Łamanie szyfru Vigenere index of coincidence

Paweł Gliwny

Wskaźnika Zbieżności (IC)

- Wskaźnik zbieżności (IC) to miara statystyczna określająca częstość powtórzeń liter w tekście.
- W normalnym języku angielskim IC wynosi około 0.0667, podczas gdy dla tekstu przypadkowego, takiego jak dobrze zaszyfrowany tekst, wartość ta spada do około 0.0385.
- IC może pomóc w odkryciu długości klucza szyfru Vigenère'a, analizując wzory powtórzeń w szyfrogramie.

Analiza Szyfrogramu za pomocą IC

- Dziel szyfrogram na ciągi na podstawie domniemanej długości klucza; każdy ciąg powinien zawierać litery zaszyfrowane tym samym znakiem klucza.
- Oblicz IC dla każdego z tych ciągów. Wysokie wartości IC (zbliżone do IC naturalnego języka) wskazują, że domniemana długość klucza może być prawidłowa.
- Porównaj IC dla różnych długości klucza, aby znaleźć najbardziej prawdopodobną długość klucza.

Łamanie Szyfru Vigenère'a

- Po określeniu długości klucza, podziel szyfrogram odpowiednio i analizuj każdy ciąg jako osobny szyfr Cezara.
- Użyj analizy częstotliwości liter (oraz innych metod kryptograficznych do odszyfrowania tekstu).
- Prawidłowa długość klucza ujawni wzorce charakterystyczne dla języka naturalnego, umożliwiając skuteczne odszyfrowanie wiadomości.