정보보호

고전암호

정보보호 연구실

이동섭

dajababa09@gmail.com

ISLAB
INFORMATION SECURITY LABORATORY CNU

실습 계획

주차	날짜	실습 내용	과제	이론
1	09.02	Introduce	-	암호 소개
2	09.09	기초 암호기술 및 암호문 해독	시저, 비즈네르 암호문 해독	고전 암호 / 블록 암호
3	09.18	블록 암호 실습	메시지 AES 암호화	블록 암호
4	09.25	암호화 채팅프로그램 구현	채팅 프로그램 구현	공개키 암호
5	10.02	공개키 암호	RSA 실습	
6	10.09	한글날	-	전자서명
7	10.16	전자서명	전자서명 실습	
8	10.23	중간고사 (예정)	-	
9	10.30	해시	Sha 256 실습	해시
10	11.06	하이브리드 암호 시스템 구현	암호화 채팅 프로그램 구현	하이브리드 암호 시스템
11	11.13	블록체인 기초	환경 세팅	블록체인
12	11.20	블록체인 지갑주소 생성	지갑주소 생성	
13	11.27	블록체인 거래	블록체인 거래	SSL
14	12.04	블록 해더 확인	블록 해더 확인	
15	12.11	기말고사 (예정)	-	

실험 환경

- **가상환경에서 실험**
  - ubuntu 16.04
  - Python 3.6
- **오늘만 https://hashcode.co.kr/code_runners 에서 실습 진행**

시저 암호

■ 시저 암호 (Caesar Cipher)

- ▶ 로마의 줄리어스 시저(유리우스 케사르)가 사용했다고 한 암호
- ▶ 단순 치환 암호(MonoAlphaberic Cipher) 방식 = Simple Substitution Cipher
  - ● 평문을 다른 문자와 1:1로 대응시켜 암호화
  - ● 시저 암호는 알파벳을 일정 수 만큼 “평행이동” 시켜서 암호화
  - ● Key = 평행이동 시키는 거리 값

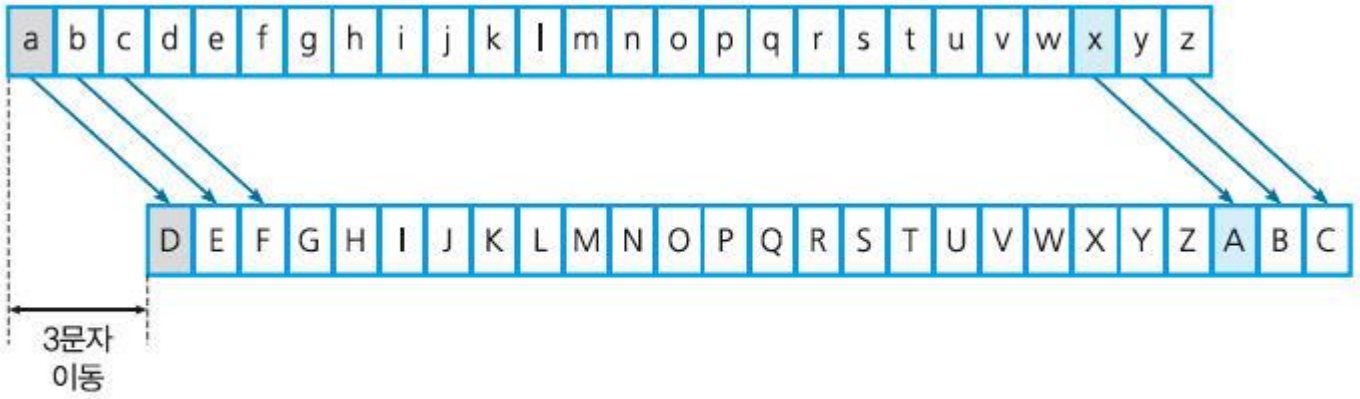
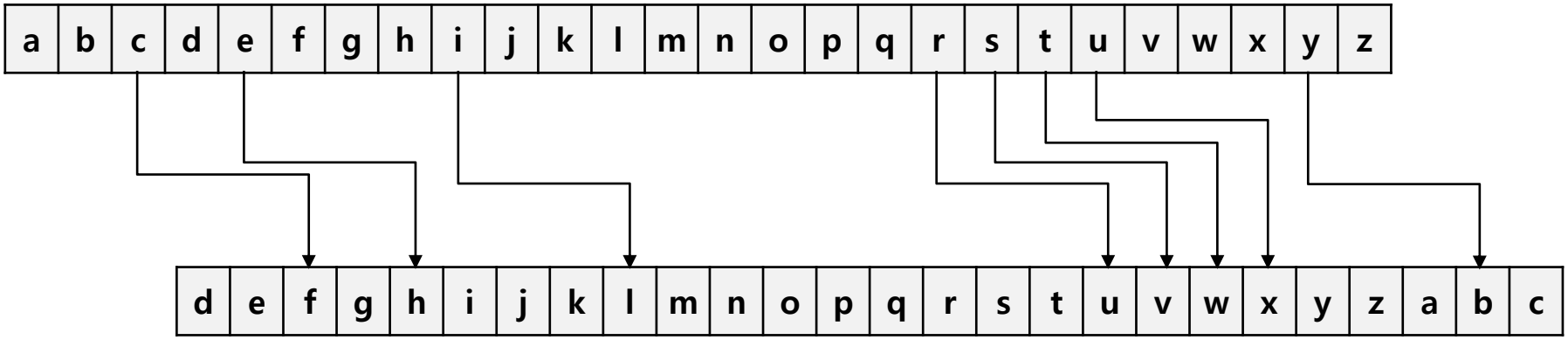


