Problem 25: Szyfr Playfaira

Punkty: 75

Autor: Brett Reynolds, Annapolis Junction, Maryland, Stany Zjednoczone

Wprowadzenie

Szyfry podstawieniowe są metodą szyfrowania tekstu, która polega na zastąpieniu każdej litery tekstu niezaszyfrowanego inną literą w celu utworzenia tekstu zaszyfrowanego. Choć są one łatwe w użyciu i proste do zapamiętania, to jednak są słabymi szyframi. Pewne litery występują częściej niż inne, co pozwala na złamanie szyfru poprzez zgadywanie, z wykorzystaniem wiedzy o danym języku, jakich liter użyto do zastąpienia innych. Do połowy XIX wieku siły rządowe dobrze zapoznały się z takimi metodami, a ewentualne złamanie przechwyconej wiadomości było relatywnie proste.

W 1854 roku angielski wynalazca, Sir Charles Wheatstone, opracował szyfr, który miał zmierzyć się z tym problemem. Ten szyfr - nazwany później szyfrem Playfaira od nazwiska jego popularyzatora, Lorda Playfaira - zastępował pary liter zamiast pojedynczych liter. Ponieważ angielski język zawiera 26 liter, szyfrowanie liter parami oznaczało, że było dostępnych ponad 600 potencjalnych par, co czyniło analizę częstotliwościową mało praktyczną. Szyfr Playfaira był też prosty w użyciu, co spowodowało, że siły zbrojne używały go przez całą II wojnę światową, aż do nadejścia komputerów.

Opis problemu

Szyfr Playfaira używa słowa lub krótkiego zdania jako klucza, który służy do zbudowania tabeli szyfrowania. Tabela szyfrowania jest kwadratem 5x5 wypełnionym literami angielskiego alfabetu (dla potrzeb opisywanego problemu pominięto literę „J"; później odniesiemy się do tej kwestii).

Przykładowo, jeśli kluczem jest wyrażenie „PLAYFAIR DEMO", to zaczynamy od usunięcia spacji i wpisania liter klucza do tego kwadratu. W przypadku powtórnego wystąpienia litery A pomijamy ją, co daje w rezultacie: „PLAYFIRDEMO." Wpisujemy te litery w kwadrat o wymiarach pięć na pięć, zaczynając od lewego górnego rogu i poruszając się od lewej do prawej i od góry do dołu.

P	L	A	Y	F
I	R	D	E	M
O				

Następnie pozostałe litery alfabetu (z wyjątkiem J) są w kolejności alfabetycznej wpisywane do tego kwadratu. Litery już obecne w tabeli są pomijane.

P	L	A	Y	F

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

W ten sposób uzupełnia się tabelę szyfrowania, której można następnie użyć do zaszyfrowania lub odszyfrowania wiadomości. Zaczynamy od połączenia liter w pierwotnej wiadomości w pary. Ponieważ pominęliśmy literę „J", podczas szyfrowania zastąpimy występujące litery „j" literą „x". Jeśli chcemy zaszyfrować wyrażenie „code quest", otrzymamy:

co de qu es tx

Ponieważ „code quest" zawiera nieparzystą liczbę liter, na końcu dodaliśmy „x", by utworzyć ostatnią parę. Następnie każda para liter jest szyfrowana według poniższych reguł:

1. Jeśli litery w parze są identyczne (np. „ss"), zastępuje się drugą literę literą „x" (np. „sx") i kontynuuje szyfrowanie zgodnie z instrukcją.
2. Jeśli litery pojawiają się w tym samym rzędzie tabeli szyfrowania, zastępuje się każdą literę tą, która znajduje się zaraz na prawo w tabeli (zawijając tabelę do lewej strony w razie potrzeby).
3. Jeśli litery pojawiają się w tej samej kolumnie tabeli szyfrowania, zastępuje się każdą literę tą, która znajduje się zaraz poniżej w tabeli (zawijając tabelę do góry w razie potrzeby).
4. Jeśli litery nie są w tym samym rzędzie ani tej samej kolumnie, zastępuje się każdą literę literą w tym samym rzędzie, co ona, ale w tej samej kolumnie, co jej litera z pary.

