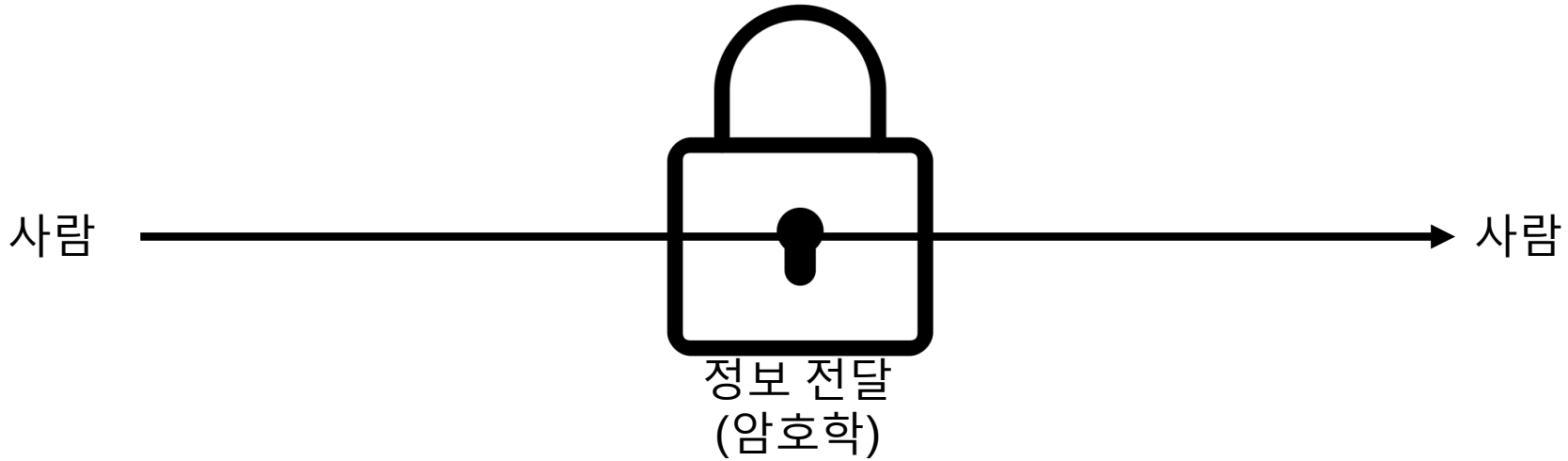

암 호 학
COLONY - 정상지

○ 목차

1) 암호학

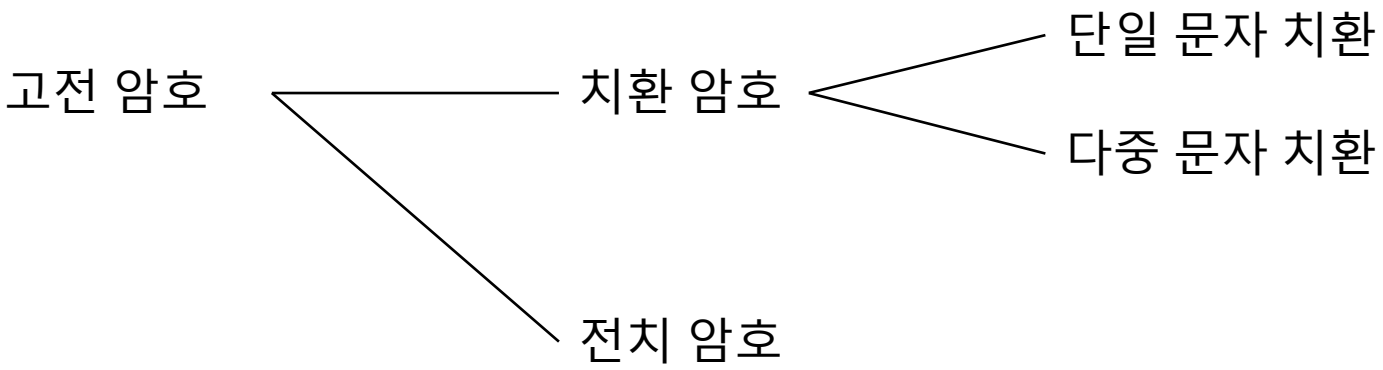
- 암호학은 정보를 보호하기 위한 언어학적 및 수학적 방법론을 다루는 학문
- 평문(Plain text)의 메시지를 변환하여 암호문을 만드는 암호화 과정과 반대로 암호문을 평문으로 만드는 복호화 과정으로 나뉨



