Algorytmy Szyfrujące

Prezentacja LaTeX

Rafał Bocul, Marcin Kubański, Hiacynta Stypuła

11.06.2021

Plan prezentacji

- Wstęp
- Definicja algorytmu szyfrującego
- Rodzaje algorytmów
- Opis problemu
- Rozwiązanie problemu
- Podsumowanie
- Bibliografia

Wstęp

Ludzie od zawsze potrzebowali ukrywać jakieś informacje. Kryptografia była znana już za czasów Cesarstwa Rzymskiego, kiedy to sam Juliusz Cezar używał szyfrów do komunikacji ze swoimi znajomymi. W XVII wieku kryptografia pojawiła się w zastosowaniach wojskowych i jest stosowana do tej pory. Pierwotnie były to proste szyfry podstawieniowo - przestawieniowe.

Definicja algorytmu szyfrującego

Wraz z rozwojem technologii pojawiły się bardziej zaawansowane i trudniejsze do złamania algorytmy szyfrujące.

Definicja algorytmu szyfrującego

Wraz z rozwojem technologii pojawiły się bardziej zaawansowane i trudniejsze do złamania algorytmy szyfrujące.

Algorytm szyfrujący – funkcja matematyczna, dzięki której możliwa jest zmiana zwykłego tekstu w zakodowaną wiadomość. Zakodowany tekst to szyfrogram, natomiast wiadomość przed szyfrowaniem to tekst jawny.

Rodzaje algorytmów

Ze względu na wykorzystanie liczby kluczy wyróżniamy:

- algorytmy symetryczne, które podzielić można na dwa typy: strumieniowe oraz blokowe;

Rodzaje algorytmów

Ze względu na wykorzystanie liczby kluczy wyróżniamy:

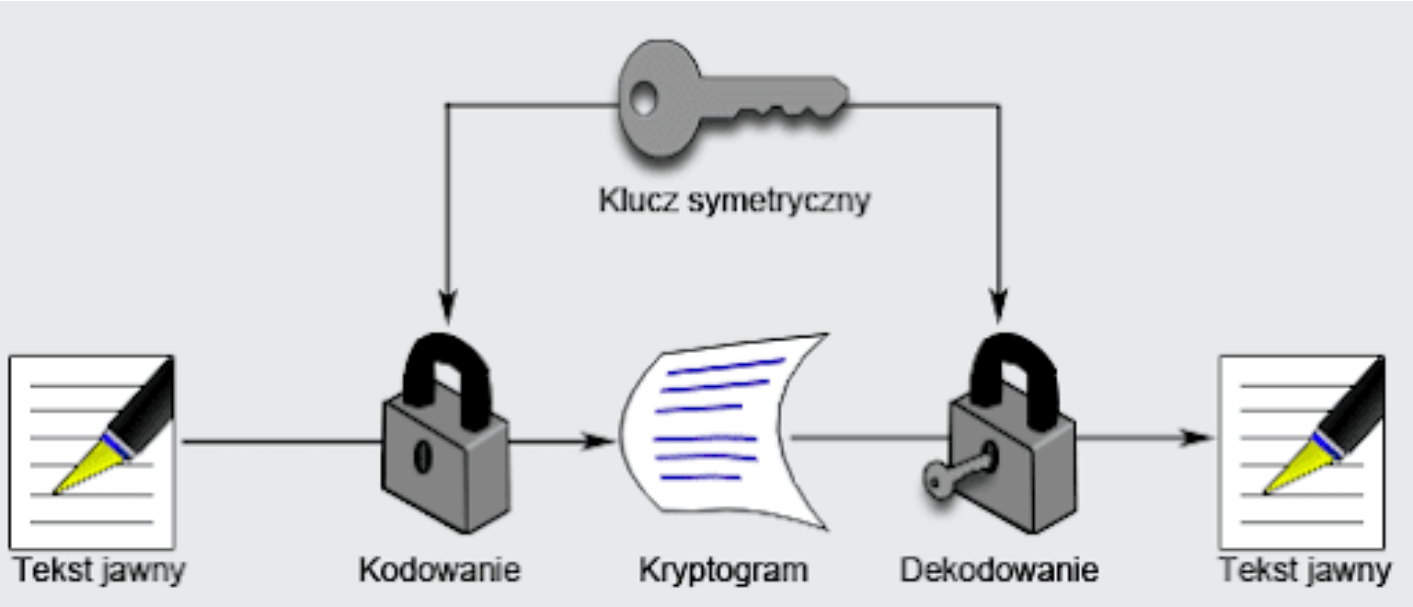
- algorytmy symetryczne, które podzielić można na dwa typy: strumieniowe oraz blokowe;
- algorytmy asymetryczne;

Rodzaje algorytmów

Ze względu na wykorzystanie liczby kluczy wyróżniamy:

