암호화

암호화 기술

§ 보안 문제 발생: 해킹, 바이러스 등의 사이버 범죄나 개인정보 유출

§ 필요 기능: 신원 확인, 정보 비밀성 유지, 무결성 유지

§ 보안 주체 : 국가(1960년대 이전) ➔ 민간(1970년대 중반)

시저 암호

§ 알파벳을 왼쪽으로 세 자리 이동해서 작성한 것이다.

▸평문 문자와 암호 문자의 관계

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	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

[그림 11-1] 시저 암호의 평문 문자와 암호 문자의 관계를 나타내는 암호화 표

▸스물다섯 자리 이동한 암호화

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	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

▸키를 알지 못할 경우 암호문의 해독

① 암호문을 맨 위에 놓는다.

VLA SP

② 각각의 암호화된 알파벳을 알파벳순에 따라 왼쪽 수만큼 더한 값으로 써 내려간다. V에 +1을 해서W로, 다음에는 +2번째인 알파벳 X로, 다음에는 +3번째인Y로, …

③ 어느 순간 의미 있는 문장이 되는 값이 보일 것이다. 23번째 더하기 작업 후, 의미 있는 문장 SIX PM이 보인다.

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

▸ 평문을 암호화

사용할 단어 : JEJUEDUCATION
암호화할 문장 : NEVER TRUST BRUTUS

① 단어 JEJUEDUCATION에서 반복되는 문자가 있으면 처음 나오는 문자 외에는 모두 삭제한다. 그러면 다음과 같이 되는데, 이것이 키가 된다.

JEUDCATION

② 윗줄에는 평문 문자인 알파벳을, 아랫줄에는 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

③ 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

④ 완성된 암호화 표를 이용해서 평문을 암호문으로 바꾸면 다음과 같이 된다.

HCVCP RPSQR EPSRSQ

▸ 단어와 숫자 키를 동시에 사용하여 암호화하는 과정

7과 단어 LINUXANDWINDOWS를 동시에 사용해서 암호화하는 과정

① 단어 LINUXANDWINDOWS에서 처음 나오는 문자를 제외한 반복되는 문자를 삭제하여 단어 키를 구한다. 결국 키는 7과LINUXADWOS가 된다.

LINUXADWOS

② 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

③ 단어 키에서 사용된 문자를 제외한 알파벳의 나머지 문자를 순서대로 쓴다. 평문 문자 Z까지 채워 넣었으면 다시A부터 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

④ 완성된 암호화 표를 이용해서 평문을 암호문으로 변경해보자.

NEVER TRUST BRUTUS -> DVGVB EBFCE QBFEFC

▸ 암호화 표를 사용한 암호화

"WE ATTACK BEFORE THREE AM"

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

① 암호문은"HG YBBYWE OGLURG BMRGG YX"
② 메시지에G가 5개, B가 3개 있음을 알아내고는G를 E로, B를 T로 바꾼다.
- ü 알파벳 문자 중 E는 가장 많이 사용되는 알파벳

§ 암호 해독가가 키를 몰라도 쉽게 암호를 푸는 이유
- ü 시저 암호화 방법으로는 언어적인 패턴과 단어의 중복 사용을 숨길 수 없기 때문이다.
- ü 평문에서 암호문으로 바뀔 때 문자만 바뀔 뿐 암호화 패턴이 똑같다.
- ü 암호 분석가에게는 충분히 해독할 수 있는 단서를 제공한다.