2) 고전 암호

- 비교적 간단한 기계와 손 등으로 암복호화를 수행하던 암호

- 치환 : 평문 문자를 다른 문자로 바꾸는 것
- 전치 : 평문 문자의 위치를 바꾸는 것

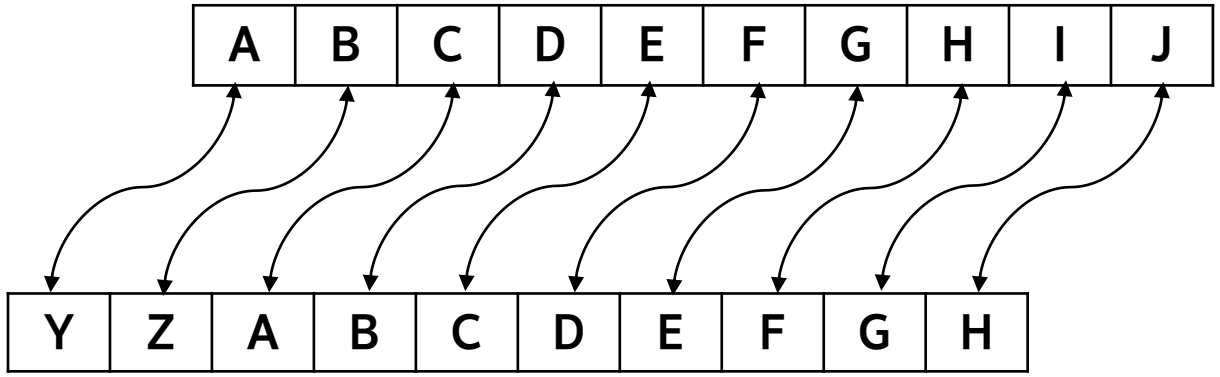


2) 고전 암호

(1) 치환 암호

① 단일 문자 치환 암호

- 단일 문자를 다른 문자나 기호로 치환하여 암호문을 만드는 방법
- 아래와 같이 각 알파벳을 일정한 거리만큼 밀어서 치환하는 카이사르 암호
- 글자를 기호로 치환하는 프리메이슨 암호(돼지우리 암호)



2) 고전 암호

(1) 치환 암호

② 다중 문자 치환 암호

- 평문의 한 문자를 암호문에서 여러 종류의 문자로 치환이 가능
- 미리 정해진 키워드를 통해 평문을 암호화 하는 비제네르 암호

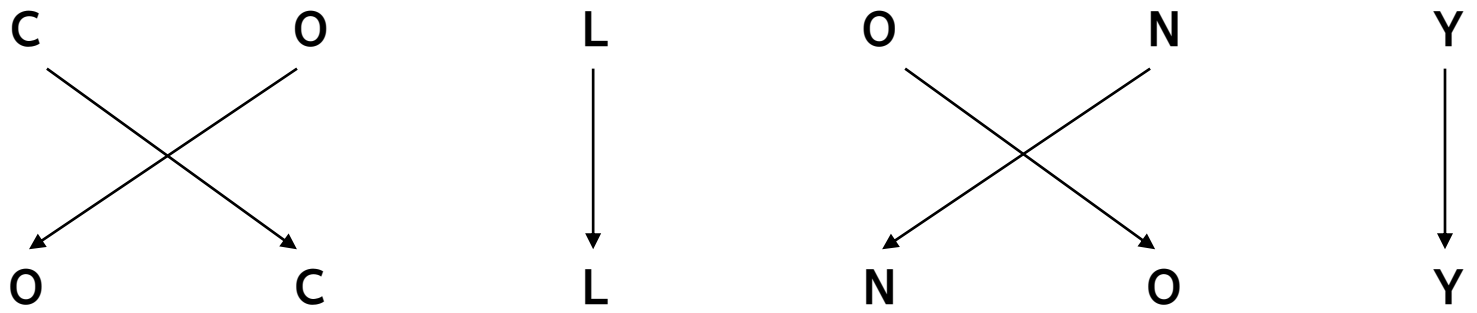
키워드	W	I	N	W	I	N	W	I	N	W	I	N	W	I
평문	C	O	L	O	N	Y	F	I	G	H	T	I	N	G
암호문	Y	W	Y	K	V	L	B	Q	T	D	B	V	J	O

	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	D
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	C
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	B
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

2) 고전 암호

(2) 전치 암호

- 평문을 구성하는 문자들의 순서를 재배열하여 만드는 암호문
- 정해진 길이를 나눈 후 규칙을 적용하여 블록 안의 문자들을 재배치
- 밑의 전치 암호 방법 이외에도 나무봉을 이용한 스키테일 암호도 존재



