문자에 대한 빈도를 암호문에서 무의미하게 하여 암호 해독을 더욱 어렵게 하는 암호
  - 현대암호학의 블록암호 알고리즘의 기본 아이디어
- **Playfair 암호화**
  - 두 글자 씩 묶어 암호화

Playfair 암호(1)

블럭암호기

- **L. Playfair**의 이름을 따라 명명된 두 문자 대치 암호로 **C. Wheatstone**이 개발
- 제 **1**차 세계대전 당시 사용된 암호
- 키는 **25**개 문자의 **5 × 5** 행렬, **J**는 **I**와 동일

Playfair 암호의 키

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

Playfair 암호(2)

① m_1과 m_2가 같은 행에 존재 : c_1과 c_2는 m_1과 m_2의 오른쪽의 문자로 대치하며 이때 첫번째 열은 마지막 열의 오른쪽 문자로 함.

② m_1과 m_2가 같은 열에 존재 : c_1과 c_2는 m_1과 m_2의 밑의 문자로 대치하며 첫번째 행은 마지막 행 밑의 문자로 간주

③ m_1과 m_2가 다른 열과 행에 존재 : c_1과 c_2는 m_1과 m_2를 포함하는 사각형의 모퉁이 문자로 하되 c_1을 m_1과 같은 행에, c_2는 m_2와 같은 행의 문자로 함.

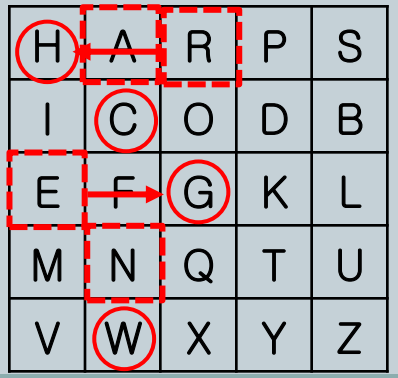
④ $m_1 = m_2$ 일 경우 : m_1과 m_2 사이에 모조 문자 X를 삽입

⑤ 문자의 수가 홀수일 경우 : 평문의 끝에 모조문자 X를 추가

예) 평 문 : RE NA IS SA NC EX

암호문 : HG WC BH HR WF GV

복호는 역과정을 거치면 됨



4. 전치(Transposition)암호

- 문자를 재배열하여 만든 암호
  - ILOVEYOU → OVEYOUIL
- 평문을 d개의 문자단위로 나누고, d개의 문자에 대한 재배치는
- $Z_d=\{1,2,\ldots,d\}$, $f: Z_d \rightarrow Z_d$는 Z_d위에서의 치환이라 할 때,

키 : $K = (d, f)$ d=마디수, f=치환함수

암호화 : 평 문 : $M= m_1 \ldots m_d \quad m_{d+1} \ldots m_{(2d)} \ldots$

암호문 : $C=m_{f(1)} \ldots m_{f(d)} \; m_{d+1f(1)} \ldots m_{2df(d)} \ldots$

- 평문의 각 문자의 빈도가 암호문에서도 같게 되어 전이 암호를 사용한 사실을 암호 해독자가 알 수 있음.

예) d=4, $C= m_{(2)} m_{(4)} m_{(1)} m_{(3)}$

RENA ISSA NCE

암호문→ EARN SAIS CNE

전치암호의 예(컬럼암호화)

- 암호화할 문장 : LINUX PROGRAMMING LANGUAGE
- 적당한 행렬(여기서는 4x6)에 가로 방향으로 문장을 나열해보자

L	I	N	U	X	P
R	O	G	R	A	M
M	I	N	G	L	A
N	G	U	A	G	E

L	I	N	U	X	P
R	O	G	R	A	M
M	I	N	G	L	A
N	G	U	A	G	E

세로로 쓰고
가로로 읽음

- 첫 번째 열을 시작으로 세로 방향으로 읽어 표현하면?
- LRMNIOIGNGNUURGAXALGPMAE
- 한번 더 해주면 더욱 어려워짐(암호문을 다시 행렬에 대입)

L	R	M	N	I	O
I	G	N	G	N	U
U	R	G	A	X	A
L	G	P	M	A	E

L	R	M	N	I	O
I	G	N	G	N	U
U	R	G	A	X	A
L	G	P	M	A	E

세로로 쓰고
가로로 읽음

- LIULRGRGMNGPNGAMINXAOUAE

전치암호의 예(키워드암호화)

- 암호화할 문장: HEAVEN HELPS THOSE WHO HELP THEMSELVES
- NETWORK라는 단어를 키워드로 사용해 전치 암호화
  - NETWORK의 각 문자 N, E, T, W, O, R, K에 알파벳 순으로 일련번호를 부여
  - 그 아래에 원문서의 문자를 차례대로 적는다
  - 칼럼의 길이는 키워드 단어의 문자 길이와 동일(여기서는 7)

키워드	N	E	T	W	O	R	K
순서	3	1	6	7	4	5	2
	H	E	A	V	E	N	H
	E	L	P	S	T	H	O
	S	E	W	H	O	H	E
	L	P	T	H	E	M	S
	E	L	V	E	S	Z	Z

알파벳 순으로 부여된 번호 순서에 따라 컬럼방향으로 읽어보자

- 암호문: elepl hoesz hesle etoes nhhmz apwtv vshhe