SEOULTECH

Confidentiality (기밀성) 실습

2021년도 1학기 **정보보호론 실습**

SeoulTech UCS Lab

Ubiquitous Computing & Security Laboratory

Confidentiality (기밀성) 실습

실습 내용

- 기밀성과 밀집한 관련이 있는 암호의 정의에 대해 학습한다.
- 고전암호에 대해 학습하고, 암호화 및 복호화 실습을 진행한다.

실습 방법

- 실습 PPT 파일과 책을 참고하여 실습문제로 제시된 암호문을 해독한다.

기밀성(Confidentiality)과 암호(Cryptography)

Confidentiality, 기밀성

- 보안의 세 가지 요소 중 기밀성(Confidentiality)은 인가(authorization)된 사용자만 정보 자산에 접근할 수 있는 것을 의미

- 허가되지 않은 사람, 즉 비인가자의 정보에 대한 접근을 막는 역할을 함. 보안과 관련된 많은 시스템과 소프트웨어가 기밀성과 밀접한 관련이 있음.

- 암호가 기밀성의 대표적인 예이다.

Cryptography, 암호

- 평문을 해독 불가능한 형태로 변형하거나, 암호문을 원래의 해독 가능한 상태로 변환하기 위한 모든 수학적인 원리, 수단, 방법 등을 취급하는 기술 또는 과학.

- 허가되지 않은 사람, 즉 비인가자의 정보에 대한 접근을 막는 역할을 함. 보안과 관련된 많은 시스템과 소프트웨어가 기밀성과 밀접한 관련이 있음.