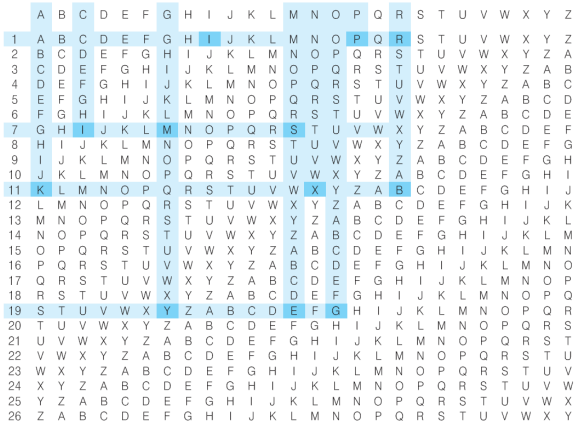
트리테미우스 암호

§ 암호 표를 이용해 암호화를 하는데, 이 암호 표에 있는 알파벳은 줄이 바뀜에 따라 왼쪽으로 한 자리씩 이동하고 왼쪽에서 밀려난 알파벳은 오른쪽 끝으로 이동한다

	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

비게네르 암호

§ 트리테미우스 암호의 i 번째 문자에 i 번째 줄에 있는 암호문을 적용하는 규칙성을 벗어난 암호화 방법



	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

비게네르 암호 예

§ 다음이 암호화 키라 하자 **7, 1, 11, 19**

§ 다음 문장을 암호화 해보자. **C PROGRAMMING**

§ 암호화 키가 7, 1, 11, 19라는 의미는 다음과 같이 첫 번째 글자에는 [그림 11-3] 암호표에서 7번째 줄의 암호문을 적용

§ 두 번째 글자에는 1번째 줄의 암호문, 세 번째 글자에는 11번째 줄의 암호문, 네 번째 글자에는 19번째 줄의 암호문, 다섯 번째 글자에는 다시 7번째 줄의 암호문을 적용한다.

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

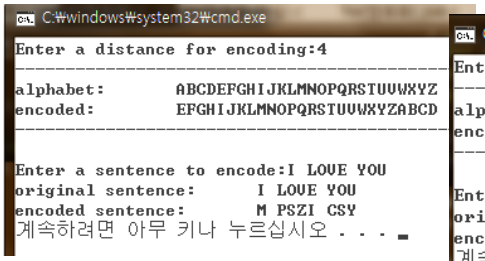
§ 이런 과정을 모두 거치면 결국 다음과 같은 암호문이 생성된다.

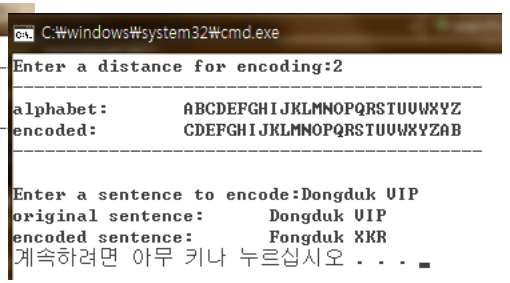
I PBGMRKESIXY

LabHW(암호화)

Lab1(숫자를 이용한 암호화)

- 시저 암호로 입력받은 문장을 암호화하여 출력하라.
  - distance를 입력 받는다
  - 문제를 단순화하기 위해 대문자만 암호화하기로 한다.
  - 문장(대문자와 공백만으로 구성된)을 입력 받아 암호화해서 출력한다.





Functional Decomposition(함수적 분해)

- 어떻게 문제를 나눌 것인가? 각각 매개변수는?
  1. 암호화코드 만들기
  2. 암호화코드 출력
  3. 암호화하기

- Tips
  - 한 문장(공백 문자가 포함된)을 읽기 위해 fgets를 사용

```
char sentence[80];
...
printf("Enter a sentence to encode:");
fgets(sentence, sizeof(sentence), stdin);
```

  - 위에서 문제를 나눈 요소들을 아래의 순서로 완성한다.
    - 1과 2
    - 3

- 어떤 변수를 사용할 것인가?
  - 암호화 코드를 저장할 변수(예: distance가 3일 때)
    - 1차원 배열 사용

[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	...	[22]	[23]	[24]	[25]
D	E	F	G	H	I	J	K	L		Z	A	B	C

- distance
- 입력받은 문장
- 암호화한 문장