프로그래밍

고 2

카이사르 암호문 만들기

아스키 코드로 암호화 & 복호화 해보기

카이사르 암호문의 기원

율리우스 카이사르(Caesar)는 (기원전 100년~44년)
고대 로마의 황제이자 군인이었다.

카이사르가 친지들에게 비밀리에 편지를
보내고자 할 때 사용한 암호가 있는데
이 암호를 오늘날 **"카이사르 암호문"**이라고 부른다.

카이사르 암호문은 가장 오래된 암호법 중 하나로
꼽힌다.

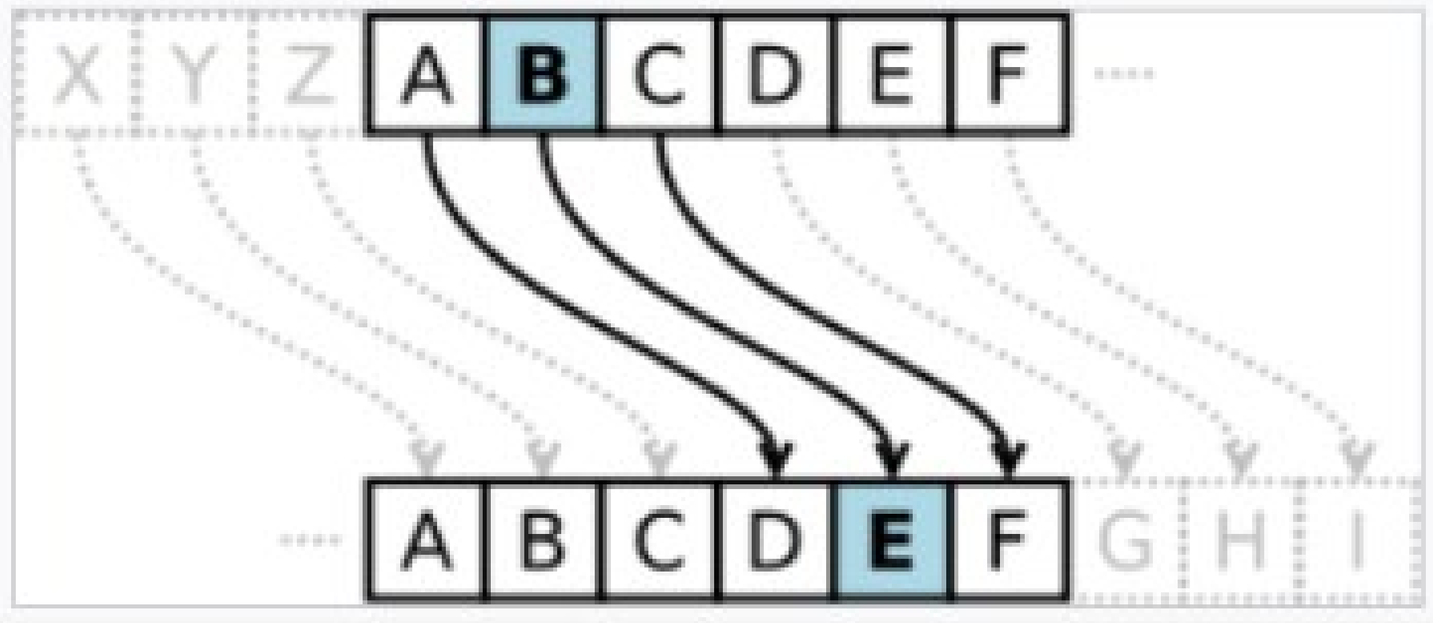
도입

카이사르 암호문이 무엇인가?

카이사르 암호는 간단한 "치환 암호" 의 일종으로,
암호화하고자 하는 내용을 다른 글씨로 "치환" 해서
암호화하는 방법이다.

암호를 보내는 사람과 받는 사람 사이에서
"키(key) 값"이 정해지면 **각각의 알파벳을 키 값 만큼씩 뒤로 밀어서 다른 알파벳으로 치환**하는 방식이다.

