Historia i podstawy kryptografii
Spotkanie 9
Wiek XIX
Bezpieczeństwo szyfrowania

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Auguste Kerckhoffs (1835 –1903)

Auguste Kerckhoffs był holenderskim językoznawcą i kryptografem, profesorem w paryskiej *École des Hautes Études Commerciales*.

Kerckhoffs w roku 1883 opublikował dwie prace pod wspólnym tytułem *La Cryptographie Militaire*, które były przeglądem metod wojskowej kryptografii i zawierały wiele praktycznych rad, w tym sześć reguł praktycznego szyfrowania.

Reguły Kerckhoffsa

(1) System kryptograficzny powinien być, jeśli nie teoretycznie, to w praktyce nie do złamania.

(2) System nie powinien wymagać tajności (poza kluczem), a jego ewentualne ujawnienie nie powinno wywołać negatywnych konsekwencji.

(3) Klucz powinien być: możliwy do zapamiętania bez notowania i łatwy do zmienienia.

(4) Kryptogramy powinny być możliwe do przesłania telegraficznie.

(5) Aparatura i dokumenty powinny być możliwe do przeniesienia i obsłużenia przez jedną osobę.

(6) System powinien być prosty – nie wymagający znajomości wielu reguł ani nie obciążający zbytnio umysłu.

Zasada Kerckhoffsa

Najlepiej jest znana zasada druga, zwana **zasadą Kerckhoffsa**:

Zasada Kerckhoffsa

Bezpieczeństwo kryptosystemu powinno zależeć wyłącznie od tajności jego klucza, natomiast powinno być niezależne od zachowania tajności jakiejkolwiek innej części kryptosystemu, takiej jak:

- algorytm szyfrowania,
- kanał przesyłania wiadomości,
- urządzenie szyfrujące / deszyfrujące.

Nieprzestrzeganie zasady Kerckhoffsa skutkuje na ogół osłabieniem kryptosystemu.

Dalsze zasady bezpieczeństwa

- Nie wolno lekceważyć przeciwnika.
- Nie wolno opierać bezpieczeństwa systemu kryptograficznego na tajności algorytmu.
- Nie należy poprawiać skutecznie działających systemów kryptograficznych.
- Bezpieczeństwo danego kryptosystemu może kompetentnie ocenić tylko kryptoanalityk.
- Należy zawsze brać pod uwagę możliwość popełnienia błędów kryptograficznych lub naruszenia dyscypliny szyfrowania.
- Prawidłowe stosowanie systemu kryptograficznego nie zwalnia ze stosowania innych zabezpieczeń.

Najczęstsze błędy popełniane w czasie szyfrowania

- Równoczesna transmisja tekstu tajnego i jawnego.
- Użycie tego samego klucza do zaszyfrowania dwóch różnych tekstów jawnych.
- Użycie dwóch różnych kluczy do zaszyfrowania tego samego tekstu jawnego.
- Powtarzanie stereotypowych zwrotów w szyfrowanym tekście.
- Używanie zbyt krótkich haseł i kluczy.
- Używanie haseł i kluczy, które łatwo odgadnąć.
- Używanie znaków interpunkcyjnych, a w szczególności znaku spacji.
- Poprawność ortograficzna i stylistyczna.

Typy ataku kryptoanalitycznego

- **Atak siłowy** (zwany metodą *brute force*) polegający na przejrzeniu listy wszystkich możliwych kluczy.
- **Atak tylko z tekstem zaszyfrowanym.** Wymaga stosowania technik kryptoanalitycznych dostosowanych do konkretnego algorytmu szyfrowania.
- **Atak ze znanym tekstem jawnym.** Kryptoanalityk dysponuje parą *tekst jawny–tekst tajny*.
- **Atak z wybranym tekstem jawnym.** Kryptoanalitykowi udało się spowodować, aby został zaszyfrowany wybrany przez niego tekst jawny i teraz dysponuje parą takich tekstów.
- **Atak z wybranym tekstem tajnym.** Kryptoanalitykowi udało się uzyskać dostęp do aparatury deszyfrującej i przy jej pomocy odszyfrować wybrany przez siebie tekst tajny.