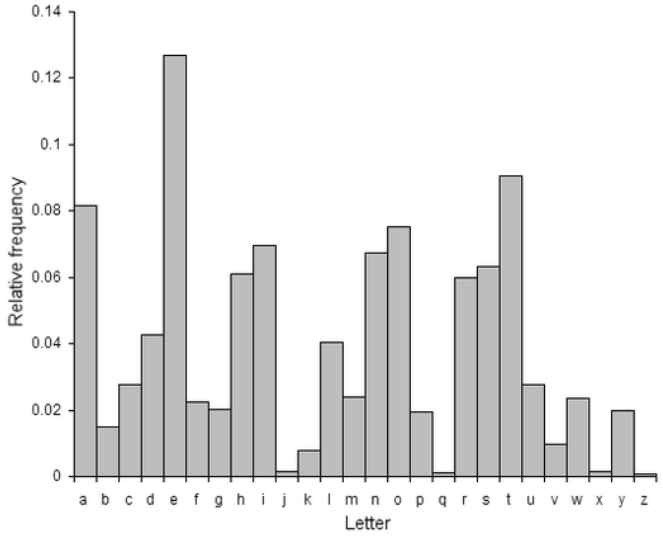
2) 고전 암호

(3) 고전 암호 공격

- 전수 키 탐색 공격 : 평문과 암호문을 알 때, 키 공간을 전부 탐색하여 암호문과 같은 암호문을 생성하는 방법

- 빈도수 공격 : 단일 치환 암호의 경우 평문의 문자와 항상 일대일 대응으로 이루어지기 때문에 평문의 특성을 그대로 따라감. 이러한 특성을 따라 평문에서 많이 사용되는 문자를 기준으로 암호문을 복호화하는 방법

- 옆의 표는 영어의 알파벳 사용빈도로 e등의 문자가 많이 사용되는 특성을 따라 빈도수 공격을 시도할 수 있다



3) 현대 암호

- 현대의 고도한 기계나 컴퓨터의 발달로 고전 암호체계가 쉽게 파악
- 현대의 많은 암호 시스템이 혼돈과 확산의 성질을 만족

- 혼돈 : 암호문에서 평문의 특성을 알아내기 힘든 성질 (암호문을 보고 평문 유추가 어려움)
- 확산 : 평문의 작은 변화가 암호문에서 큰 변화로 이어지는 성질

- 비밀 유지를 위한 세가지 특성 : 기밀성, 무결성, 인증
- 기밀성 : 암호화된 데이터를 알 수 없어야 함
- 무결성 : 암호화된 데이터가 원본과 같아야 함
- 인증 : 권한이 있는 사람만 데이터에 접근 가능해야 함

3) 현대 암호

- 대칭키 암호 시스템 : 암호화와 복호화에 같은 키를 사용하는 암호 시스템
- 공개키 암호 시스템 : 공개키로 암호화하여 데이터를 전송하고 해당 데이터를 비밀키로 복호화 하는 암호시스템

대칭키 암호 시스템

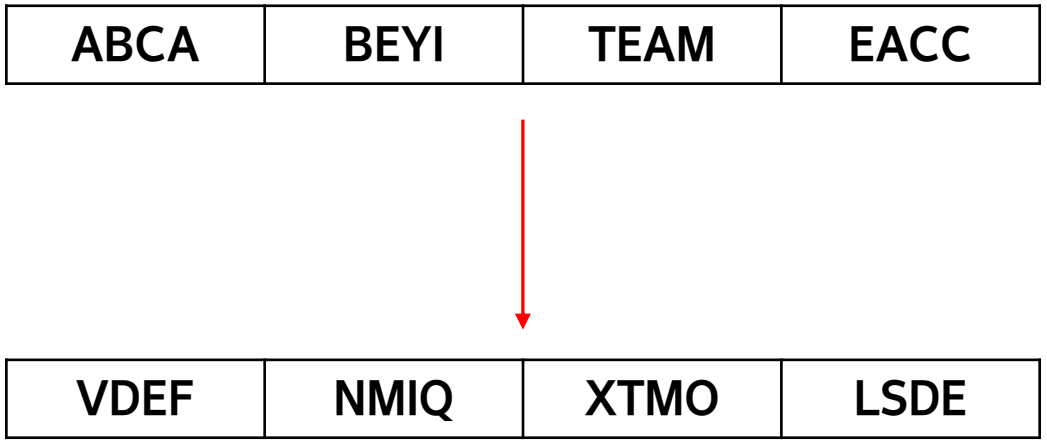
공개키 암호 시스템

4) 대칭키 암호 시스템

- 대칭키 암호 시스템에는 크게 블록 암호와 스트림 암호로 구분

(1) 블록 암호

- 정해진 크기의 블록을 지정하여 블록 단위로 암호화
- 크기에 맞지 않을 경우 평문에 데이터를 추가하는 패딩을 먼저 수행
- 블록 암호의 대표적인 예시로 DES 와 AES가 있습니다

