

Kryptografia – Podstawowe pojęcia

Kryptologia (cryptology) jest dziedziną matematyki najogólniej mówiąc zajmującą się szyframi. Można podzielić ją na **kryptografię (cryptography)** oraz **kryptoanalizę (cryptoanalysis)**. Kryptografia zajmuje się tworzeniem algorytmów kryptograficznych a kryptoanaliza ich łamaniem.

Tekst jawny, czysty, otwarty (plaintext, opentext) – to tekst, który będzie podlegał szyfrowaniu (M)

Tekst zaszyfrowany, szyfrogram (ciphertext)- to tekst będący wynikiem szyfrowania (C)

Szyfrowanie (encryption) – proces zamiany tekstu jawnego na tekst zaszyfrowany (E)

$$E(M)=C$$

Deszyfrowanie (decryption) – jest procesem odwrotnym, a w jego wyniku otrzymujemy tekst jawny (D)

$$D(C)=M$$

Aby wiadomość mogła być zaszyfrowana a następnie prawidłowo odszyfrowana musi być spełniona następująca zależność:

$$D(E(M))=M$$

Algorytm kryptograficzny – jest to funkcja użyta do szyfrowania i deszyfrowania (czasami są to dwie różne funkcje)

Algorytmy kryptograficzne podzielić możemy na **algorytmy symetryczne** (z kluczem prywatnym) (symmetric algorithm) lub **asymetryczne** (z kluczem publicznym). W przypadku tych pierwszych do zaszyfrowania i odszyfrowania wiadomości używamy takiego samego klucza. Wśród algorytmów symetrycznych istnieje podział na **algorytmy blokowe (block algorithm)** oraz **strumieniowe (stream algorithm)**. W pierwszym przypadku tekst jawny dzielony jest na bloki o odpowiedniej długości (najczęściej 64 lub 128 bitów) a

następnie każdy blok jest szyfrowany oddzielnie. W algorytmach strumieniowych – tekst jest szyfrowany bit po bicie lub bajt po bajcie. W przypadku algorytmów asymetrycznych do szyfrowania używamy **klucza publicznego (public key)** osoby, do której przesyłamy wiadomość a do odszyfrowania szyfrogramu osoba ta używa własnego **klucza prywatnego (private key)**. Klucz publiczny może być publicznie wszystkim udostępniony.

Algorytmy ograniczone (restricted algorithm) - są to algorytmy kryptograficzne, w których trudność deszyfrowania szyfrogramu oparta jest na ukryciu algorytmu w tajemnicy.

Szyfry podstawieniowe (substitution cipher) powstają poprzez podstawienie w miejsce litery w tekście jawnym jakiejś innej litery (wg jakiegoś wzoru) w wyniku czego otrzymujemy szyfrogram.

Wyróżniamy wśród nich:

- szyfry monoalfabetyczny (monoalphabetic cipher)** np. szyfr Cezara, ROT13 – każda litera tekstu jawnego zamieniana jest w inną literę na podstawie jednego alfabetu (np. alfabetu z przesunięciem o 3 lub 13)

- szyfry polialfabetyczny, wieloalfabetyczny (polyalphabetic cipher)** np. szyfr Vigenere'a – pojedyncze litery zastępowane są literami z wielu alfabetów (np. jedna z alfabetu z przesunięciem o 1, druga o 2 itd.)

- szyfr homofoniczny (homophonic cipher)** – jest to szyfr odporny na atak typu analizy częstości występowania poszczególnych liter – cechuje się on tym, że każda litera z tekstu jawnego może mieć kilka (ilość zależy od procentu występowania danej litery w tekście) swoich odpowiedników w tekście zaszyfrowanym

- szyfr poligramowy (polygram cipher)** – zamieniane są nie pojedyncze litery, lecz np. pary liter jak w przypadku szyfru Playfair'a, szyfru Hilla, tablicy Polibiusza, metody nihilistycznej czy też szyfru ADFGVX.

Szyfry przestawieniowe (transposition cipher) powstają poprzez przestawienie liter tekstu jawnego w określony sposób na skutek, czego otrzymujemy szyfrogram.

Szyfrator synchroniczny- klucz generowany jest niezależnie od wiadomości

Szyfrator samosynchronizujący- klucz generowany jest na podstawie ustalonej liczby n poprzednich znaków szyfru