Szyfr Vigenère

Paweł Gliwny

Szyfr Vigenère

- Szyfr Vigenère to metoda szyfrowania tekstu alfabetycznego za pomocą serii różnych przesunięć alfabetu Cezara w oparciu o litery hasła. Jest to forma szyfrowania polialfabetycznego, co oznacza, że używa wielu alfabetów do szyfrowania danych.
- W szyfrze Vigenère używa się klucza, który jest powtarzanym słowem lub frazą. Długość klucza może być różna, ale im jest dłuższa, tym szyfr jest trudniejszy do złamania. Każda litera klucza odpowiada przesunięciu w alfabecie, np. 'A' odpowiada przesunięciu o 0, 'B' o 1, 'C' o 2, itd.

Działania

1) Przygotuj tekst jawny i klucz.
2) Ustaw tekst jawny i klucz jeden pod drugim, powtarzając klucz, aż do osiągnięcia długości tekstu jawnego.
3) Dla każdej pary liter (jedna z tekstu, druga z klucza) dodaj wartości przypisane do liter (A=0, B=1, ..., Z=25) i oblicz wynik modułu 26 (długość alfabetu).
4) Znajdź literę w alfabecie, która odpowiada wynikowi z punktu 3 - ta litera jest literą szyfru.

Deszyfrowanie

- Deszyfrowanie jest procesem odwrotnym: dla każdej pary liter (jedna z tekstu zaszyfrowanego, druga z klucza) odejmuj wartości liter i oblicz wynik modułu 26, aby uzyskać oryginalną literę tekstu jawnego.
- Szyfr Vigenère był kiedyś uważany za niezwykle bezpieczny, zwłaszcza kiedy używano długich, nieregularnych kluczy. Jednak z czasem został złamany, szczególnie za pomocą metody statystycznej znaną jako analiza Kasiskiego.