카이사르 암호문의 작동 방식 1



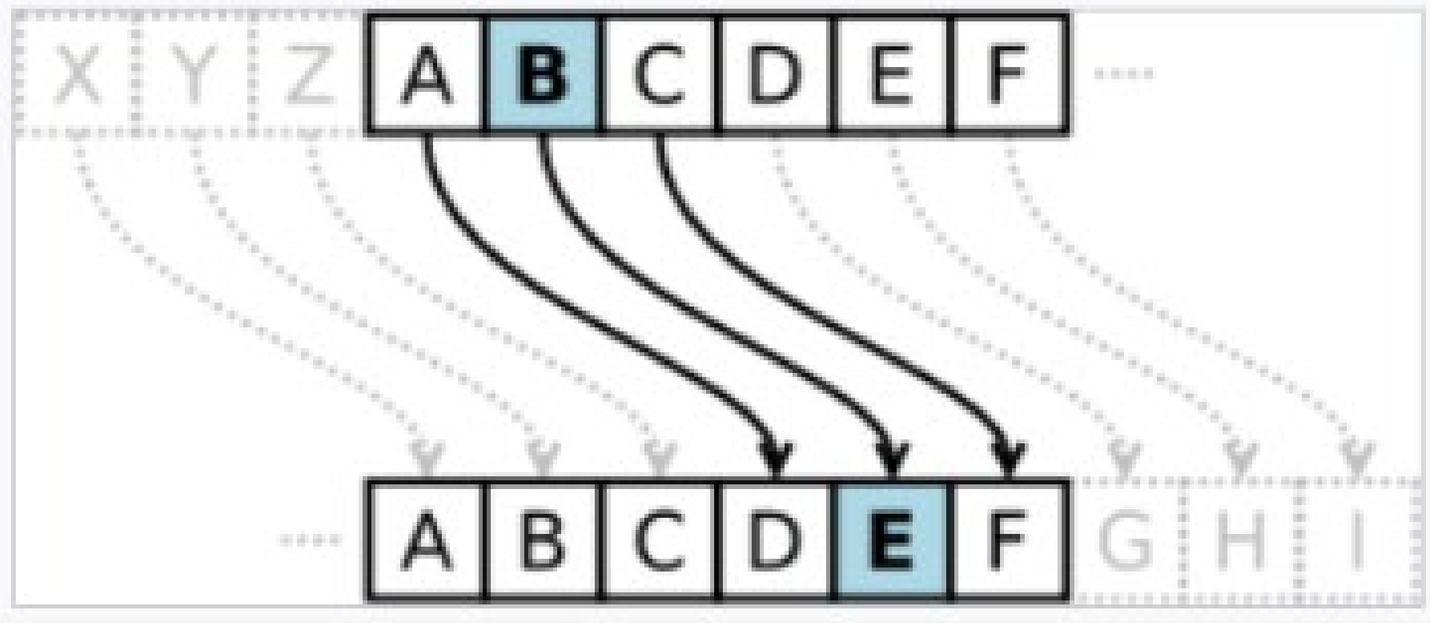
ex) 비밀 키 값이 "3" 이라면 "RUN" 이라는 단어는

R -> RST U

U -> UVW X

N -> NOP Q "UXQ" 라는 단어로 암호화될 것이다.

