

Algorytm Szyfru płotkowego

Szyfr płotkowy to szyfr przestawieniowy, opisywany przez pewną liczbę **n**, oznaczającą „wysokość” tworzonych schodków – kolejne litery tekstu jawnego zapisywane są na zmianę w **n** rzędach. Kryptogram tworzony jest poprzez połączenie ciągu kolejnych liter pierwszego rzędu, po którym umieszcza się rząd drugi, itd.

$n = 4$

K						G					
	R				O		R				A
		Y		T				A		I	
			P						F		

KRYPTOGRAFIA → KGORRAYTAIPF

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

Im większa „wysokość” użytych schodków, tym ewentualna kolejność i powiązanie liter będzie bardziej zaburzone, a szyfrogram będzie trudniejszy do dekryptażu.

Właściwości szyfru PŁOTKOWEGO

Jest to rodzaj szyfru przestawieniowego, w którym każda litera tekstu jawnego jest przestawiana w inne miejsce.

Kryptoanaliza:

Nieskuteczną metodą dekryptażu jest **analiza częstości**. Zestawienie będzie takie same jak w tekście naturalnym.

Jednocześnie pozwoli to wywnioskować, że użyty szyfr jest szyfrem przestawieniowym. Dzięki temu deszyfrant będzie wiedział, że należy wypróbować znane szyfry przestawieniowe lub przestawiać litery w różnych kombinacjach.

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.

Można też użyć specjalnych tekstów:

- Wiadomością pozwalającą złamać szyfr jest ciąg kolejnych liter alfabetu (**abcdefghijklmnopqrstuvwxyz**). Dzięki temu możliwe jest ustalenie użytego hasła i wielkości klucza przesuwającego.

Ćwiczenia

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

Program ma wczytywać wysokość schodków i tekst do szyfrowania.

2. Używając szyfru płotkowego napisz program, który odwraca kierunek szyfrowania, tworząc piramidę według wzoru:

			P						F		
		Y		T				A		I	
	R				O		R				A
K						G					

Program ma wczytywać wysokość schodków i tekst do szyfrowania.

3. Używając szyfru płotkowego napisz program, który pozwala ustalić kierunek odwracania: góra lub dół.