Używając do demonstracji naszego wcześniejszego przykładu (klucz: „PLAYFAIR DEMO", tekst niezaszyfrowany „code quest"), postępuje się według podanych reguł jak niżej:

Pierwotna para	Zastosowana reguła	Tabela szyfrowania					Para wynikowa
co	2 - Ten sam rząd; zastępuje się każdą literę literą po jej prawej stronie	P	L	A	Y	F	GB
		I	R	D	E	M	
		O	B	C	G	H	
		K	N	Q	S	T	
		U	V	W	X	Z	
de	2 - Ten sam rząd; zastępuje się każdą literę literą po jej prawej stronie	P	L	A	Y	F	EM
		I	R	D	E	M	
		O	B	C	G	H	
		K	N	Q	S	T	
		U	V	W	X	Z	

Pierwotna para	Zastosowana reguła	Tabela szyfrowania					Para wynikowa
qu	4 - Różne rzędy/kolumny; zastępuje się każdą literę literą w tym samym rzędzie i w kolumnie sparowanej z nią litery	P	L	A	Y	F	KW
		I	R	D	E	M	
		O	B	C	G	H	
		K	N	Q	S	T	
		U	V	W	X	Z	
es	3 - Ta sama kolumna; zastępuje się każdą literę literą poniżej niej	P	L	A	Y	F	GX
		I	R	D	E	M	
		O	B	C	G	H	
		K	N	Q	S	T	
		U	V	W	X	Z	
tx	4 - Różne rzędy/kolumny; zastępuje się każdą literę literą w tym samym rzędzie i w kolumnie sparowanej z nią litery	P	L	A	Y	F	SZ
		I	R	D	E	M	
		O	B	C	G	H	
		K	N	Q	S	T	
		U	V	W	X	Z	

Zaszyfrowany tekst wynikowy to „GB EM KW GX SZ". Należy zwrócić uwagę, że w zaszyfrowanym tekście jedna litera występuje dwukrotnie, zamiast liter „c" i „e" - takie zdarzenia uniemożliwiają udane wykonanie próby analizy częstotliwościowej. W zależności od tego, jak parowane są litery, pojedyncza litera w zaszyfrowanym tekście może reprezentować dowolną literę tekstu niezaszyfrowanego.

W opisywanym problemie musicie napisać program, który odkoduje szyfr Playfaira, z wykorzystaniem zadanej zaszyfrowanej wiadomości i klucza służącego do zaszyfrowania. Odszyfrowanie działa podobnie jak szyfrowanie; należy jedynie przesuwać litery w lewo lub w górę, gdy pojawią się, odpowiednio, w tym samym rzędzie lub tej samej kolumnie. Nie trzeba zastępować obecnych liter „x" literami „j" lub spacjami; można je zostawić.

Przykładowe dane wejściowe

Pierwszy wiersz danych wejściowych programu, otrzymanych przez standardowy kanał wejściowy, będzie zawierać dodatnią liczbę całkowitą oznaczającą liczbę przypadków testowych. Każdy przypadek testowy będzie zawierać poniższe wiersze:

- Każdy wiersz zawiera poniższe informacje, oddzielone spacjami:
  - X, dodatnią liczbę całkowitą odpowiadającą liczbie wierszy tekstu zaszyfrowanego
  - Klucz służący do zaszyfrowania wiadomości szyfrem Playfaira, który będzie zawierać jedynie wielkie litery.
- X wierszy zawierających zaszyfrowany tekst, który ma zostać odszyfrowany, z wyłącznie wielkimi literami.

```
2
1 PLAYFAIRDEMO
GBEMKWGXSZ
2 LOCKHEEDMARTIN
KRLTUZBIDIBK
PLDIHGKH
```

Przykładowe dane wyjściowe

W każdym przypadku testowym program musi wyświetlić niezaszyfrowaną wiadomość, małymi literami.

```
codequestx
havefuntoday
goodluck
```