카이사르 암호문의 작동 방식 2



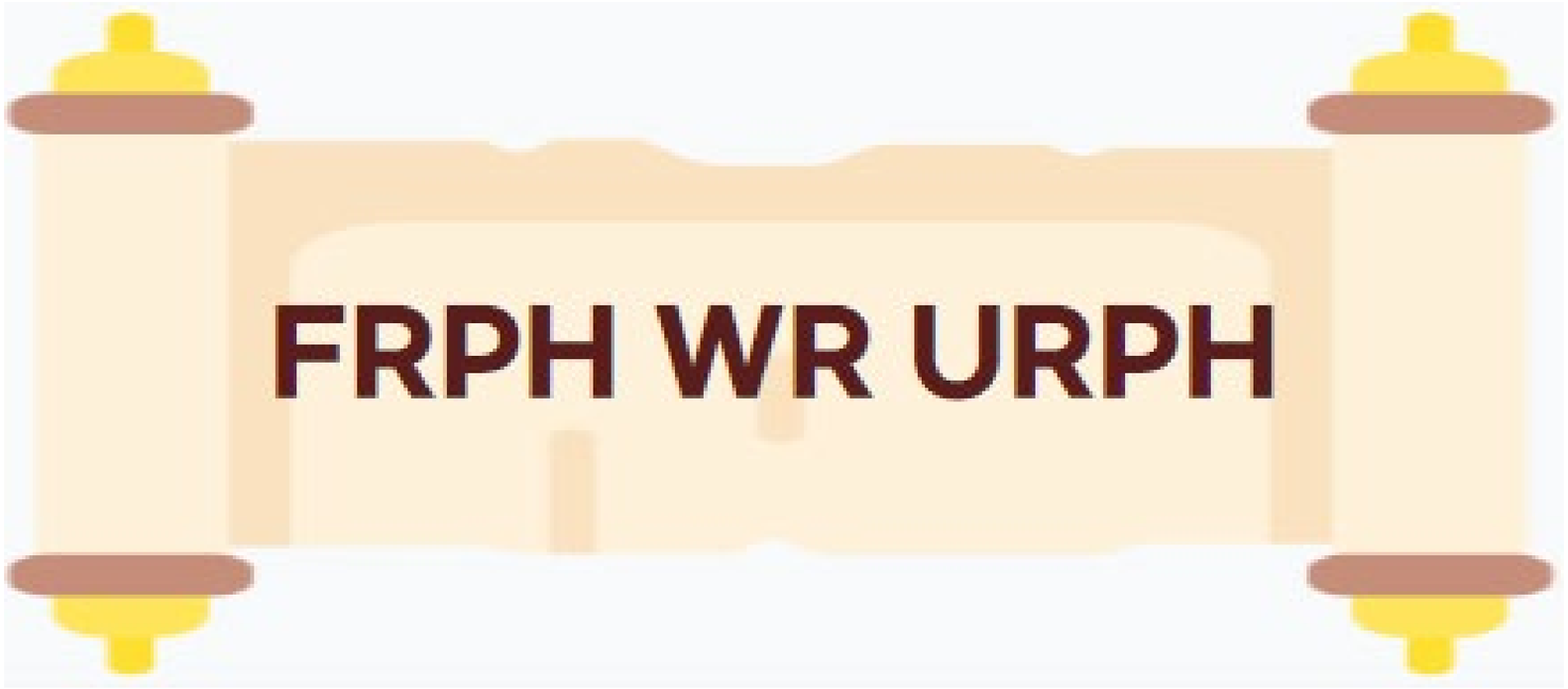
ex) 비밀 키 값이 “4" 이라면 " YOU" 라는 단어는

Y -> YZAB C

O -> OPQR S

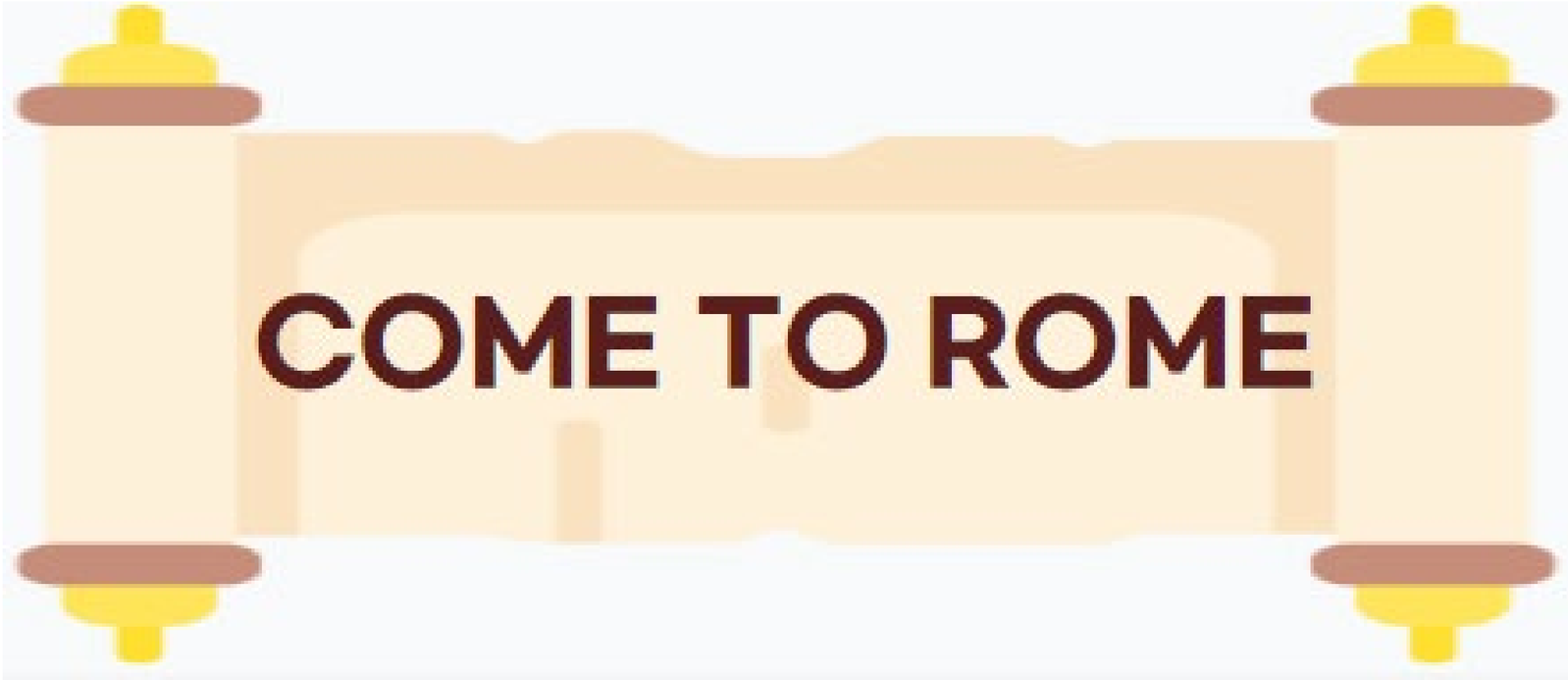
U -> UVWX Y "CSY" 라는 단어로 암호화될 것이다.