그림 3-1 • 시저 암호에서는 알파벳을 「평행 이동」시킨다.

시저 암호

■ 암호화 과정

- ▶ 평문 : security
- ▶ key : 3

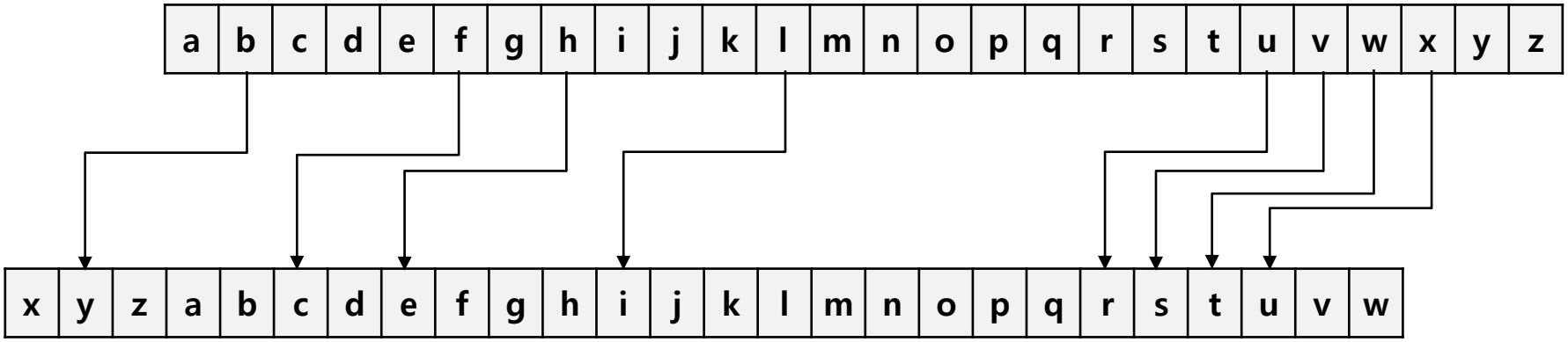


암호문 : v h f x u l w b

시저 암호

■ 복호화과정

- 평문 : vhfxulwb
- key : –3



암호문 : security

Brute-Force Attack

■ Brute-Force Attack(무차별 대입 공격)

- 어릴 때 하던 블록 놀이 – 이것저것 끼워 넣으며 맞을 때까지 시도
- 암호문에 여러 키를 대입함으로써 의미 있는 문자 (즉, 평문)을 구하는 방법

- 시저 암호의 경우 (A~Z 까지) 26가지!
- 쉽게 복호화 가능!

ASCII Code

ASCII Code

- 컴퓨터는 0,1 로만 계산 – 즉, 문자 인식 불가
- ASCII Table => 숫자와 문자 맵핑

```
quanty@ubuntu:~/Desktop/IS/ascii$ cat ascii.c
#include <stdio.h>

void main()
{
        printf("%c = %d\n", 'a', 'a');
        printf("%c = %d\n", 'A', 'A');
}
quanty@ubuntu:~/Desktop/IS/ascii$ gcc -o ascii ascii.c
quanty@ubuntu:~/Desktop/IS/ascii$ ./ascii
a = 97
A = 65
```

