

Kryptoanaliza – Wprowadzenie

Kryptoanaliza jest dziedziną wiedzy i badań zajmującą się metodami łamania szyfrów.

Bezpieczeństwo szyfrów historycznych jest z reguły niskie. Korzystając z komputera mogą być one odszyfrowane w czasie krótszym niż 1 sekunda.

W przypadku współczesnych szyfrów mówimy o szyfrach **obliczeniowo bezpiecznych**, co oznacza, że nie można ich złamać przy zastosowaniu systematycznej analizy z użyciem dostępnych zasobów.

Możemy również mówić o **bezwarunkowym bezpieczeństwie**. W przypadku takich szyfrów niezależnie od ilości przechwyconych tekstów zaszyfrowanych nie jesteśmy w stanie jednoznacznie określić tekstu jawnego. Jedynym algorytmem bezwarunkowo bezpiecznym jest algorytm one-time pad. Matematyczny dowód na to został podany w roku 1949 przez Shannon'a.

Jest to prosty algorytm wykonujący operację XOR. Jeżeli chcemy, aby algorytm był bezwarunkowo bezpieczny muszą być spełnione 3 warunki:

- hasło musi być ciągiem losowym
- hasło musi być jednorazowe
- długość hasła musi być przynajmniej tak samo długa jak szyfrowany tekst.

Metody łamania szyfrów historycznych:

1. Monoalfabetyczne szyfry podstawieniowe jak np. szyfr Cezara – wykonujemy podstawienia o wszystkie możliwe pozycje (1,2,...,25). Z otrzymanych tekstów wybieramy ten właściwy.
2. Szyfr Vigenere'a – istnieją tutaj dwie metody test Kasiskiego i indeks koincydencji.

3. Często stosowaną metodą dla wielu szyfrów historycznych jest analiza częstości występowania poszczególnych liter.
4. Analiza częstości występowania par lub trójek literowych w szyfrogramie.

Metody łamania szyfrów współczesnych:

W większości przypadków mamy tutaj do czynienia z zasadą Kerckoffsa – mówiącą, że bezpieczeństwo szyfru powinno zależeć całkowicie od długości klucza.

Wyróżniamy kilka podstawowych ataków na szyfrogram. Wymienię tutaj podstawowe:

- **Atak na tekst zaszyfrowany** – mamy do dyspozycji jedynie tekst zaszyfrowany (szyfrogram).
- **Atak na tekst częściowo znany** – znamy kilka liter z tekstu jawnego oraz odpowiadające im litery w szyfrogramie.
- **Atak za pomocą wybranego tekstu jawnego** – mamy możliwość zaszyfrowania dowolnego wybranego przez nas tekstu jawnego.
- **Atak za pomocą wybranego szyfrogramu** – mamy możliwość odszyfrowania dowolnego wybranego przez nas szyfrogramu.
- **Kryptoanaliza różnicowa** – szyfrujemy wiele wiadomości zmieniając jedynie poszczególne bity a następnie analizujemy otrzymane szyfrogramy.
- **Atak na czas wykonywania** – obliczamy czas obliczeń związanych z procesem szyfrowania.
- **Atak algorytmiczny** – atak na teorię, na podstawie której oparty jest algorytm – przykładem może być tutaj atak na algorytmy oparte na problemie placakowym jak np. algorytm Hellmana-Merkle’a (1978).
- **Metoda różnicowej analizy błędów** - w przypadku, gdy system kryptograficzny zrealizowany jest w postaci sprzętowej – urządzenie poddajemy różnego typu czynnikom zewnętrznym, aby wymusić popełnienie błędu podczas szyfrowania lub deszyfrowania – otrzymane wyniki poddajemy analizie.

Kategorie łamania szyfrów wg Larsa Knudsena:

1. Całkowite złamanie szyfru – znalezienie właściwego klucza do odszyfrowania wiadomości.
2. Ogólne wnioskowanie – znalezienie alternatywnego algorytmu niewymagającego znajomości właściwego klucza.
3. Lokalne wnioskowanie – odszyfrowanie wiadomości (nie znamy klucza).
4. Częściowe wnioskowanie – znalezienie drobnych informacji o kluczu i tekście jawnym (nie znamy klucza ani całego tekstu jawnego).