Cryptography, 암호

암호화 알고리즘

- 평문을 암호문으로 만드는 절차

복호화 알고리즘

- 암호문을 평문으로 만드는 절차

암호 알고리즘

- 암호화와 복호화 알고리즘을 합한 알고리즘

그림 2-8 • 암호화와 복호화

실습문제 1

카이사르 암호

1.카이사르 암호

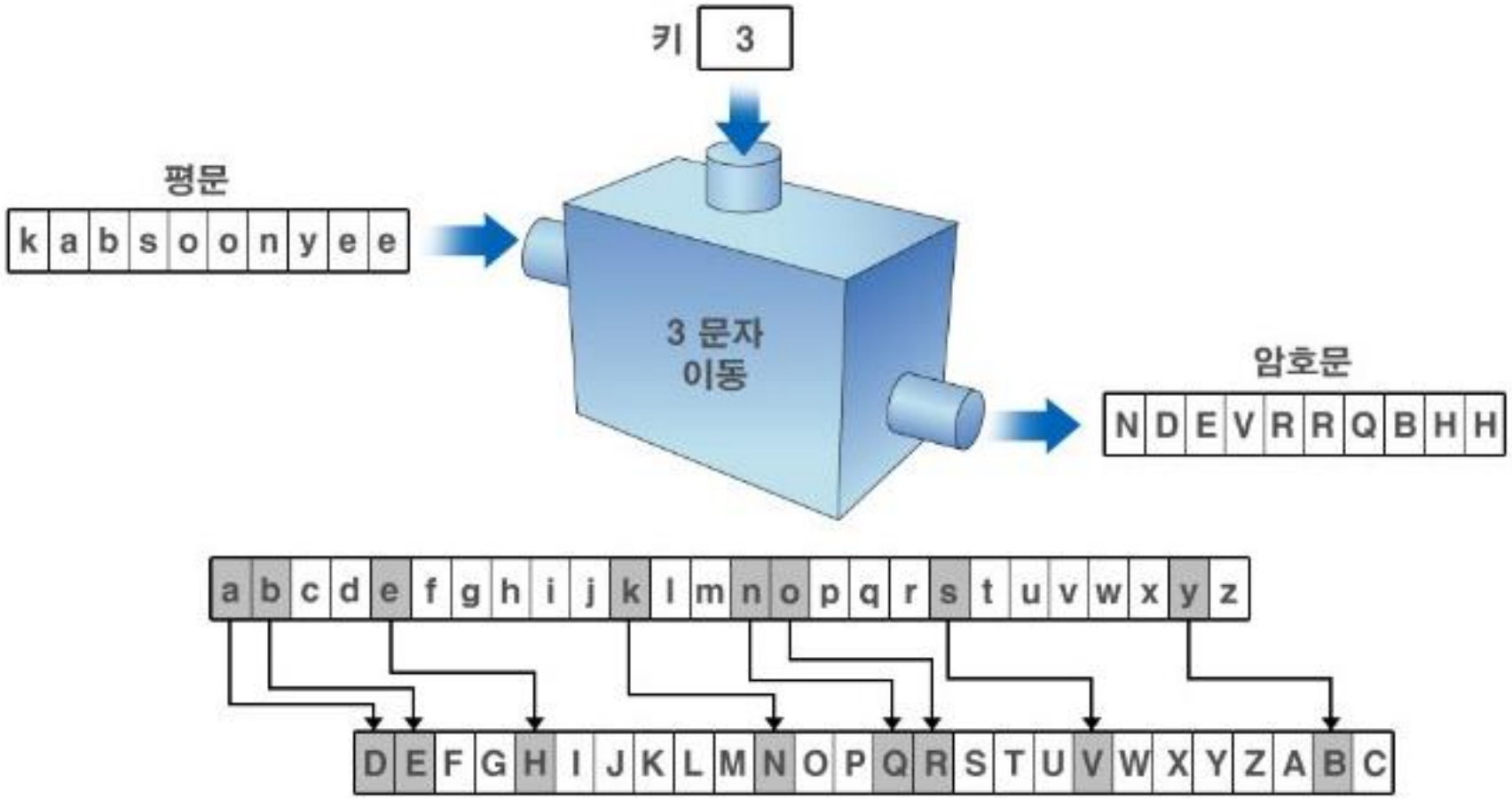
카이사르 암호

로마 시대의 율리우스 카이사르의 이름을 딴 암호로 알파벳의 순서를 키 값의 수 만큼 밀어 글자를 바꾼 이동암호.

키 값이 3이라면 A는 D, B는 E, C는 F 등으로 바뀌고 X는 A로, Y는 B, Z는 C로 바뀌어, " WE WIN " 의 경우 암호화 할 경우 " ZI ZLQ " 가 됨.

원래의 알파벳	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
키가 3일 때의 알파벳	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

카이사르 (이동)암호


키
3
평문
k a b s o o n y e e
3 문자
이동
암호문
N D E V R R Q B H H
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

1.카이사르 암호

카이사르 암호

로마 시대의 율리우스 카이사르의 이름을 딴 암호로 알파벳의 순서를 키 값의 수 만큼 밀어 글자를 바꾼 이동암호.

키 값이 3이라면 A는 D, B는 E, C는 F 등으로 바뀌고 X는 A로, Y는 B, Z는 C로 바뀌어, " WE WIN " 의 경우 암호화 할 경우 " ZI ZLQ " 가 됨.

원래의 알파벳	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
키가 3일 때의 알파벳	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

1.카이사르 암호

Q1. 다음 암호를 Key 가 5인 카이사르 암호로 암호화 하시오.

Watch out for the assassin tonight

Q2. 다음은 카이사르 암호로 암호화한 문장이다. 암호화에 사용된 키의 값과 평문 문장을 찾으시오.

