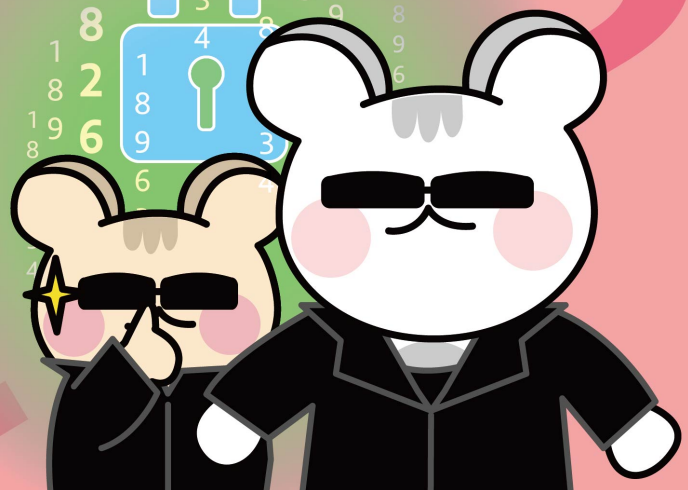


[인증평가(3차) 기출] 플레이페어.



[인증평가(3차) 기출] 플레이페어 암호

난이도 ★★☆☆☆

참가자 수 51

제출 수 127

정답률 42.39%

지원 언어



제한시간 : C/C++/Java/JS/Python(1초) | 메모리 제한 : 1024MB

대학교 학부생활을 마치고 현대자동차에 프로그래머로 취직한 사회초년생 현빈이는 팀장님에게 보안에 관련한 지식이 하나도 없음을 들키고 말았다. 그래서 현빈이는 업무시간 틈틈이 보안과 관련된 주제들을 공부하고 있다.

오늘 공부할 주제는 암호화 방식중 하나인 Playfair cipher(플레이페어 암호)다. Playfair cipher는 알파벳으로 이루어진 어떤 문자열(평문; plaintext)을 암호화하는 방법으로, 이를 위해 알파벳으로 이루어진 문자열인 키(key)가 필요하다. Playfair cipher는 빈도분석을 어렵게 하기 위해 한번에 두 글자 단위로 암호화를 진행하며, 5×5크기의 표를 사용하기 때문에 알파벳 26개를 모두 담기에는 칸이 한 개 부족해 I와 J를 동일한 것으로 생각한다. 이 문제에서는 편의상 J가 아예 주어지지 않는다.

먼저, 주어진 키를 5×5크기의 표로 변환한다. 키를 한 글자씩 보면서 왼쪽 위 칸부터 한줄씩 표를 채운다. 만약

PLAYFAIR CIPHER KEY

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

다음 일은 암호화하려는 메시지를 두 글자씩 나누는 일이다. 예를 들어, HELLOWORLD라는 메시지를 두 글자씩 나눈다면 HE LL OW OR LD가 된다. LL같이 두 글자로 이루어진 쌍이 생기면 중간에 다른 글자를 넣어 쌍을 파괴해줘야 한다. 이렇게 같은 두 글자로 이루어진 쌍이 생기면 그 중 가장 앞에 있는 쌍 사이에 X를 넣고 뒤쪽은 새롭게 쌍을 구성하면 된다. 만약, 쌍이 XX였다면 X를 넣어서는 해결이 안되기 때문에 Q를 넣는 것으로 해결 한다. 이렇게 쌍을 모두 맞추고 마지막에 한 글자가 남는다면 이것도 암호화가 불가능하기 때문에 여기도 X를 덧붙여 강제로 쌍을 맞춰준다. 마지막 남은 한 글자가 X인 경우에는 예외적으로 XX로 쌍을 맞춘다.

그러므로, HELLOWORLD를 두 글자씩 나누는 올바른 방법은 HE LX LO WO RL DX이고, XXXYY를 두 글자씩 나누는 올바른 방법은 XQ XY YX YX가 된다.

마지막으로, 쌍을 만든 두 글자를 암호화하는 일이 남았다. 다음과 같은 세 가지 경우가 있는데, 위에서 만든 5×5표를 통해 설명해본다.

HE -> EI

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

2. 1.의 경우를 만족하지 않으면서 두 글자가 표에서 같은 열에 존재하면, 아래쪽으로 한 칸 이동한 칸에 적힌 글자로 암호화된다. 예를 들어 LO를 암호화하면 RV가 된다. 위치가 다섯 번째 행이라면 첫 번째 행으로 이동하게 된다.

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

3. 1, 2의 경우를 만족하지 않으면서, 두 글자가 표에서 서로 다른 행, 열에 존재하면, 두 글자가 위치하는 칸의 열이 서로 교환된 위치에 적힌 글자로 암호화된다. 예를 들어 LX를 암호화하면 YV가 된다.

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

이 과정에 따르면, HELLOWORLD를 Playfair cipher로 암호화한 결과는 EIYVRVQBRGW가 된다.

현빈이는 어떤 메시지와 키가 주어졌을 때 주어진 메시지를 Playfair cipher로 암호화하려고 한다.

제약조건

메시지의 길이는 1 이상 1,000 이하이다.

키의 길이는 1 이상 100 이하이다.

입력형식

출력형식

첫 번째 줄에 Playfair cipher로 암호화된 결과를 출력한다.

입력예제1

HELLOWORLD
PLAYFAIRCIPHERKEY

출력예제1

EIYVRVVQBRGW

입력예제2

LEMONSTRAWBERRYAPPLEIUIICE
WATERMELON

출력예제2

NALNBQEWTTANRTZEZTKKOWQWUGW

답안 제출

아직 제출된 답안이 없습니다.

제출 언어

GNU C11

코드 편집



Softeer.ai는 현대자동차그룹 산학협력 및 인재육성 전문 기업인 현대엔지비(주)가 운영합니다.

[About Softeer](#) | [Contact Us](#) | [Privacy Policy](#)

COPYRIGHT 2022 HYUNDAI NGV COMPANY. ALL RIGHTS RESERVED.

