Szyfr (2012 R)

Rozważmy szyfr podstawieniowy działający zgodnie z następującymi zasadami:

- Tekst jawny, szyfrogram oraz klucz składają się wyłącznie z wielkich liter alfabetu angielskiego.
- Litery ponumerowano i przyporządkowano im kody ASCII (liczby z zakresu 65–90):

Tabela numerów i kodów ASCII poszczególnych liter

Litera	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
Nr litery	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Kod ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

- Kolejne litery tekstu jawnego są szyfrowane za pomocą kolejnych liter słowa będącego kluczem, być może powtórzonego wiele razy.
- W procesie szyfrowania tekst jawny przekształcany jest na szyfrogram przy pomocy klucza poprzez dodanie do kodu litery tekstu jawnego numeru odpowiadającej jej litery klucza. Jeżeli tak uzyskana wartość liczbowa będzie większa od 90, należy ją zmniejszyć o 26. Szyfrem danej litery jest litera o tak uzyskanym kodzie. Poniższy przykład precyzuje zasady szyfrowania.

Przykład:

Tekst jawny: LATO, klucz: WODA
L+W = 76+23 = 99. Ponieważ przekroczono zakres 90, należy od 99 odjąć26, czyli 99–26 = 73. Zatem zaszyfrowanym znakiem jest litera I.
A+O = 65+15 = 80, czyli zaszyfrowanym znakiem jest litera P.
T+D = 84+4 = 88, czyli zaszyfrowanym znakiem jest litera X.
O+A = 79+1 = 80, czyli zaszyfrowanym znakiem jest litera P.
Szyfrogram: IPXP

- Jeżeli użyte słowo kluczowe jest zbyt krótkie, by wystarczyło do zaszyfrowania całego tekstu, należy użyć jego powtórzeń.

Przykład:

Tekst jawny: MARTA, klucz: TOR
M+T = 77+20 = 97, 97-26=71, G
A+O = 65+15 =80, P
R+R = 82+18= 100, 100-26 = 74, J
T+T = 84+20 = 104, 104-26=78, N
A+O = 65+15 =80, P
Szyfrogram: GPJNP

- W procesie deszyfrowania szyfrogram przekształcany jest na tekst jawny przy pomocy klucza poprzez odjęcie od kodu litery szyfrogramu numeru odpowiadającej jej litery klucza (jeżeli tak uzyskana wartość liczbowa będzie mniejsza od 65, należy ją powiększyć o 26) i odczytanie litery o otrzymanym kodzie.

Korzystając z dostępnych narzędzi informatycznych, wykonaj poniższe polecenia.

a) W pliku tj.txt znajdują się niezaszyfrowane słowa, a w pliku klucze1.txt – klucze szyfrujące. W obu plikach wyrazy umieszczone są w osobnych wierszach. Zaszyfruj słowa zawarte w pliku tj.txt, wynik zapisz w pliku wynik4a.txt. Wyraz zapisany w N-tym wierszu w pliku z wynikami powinien stanowić szyfrogram tekstu jawnego znajdującego się w N-tym wierszu w pliku z tekstem jawnym uzyskany za pomocą klucza znajdującego się w N-tym wierszu pliku z kluczami.
b) W pliku sz.txt znajdują się zaszyfrowane słowa, a w pliku klucze2.txtznajdują się klucze deszyfrujące. W obu plikach wyrazy umieszczone są w osobnych wierszach. Odszyfruj słowa zawarte w pliku sz.txt, wynik zapisz do pliku wynik4b.txt. Wyraz zapisany w N-tym wierszu w pliku z wynikami powinien stanowić tekst jawny szyfrogramu znajdującego się w N-tym wierszu w pliku z szyfrogramami uzyskany za pomocą klucza zapisanego w N-tym wierszu pliku z kluczami.