DEC	HEX	OCT	Char	DEC	HEX	OCT	Char	DEC	HEX	OCT	Char
0	00	000	Ctrl-@ NUL	43	2B	053	+	86	56	126	V
1	01	001	Ctrl-A SOH	44	2C	054	,	87	57	127	W
2	02	002	Ctrl-B STX	45	2D	055	-	88	58	130	X
3	03	003	Ctrl-C ETX	46	2E	056	.	89	59	131	Y
4	04	004	Ctrl-D EOT	47	2F	057	/	90	5A	132	Z
5	05	005	Ctrl-E ENQ	48	30	060	0	91	5B	133	[
6	06	006	Ctrl-F ACK	49	31	061	1	92	5C	134	₩
7	07	007	Ctrl-G BEL	50	32	062	2	93	5D	135	]
8	08	010	Ctrl-H BS	51	33	063	3	94	5E	136	^
9	09	011	Ctrl-I HT	52	34	064	4	95	5F	137	_
10	0A	012	Ctrl-J LF	53	35	065	5	96	60	140	`
11	0B	013	Ctrl-K VT	54	36	066	6	97	61	141	a
12	0C	014	Ctrl-L FF	55	37	067	7	98	62	142	b
13	0D	015	Ctrl-M CR	56	38	070	8	99	63	143	c
14	0E	016	Ctrl-N SO	57	39	071	9	100	64	144	d
15	0F	017	Ctrl-O SI	58	3A	072	:	101	65	145	e
16	10	020	Ctrl-P DLE	59	3B	073	;	102	66	146	f
17	11	021	Ctrl-Q DC1	60	3C	074	<	103	67	147	g
18	12	022	Ctrl-R DC2	61	3D	075	=	104	68	150	h
19	13	023	Ctrl-S DC3	62	3E	076	>	105	69	151	i
20	14	024	Ctrl-T DC4	63	3F	077	?	106	6A	152	j
21	15	025	Ctrl-U NAK	64	40	100	@	107	6B	153	k
22	16	026	Ctrl-V SYN	65	41	101	A	108	6C	154	l
23	17	027	Ctrl-W ETB	66	42	102	B	109	6D	155	m
24	18	030	Ctrl-X CAN	67	43	103	C	110	6E	156	n
25	19	031	Ctrl-Y EM	68	44	104	D	111	6F	157	o
26	1A	032	Ctrl-Z SUB	69	45	105	E	112	70	160	p
27	1B	033	Ctrl-[ESC	70	46	106	F	113	71	161	q
28	1C	034	Ctrl-₩ FS	71	47	107	G	114	72	162	r
29	1D	035	Ctrl-] GS	72	48	110	H	115	73	163	s
30	1E	036	Ctrl-^ RS	73	49	111	I	116	74	164	t
31	1F	037	Ctrl_ US	74	4A	112	J	117	75	165	u
32	20	040	Space	75	4B	113	K	118	76	166	v
33	21	041	!	76	4C	114	L	119	77	167	w
34	22	042	"	77	4D	115	M	120	78	170	x
35	23	043	#	78	4E	116	N	121	79	171	y
36	24	044	$	79	4F	117	O	122	7A	172	z
37	25	045	%	80	50	120	P	123	7B	173	{
38	26	046	&	81	51	121	Q	124	7C	174	|
39	27	047	'	82	52	122	R	125	7D	175	}
40	28	050	(	83	53	123	S	126	7E	176	~
41	29	051	)	84	54	124	T	127	7F	177	DEL
42	2A	052	*	85	55	125	U	made by Lee Jae-wook			

시저 암호

■ 시저 암호(Caesar Cipher) 구현

- 입력 : 평문 or 암호문, 모드, 키 값
- 출력 : 암호문 or 평문
- 예상 결과 화면
  - 평문에는 “HelloSecurity” 라는 문자열이 존재

```
(base) dajaba@dajaba:~/lab/01$ cat test
HelloSecurity
(base) dajaba@dajaba:~/lab/01$ python Caesar.py
Enter either "encrypt" or "e" or "decrypt" or "d".
e
Enter the key number (1-26)
3
Enter your file name:
test
En(De)cryption complete
(base) dajaba@dajaba:~/lab/01$ cat encrypt.txt
KhoorVhfxulwb
(base) dajaba@dajaba:~/lab/01$
```