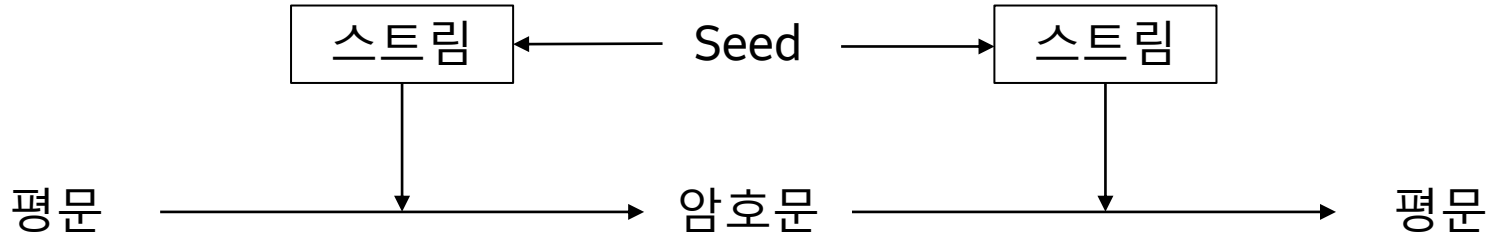


4) 대칭키 암호 시스템

(2) 스트림 암호

- 송신자와 수신자가 공유하는 데이터 스트림을 평문에 XOR하는 암호
- Seed로 불리는 작은 스트림을 공유하고 각각 합의된 함수의 인자로 넣어 스트림을 생성
- 스트림 암호는 단순 연산으로 이루어져 속도가 빠름
- 안전하지 못해 임베디드 기기나 속도가 중요한 환경서 제한적으로 사용

- 평문 암호화 과정 : P(평문) ⊕ X(스트림) = C(암호문)
- 암호문 복호화 과정 : C ⊕ X = P



5) 공유키 암호 시스템

- 송신자는 자신의 공개키로 데이터를 암호화하고 수신자는 자신의 비밀키로 복호화하는 시스템
- RSA 알고리즘은 공유키 암호 시스템 중 가장 보편적으로 사용되는 알고리즘

(1) RSA 알고리즘

- 큰 두 소수의 곱으로 이루어진 합성수를 소인수분해하기 어렵다는 성질을 이용한 알고리즘
- 전자 거래, 금융 거래, 인증서 등 다양한 분야에서 사용되며 대칭키 암호시스템 보다 많은 연산을 필요로 하여 네트워크 통신에는 잘 사용하지 않음

5) 공유키 암호 시스템

(1) RSA 알고리즘

① p와 q의 서로 다른 두 소수를 고르고 두 수를 곱하여 N을 구한다

②1과 (p-1)(q-1) 사이에 (p-1)(q-1)과 서로소인 정수 e 를 구한다

③ d x e를 (p-1)(q-1)로 나누었을 때 나머지가 1인 정수 d 를 구한다

④ M^e % N의 값을 c라고 하며 c와 공개키 <N,e>를 송신한다

⑤ c와 공개키 <N,e>를 수신하여 M=c^d % N 을 통해 복호화한다

(1) RSA 알고리즘

○ MOD는 나머지연산 기호

N = 14
e = 5

공개키 <14,5>

p = 2
q = 7

N = p*q = 14
φ(N) = (p-1)(q-1) = 6
e = 5 (공개키)

M = 3 (평문)
c = M^e MOD N = 5

암호문 c = 5

(e*d) MOD 6 = 1
→ d = 11 (비밀키)

M = c^d MOD N = 3

5) 공유키 암호 시스템

(2) 대칭키 암호 시스템과의 비교

	대칭키 암호 시스템	공유키 암호 시스템
키	하나의 키가 둘 이상의 개체에 공유	한 개체가 공개키 다른 개체가 비밀키
키 개수	개인의 수가 늘어나면 키의 개수가 기하급수적으로 늘어남	N명의 공유키 시스템은 2N개의 키만 필요
장점	속도가 빠름	키 분배가 쉬워 확장 가능성이 크다
단점	키 전달을 위한 안전한 메커니즘 필요 확장성이 용이하지 않음	연산이 많아 알고리즘이 복잡하고 속도가 느림
제공되는 보안서비스	기밀성	부인 방지, 인증

Q&A