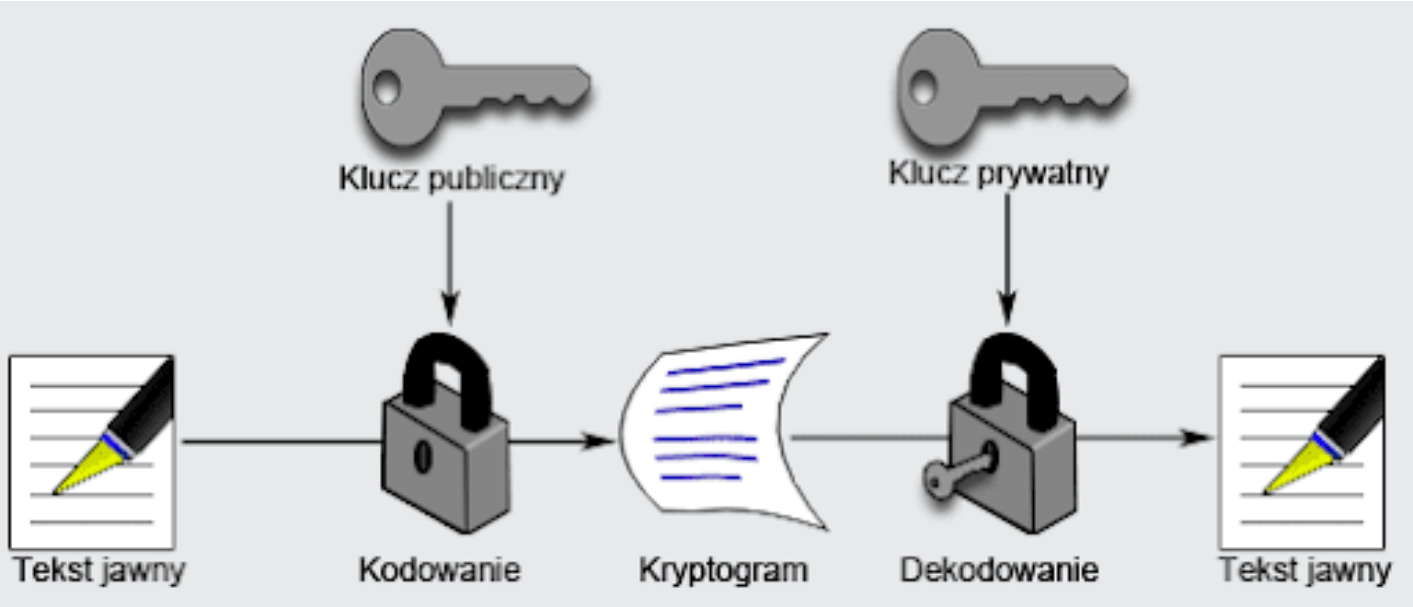
- algorytmy symetryczne, które podzielić można na dwa typy: strumieniowe oraz blokowe;
- algorytmy asymetryczne;
- algorytmy hybrydowe.

Rodzaje algorytmów



Rysunek: Szyfrowanie symetryczne

Rodzaje algorytmów



Rysunek: Szyfrowanie asymetryczne

Rodzaje algorytmów

Wśród najbardziej znanych algorytmów wyróżniamy:

- Data Encryption Standard (**DES**)

Rodzaje algorytmów

Wśród najbardziej znanych algorytmów wyróżniamy:

- Data Encryption Standard (**DES**)
- Advanced Encryption Standard (**AES**)

Rodzaje algorytmów

Wśród najbardziej znanych algorytmów wyróżniamy:

- Data Encryption Standard (**DES**)
- Advanced Encryption Standard (**AES**)
- Algorytm Rivesta-Shamira-Adlemana (**RSA**)

Rodzaje algorytmów

Wśród najbardziej znanych algorytmów wyróżniamy:

- Data Encryption Standard (**DES**)
- Advanced Encryption Standard (**AES**)
- Algorytm Rivesta-Shamira-Adlemana (**RSA**)
- Message-Digest Algorithm 5 (**MD5**)

Rodzaje algorytmów

Wśród najbardziej znanych algorytmów wyróżniamy:

- Data Encryption Standard (**DES**)
- Advanced Encryption Standard (**AES**)
- Algorytm Rivesta-Shamira-Adlemana (**RSA**)
- Message-Digest Algorithm 5 (**MD5**)
- Secure Sockets Layer (**SSL**)