간단한 QUIZ!



카이사르는 절친한 친구에게 다음과 같은 메세지를 보냈다.
친구와 사전에 정한 **비밀키는 3** 이다. 이 **메세지의 의미**는 무엇일까?

간단한 QUIZ!



복호화(해독)할 때는 **거꾸로 3칸 씩 앞으로** 옮기면 된다.

* **복호화(decryption) :** 암호화된 데이터를 암호화되기 전의 형태로 되돌리는 처리
(암호화(encryption)의 반댓말)

이번 시간 우리의 목표

손으로 하나 하나 직접 암호화 / 복호화 하는 일은
너무나 귀찮고 비효율적인 일이다 !

그래서 이번 시간에는 나를 대신해서
메세지와 비밀키가 주어졌을 때 암호화를 시켜주고,
암호화된 메세지가 주어졌을 때 복호화를 시켜주는 **코드를**
작성해보고 친구와 비밀 메세지를 교환해보자.

먼저 코드를 작성하기 위해 **"아스키 코드"** 의 개념에 대해 알아보자 !

“아스키 코드” 란 무엇인가?

컴퓨터는 1과 0으로 이루어진 이진법을 바탕으로 작동한다.
이진법 숫자를 통해 문자를 표현하기 위해
각 문자별로 숫자를 하나씩 대응시켜 놓았는데,

'아스키(ASCII) 코드’
(American Standard Code for Information Interchange)는
영문 알파벳을 표현할 수 있는 대표적인 문자 인코딩이다.

전개

아스키 코드

10	HEX	문자	10	HEX	문자	10	HEX	문자	10	HEX	문자
44	0x2C	,	66	0x42	B	88	0x58	X	110	0x6E	n
45	0x2D	-	67	0x43	C	89	0x59	Y	111	0x6F	o
46	0x2E	.	68	0x44	D	90	0x5A	Z	112	0x70	p
47	0x2F	/	69	0x45	E	91	0x5B	[	113	0x71	q
48	0x30	0	70	0x46	F	92	0x5C	₩	114	0x72	r
49	0x31	1	71	0x47	G	93	0x5D	]	115	0x73	s
50	0x32	2	72	0x48	H	94	0x5E	^	116	0x74	t
51	0x33	3	73	0x49	I	95	0x5F	_	117	0x75	u
52	0x34	4	74	0x4A	J	96	0x60	`	118	0x76	v
53	0x35	5	75	0x4B	K	97	0x61	a	119	0x77	w
54	0x36	6	76	0x4C	L	98	0x62	b	120	0x78	x
55	0x37	7	77	0x4D	M	99	0x63	c	121	0x79	y
56	0x38	8	78	0x4E	N	100	0x64	d	122	0x7A	z
57	0x39	9	79	0x4F	O	101	0x65	e	123	0x7B	{
58	0x3A	:	80	0x50	P	102	0x66	f	124	0x7C	|
59	0x3B	;	81	0x51	Q	103	0x67	g	125	0x7D	}
60	0x3C	<	82	0x52	R	104	0x68	h	126	0x7E	~
61	0x3D	=	83	0x53	S	105	0x69	i	127	0x7F	DEL
62	0x3E	>	84	0x54	T	106	0x6A	j			
63	0x3F	?	85	0x55	U	107	0x6B	k			
64	0x40	@	86	0x56	V	108	0x6C	l			
65	0x41	A	87	0x57	W	109	0x6D	m			

아스키 코드란 무엇인가?