ijustfoundouttheonlyreasonthatyoulovinme

실습문제 2

춤추는 사람 그림 암호

2. 춤추는 사람 그림 암호

춤추는 사람 그림 암호

- 셜록홈즈에 등장한 암호로 1대1로 치환되는 대치 암호

- 대치암호는 알파벳 한 문자와 어떠한 문자 하나를 1대 1로 대치시키는 암호화 기법

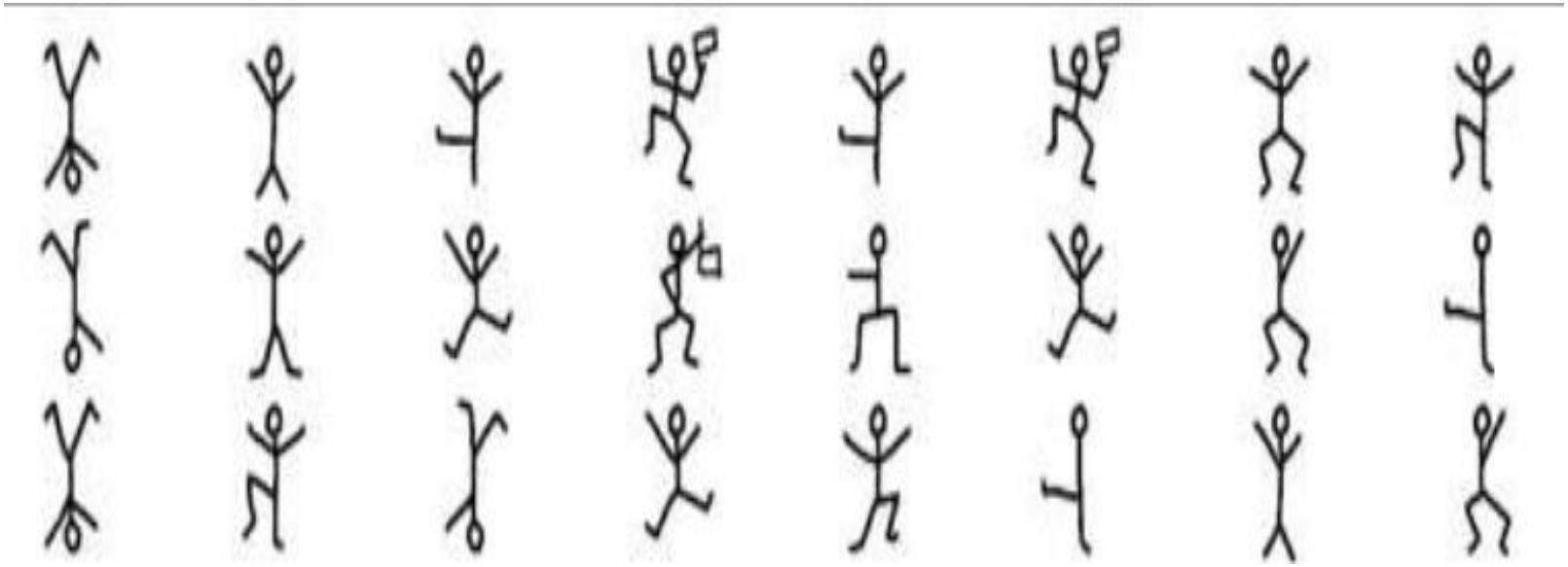
 = A

 = E

2. 춤추는 사람 그림 암호

춤추는 그림 암호

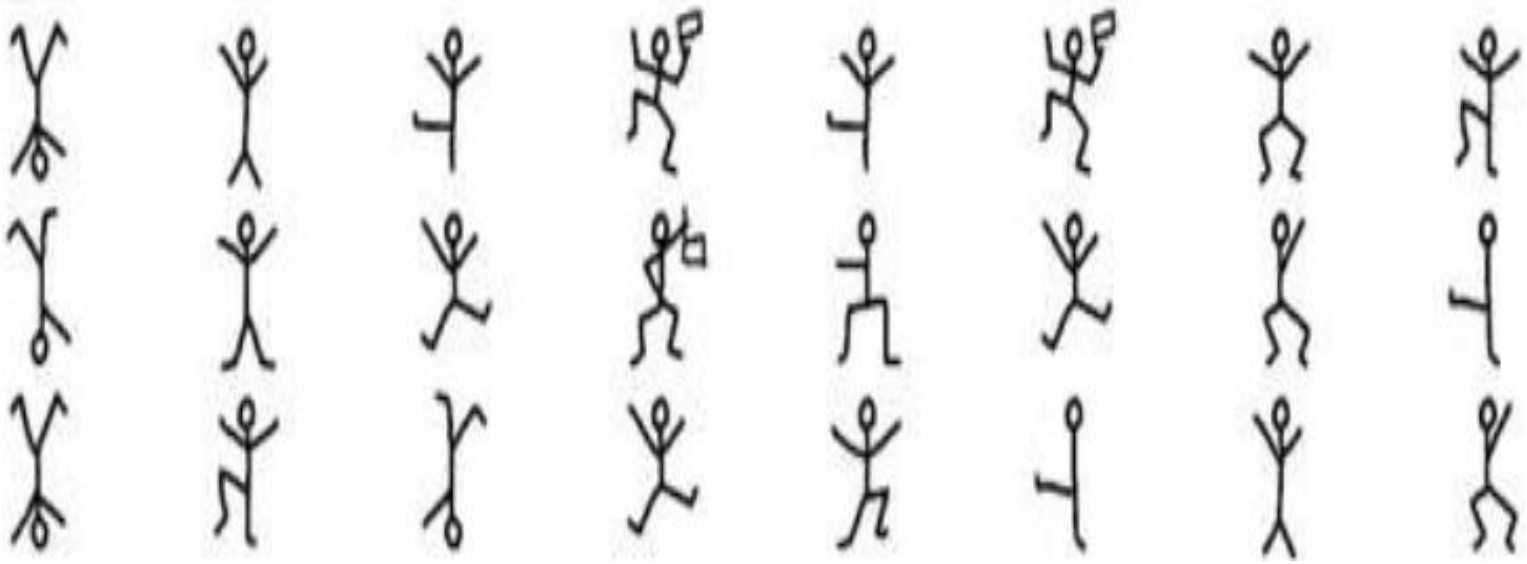
- 다음 암호를 해독하시오.



2. 춤추는 사람 그림 암호

춤추는 그림 암호

- 다음 암호를 해독하시오.



T □ i □ □ s m □ d e □ n

□ □ y p □ o g r a □ h □

Q & A

실습 문의

정보보호론 조교 김태우
tang_kim@seoultech.ac.kr