시저 암호

■ 시저 암호(Caesar Cipher) 구현

- ▶ 입력 : 평문 or 암호문, 모드, 키 값
- ▶ 출력 : 암호문 or 평문
- ▶ 예상 결과 화면
  - ● 복호화 결과

```
(base) dajaba@dajaba:~/lab/01$ cat encrypt.txt
KhoorVhfxulwb
(base) dajaba@dajaba:~/lab/01$ python Caesar.py
Enter either "encrypt" or "e" or "decrypt" or "d".
d
Enter the key number (1-26)
3
Enter your file name:
encrypt.txt
En(De)cryption complete
(base) dajaba@dajaba:~/lab/01$ cat decrypt.txt
HelloSecurity
(base) dajaba@dajaba:~/lab/01$
```

시저 암호

■ 시저 암호(Caesar Cipher) 구현

▶ Hint 1 : main 함수

```
mode = getMode()
key = getKey()
fileName = getFileName()
encrypt(mode, fileName, key)
```

```
MAX_KEY_SIZE = 26

def getMode():
    while True:
        print('Enter either "encrypt" or "e" or "decrypt" or "d".')
        mode = input().lower()
        if mode in 'encrypt e decrypt d'.split():
            return mode
        else:
            print('The value you entered its invalid')

def getFileName():
    print('Enter your file name:')
    return input()

def getKey():
    key = 0
    while True:
        print('Enter the key number (1-%s)' % (MAX_KEY_SIZE))
        key = int(input())
        if (key >= 1 and key <= MAX_KEY_SIZE):
            return key
```

시저 암호

■ 시저 암호(Caesar Cipher) 구현

▶ Hint 2 : encryptd(mode, filename, key)

```
def encrypt(mode, fileName, key):
    outputFileName = 'encrypt.txt'
    if mode[0] == 'd':
        key = -key
        outputFileName = 'decrypt.txt'
    translated = ''
    outputFile = open(outputFileName, 'w')

    inputFile = open(fileName, 'r')
    message = inputFile.read()

    for symbol in message:
       translated += shift(symbol, key)

    outputFile.write(translated)
    outputFile.close()
    inputFile.close()
    print('En(De)cryption complete')

def shift(symbol, key):
    '''
    Fill in the blank
    '''
```

비제네르 암호

■ 비제네르 암호(Vigenere Cipher)

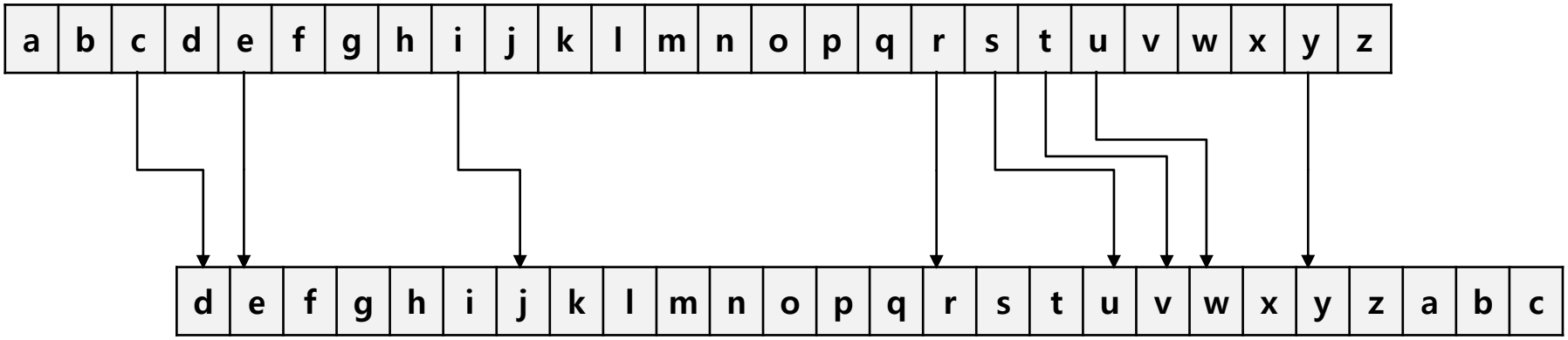
- ▶ 프랑스 외교관 블레즈 드 비제네르에 의해 정리, 발표된 암호
- ▶ 다중 치환 암호(PolyAlphabetic Cipher) 방식
  - ● 평문을 다른 문자와 1:1로 대응시켜 암호화 하지만, 한 글자마다 다르게 적용
  - ● **Key = 평행이동 시키는 거리 값**

	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

비제네르 암호

■ 암호화 과정

- ▶ 평문 : security
- ▶ key : cab (201)