파이썬 코드를 통해 문자의 아스키 코드 값을 눈으로 직접 확인해보자

- chr (숫자) : 아스키 코드 숫자 값을 **문자**로 반환

```
print( chr(97) )
print( chr(65) )
```

- ord (문자) : 문자를 **아스키 코드 숫자 값**으로 반환

```
print( ord("A") )
print( ord("a") )
```

아스키 코드란 무엇일까?

파이썬을 열어서 입력한 문자열의 아스키 코드 값을 확인해보자.

```
text = input( "문장 입력:" )

for  i  in  range( len(text) ) :
        print( text[i] ,  ord(text[i]) )    # 문자와 아스키코드 값 출력
```

* len(text) : 문자열 text의 길이를 반환
* range(len(text)) : 0 ~ (text의 길이 - 1) 범위를 표현

아스키 코드 + 카이사르 암호문

방금 배운 아스키코드의 개념을 카이사르 암호문에 적용해보자 !

원래 문자 : C A T
아스키 코드 값 : 67 65 84

주어진 **비밀키 값이 3** 일 때,

아스키 코드 값 :
암호화된 문자 :

>> 코드를 작성하기 위해 **암호화 시키는 과정의 일반화된 식**을 만든다면?

암호화 코드 작성 _ 1

```
text = input( "문장 입력:" )     # text 변수에 원래 문장을 입력
key = int( input("비밀키 입력:") )     # key 변수에 비밀키 값 입력
code = ""     # code 변수에는 암호화된 결과를 저장할 예정 (처음은 빈 문자열 상태)

for  i  in  range( len(text) ) :
        x = ord( text[i] ) + key
        # i+1 번째 문자의 아스키 코드 값에서 key 값을 더한 값을 변수 x 에 저장하기
        code += chr(x)
        # 숫자 값 x 를 문자로 변환하고, code 뒤에 이어 붙이기  ( code = code + chr(x) )

print(code)
```

>> 코드를 작성하고 "CAT" 과 비밀키 3 을 입력해보고 결과를 확인해보자.

>> "YOU" 와 비밀키 6 을 입력해보고 결과를 확인해보자

문제 상황 1 _ if 문으로 처리?

문자의 아스키코드 숫자 값에 비밀키 값을 더했을 때 결과가
A~Z 의 아스키코드 값 범위인 65~90을 넘어서는 경우라면?

> if 문으로 지정해서 처리해주기

ex.
비밀키가 3 이라고 했을 때

A (65) -> 65+3 = **68 < 90** -> D (68) 로 변환
Y (89) -> 89+3 = **92 > 90** -> ?????

문제 상황 1 _ if 문으로 처리?

```
text = input( "문장 입력:" )
key = int( input("비밀키 입력:") )
code = ""

for  i  in  range( len(text) ) :
        x = ord( text[i] ) + key
        if  x  >  90 :                  #  key 값을 더했을 때 A-Z 범위를 넘어가는 경우라면
              x = x – 26
        code += chr(x)                  >> 띄어쓰기도 처리할 수 있도록 바꿔보자

print(code)                             >>  그런데 만약 키값이 30 이라면...?!
```

문제 상황 2 _ 키 값이 매우 큰 경우 처리하기

```
text = input( "문장 입력:" )
key = int( input("비밀키 입력:") )
code = ""

for  i  in  range( len(text) ) :
        x = ord( text[i] ) + key
        key = key%26          >> 키 값이 매우 큰 경우 처리
        if  x  >  90 :
              x = x – 26
        code += chr(x)

print(code)
```

친구가 보낸 암호문 해독해보기 !

친구에게 보내고 싶은 메세지를 비밀키를 가지고 암호화하여
암호화된 메세지를 비밀키와 함께 친구에게 보내봅시다.

받은 **암호문을 해독(복호화)하는 코드를 작성**하고
암호문을 해독해서 어떤 의미인지 파악해보세요.

해독(복호화) 코드와 암호문을 해독한 결과 화면을
캡처해서 제출하세요!