Algorytm Szyfru Argentiego

Szyfr Argentiego stanowi odmianę szyfru Cezara. Jego autorem jest Matteo Argenti, żyjący w drugiej połowie XVII wieku. Razem ze swoim wujem Giovanni Battista Argenti byli twórca szyfrów w Państwie Kościelnym.

Szyfr jest podobny do algorytmu Cezara, ale alfabetyczny układ liter jest dodatkowo zaburzony poprzez wprowadzenie hasła (klucza mnemonicznego). W poniższym przykładzie hasłem jest ARGENTI.

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
V	W	X	Y	Z	**A**	**R**	**G**	**E**	**N**	**T**	**I**	B	C	D	F	H	J	K	L	M	O	P	Q	S	U
Przesunięcie					Hasło							Pozostałe litery w kolejności alfabetycznej													

W wypadku używania słowa, w którym litery się powtarzają, należy wyeliminować kolejne wystąpienia tej samej litery.

ABRAKADABRA →ABR**A**K**A**D**ABRA** →ABRKD

Zaletą tej metody jest prostota i łatwość tworzenia kolejnej odmiany szyfru.

Im dłuższe słowo (lub zdanie) będzie hasłem, tym mniej liter będzie występować w naturalnym porządku alfabetycznym, a szyfrogram będzie trudniejszy do dekryptażu. Jako klucza użyć najlepiej długiego tekstu, który jest znany wszystkim i którego posiadanie nie budzi żadnych podejrzeń. W kręgu kultury chrześcijańskiej może to być fragment Biblii, w islamie Koran.

Właściwości szyfru Argentiego

Jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego (niezaszyfrowanego) zastępowana jest inną. Nie rozróżnia się przy tym liter dużych i małych.

Nie działa tu metoda znana z szyfru Cezara, czyli sprawdzenie wszystkich kombinacji przesunięcia.

Kodowanie szyfru Argentiego

Poniższy przykład korzysta z dwuwymiarowej tablicy [2, 26]. W pierwszej mamy kompletny alfabet, a druga jest pusta.

.

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

Do dolnego wiersza wpisujemy hasło mnemoniczne.

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
B O R S U K

Następnie przepisujemy do dalszej części litery nieużyte w haśle.

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

Ostatnim krokiem jest przesunięcie o zadany klucz.

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

Ta sama tablica może służyć do szyfrowania i deszyfrowania wiadomości.

Redukcja powtarzających się znaków w haśle

Heterogram – wyraz, w którym żadna litera się nie powtarza.
Pierwszym krokiem jest modyfikacja hasła (klucza mnemonicznego). Należy wczytać hasło i usunąć powtarzające się litery.

Za pomocą pętli należy sprawdzać kolejne litery czy występują w dalszej części. Jeśli tak to należy je skasować, a łańcuch tekstowy przesunąć o 1 pozycję w lewo.

A	B	R	A	K	A	D	A	B	R	A
↑↑			↑							

Usuwamy ją a pozostałe znaki przesuwamy o 1 w lewo

A	B	R	K	A	D	A	B	R	A	
↑↑			↑							

Całość jest powtarzana do momentu dojścia do końca hasła.

Kryptoanaliza:

Powyższy szyfr jest dość odporny na metodę *brute-force* (istnieje zbyt dużo kombinacji).

Skuteczną metodą dekryptażu jest ***analiza częstości***. Wystarczy zestawić i sprawdzić rozkład częstości występowania pojedynczych liter (czy ich par) i dopasować go do statystyki danego języka.

Inną metodą jest próba odkrycia użytego hasła. Stosuje się tu ***metodę słów prawdopodobnych*** wynikającą ze znajomości poruszanej tematyki i osób posługujących się tym szyfrem. Inną metodą jest ***metoda słownikowa*** stosowana, gdy wcześniejsza nie dała wyniku.

Przydatna jest też ***metoda słów prawdopodobnych***. Odczytanie fragmentu wiadomości pozwala na złamanie reszty szyfru.

Ćwiczenia

1. Używając szyfru Argentiego napisz program:
   a. szyfrujący wiadomość
   b. deszyfrujący wiadomość

   Program ma wczytywać długość przesunięcia i hasło (klucz mnemonicznego).
   c. Dodaj opcję modyfikacji hasła tak, by usunąć powtarzające się znaki.