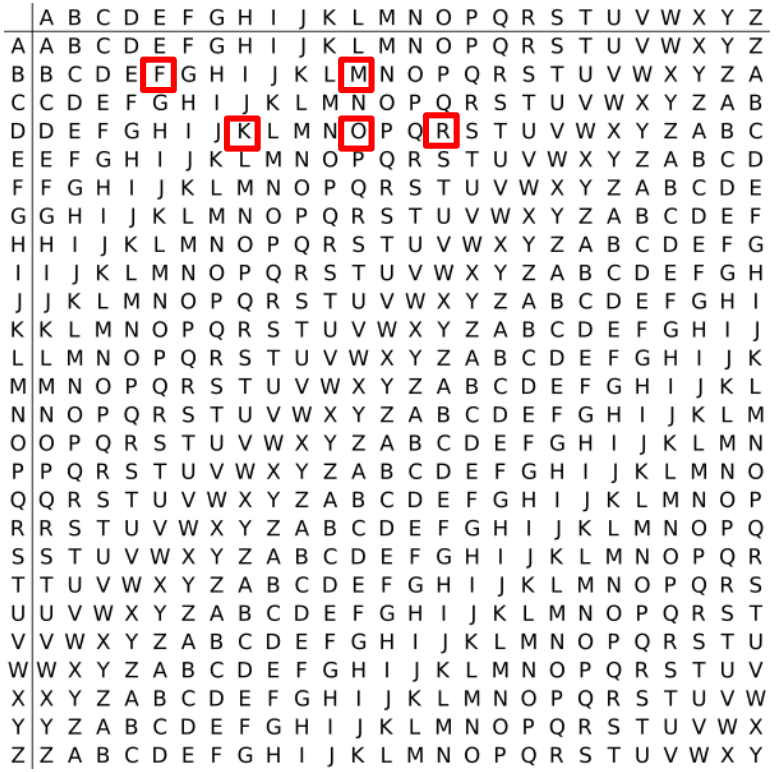
암호문 : uedwrj vy

비제네르 암호

■ 암호화 과정(2)

- ▶ 평문 : H E L L O
- ▶ 키 : D B
- ▶ 암호문 : K F O M R

H	E	L	L	O
D	B	D	B	D
K	F	O	M	R



비제네르 암호

■ 비제네르 암호(Vigenere Cipher) 구현

- 입력 : 평문 or 암호문, 모드, 키 값
- 출력 : 암호문 or 평문
- 예상 결과 화면
  - 입력을 받아서 암/복호화
  - 평문 : test
  - 모드 : e
  - 키 값 : key
  - 암호문 : encrypt.txt
  - 모드 : d
  - 키 값 : key

(1) 암호화

```
(base) dajaba@dajaba:~/lab/01$ cat test
HelloSecurity
(base) dajaba@dajaba:~/lab/01$ python Vigenere.py
Enter either "encrypt" or "e" or "decrypt" or "d".
e
Enter the key
key
Enter your file name:
test
En(De)cryption complete
(base) dajaba@dajaba:~/lab/01$ cat encrypt.txt
RijvsQogsbmri
```

(2) 복호화

```
(base) dajaba@dajaba:~/lab/01$ cat encrypt.txt
RijvsQogsbmri
(base) dajaba@dajaba:~/lab/01$ python Vigenere.py
Enter either "encrypt" or "e" or "decrypt" or "d".
d
Enter the key
key
Enter your file name:
encrypt.txt
En(De)cryption complete
(base) dajaba@dajaba:~/lab/01$ cat decrypt.txt
HelloSecurity
```

제출 요령

- **보고서 (*.pdf)**
  - 문서는 PDF로 변환하여 제출
  - 과제 해결 과정
    - 과제를 어떻게 이해했는지
    - 어떻게 해결했는지

- **소스코드 (*.py)**
  - 과제 해결에 작성한 코드

❖ 소스코드

1) 실습 부분 코드

- 시저 암호 암복호화 코드
- 비제네르 암호 암복호화 코드

제출 요령

■ 제출 방법

- ▶ 사이버 캠퍼스 (e-learn.cnu.ac.kr)
- ▶ 파일명 [IS00]_02_학번_이름
- ▶ 강의 〉 과제제출
  - ● 사이버 캠퍼스로 제출한 과제만 인정

■ 제출 기한

- ▶ 2019 09. 11 10:00:00 ~ 2019 09. 17 23:59:59
  - ● 추가 제출 기한 : 2019 09. 18 ~ 2019 09. 24 23:59:59