Opis problemu

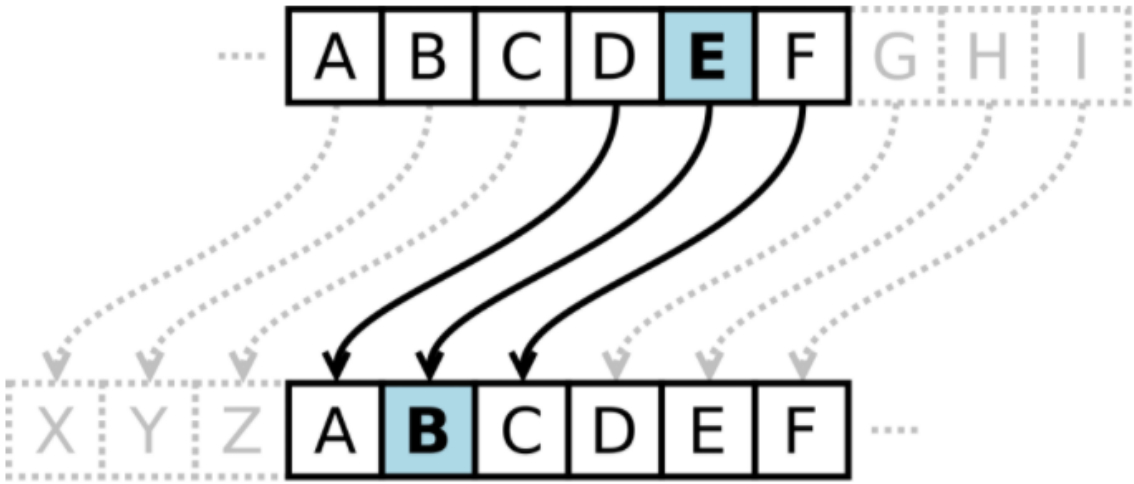
Współczesna technologia pozwala nam na bardzo szybki dostęp do informacji. Aby uniemożliwić osobom niepowołanym dostęp do wrażliwych danych, powstał proces zwany szyfrowaniem. Wraz z rozwojem techniki rosną także możliwości łamania algorytmów szyfrujących. Co za tym idzie, trzeba również doskonalić metody zabezpieczeń.

Opis problemu

Jednym z dostępnych rozwiązań jest zastosowanie algorytmu szyfrującego. W naszym programie zaimplementowaliśmy trzy algorytmy szyfrujące o różnym stopniu zabezpieczeń: **Szyfr Cezara**, **ROT13** i **RSA**. Naszym celem jest sprawdzenie, który z nich jest najtrudniejszy do złamania.

Rozwiązanie problemu

Szyfr Cezara to szyfr podstawieniowy, w którym każda litera tekstu jawnego zostaje zamieniona na literę oddaloną od niej o trzy pozycje.



Rysunek: Szyfr Cezara

Rozwiązanie problemu

ROT13 jest odmianą Szyfru Cezara. Jego działanie opiera się na tym samym algorytmie. Różni się jedynie wartością, służącego do szyfrowania i deszyfrowania tekstu, klucza. Funkcję klucza pełni liczba znaków.

Rozwiązanie problemu

Algorytm Rivesta-Shamira-Adlemana (**RSA**) opiera się utworzeniu dwóch powiązanych kluczy: publicznego oraz prywatnego, a następnie wykorzystywanie ich w celu ochrony treści przekazywanych wiadomości. Klucz publiczny jest powszechnie znany i każdy może za jego pomocą zaszyfrować dowolną wiadomość. Natomiast jedynie posiadacz klucza prywatnego może odszyfrować otrzymane szyfrogramy.

Rozwiązanie problemu

Najprostszym algorytmem do złamania okazał się Szyfr Cezara, a nieco trudniejszym ROT13.

Spośród wykorzystanych w naszym programie algorytmów szyfrujących najbezpieczniejszym okazał się algorytm RSA.

Potwierdziły się więc nasze założenia odnośnie siły ich zabezpieczeń.

Podsumowanie

Szyfr Cezara, podobnie ROT13, jak każda technika podmieniająca pojedyncze litery alfabetu na inne, niestety nie oferuje żadnego bezpieczeństwa komunikacji, jako że zakodowane słowa przybierają formę innych słów w tekście oryginalnym (niezakodowanym). W skrajnym przypadku może dojść jedynie do zamiany słów miejscami.

W przypadku kryptografii wykorzystującej algorytm RSA, klucz publiczny tworzony jest na podstawie klucza prywatnego oraz wyjątkowo trudnego do złamania iloczynu losowo wybranych liczb pierwszych. Jego użycie pozwala uniknąć słabości szyfrowania symetrycznego, w którym klucz tajny jest współdzielony przez obie strony komunikacji (tzw. problem dystrybucji klucza).

Podsumowanie

Reasumując, w dobie wszech dostępnej wiedzy, znajdującej się w zasobach sieciowych, każdy może zostać hakerem. A więc każdy nieostrożny użytkownik internetu może stać się ich ofiarą. Dlatego ważne jest, aby odpowiednio chronić swoje dane, których wolelibyśmy nie udostępniać.

Bibliografia

[1]https://www.eauditor.eu/
zdalne-szyfrowanie-dyskow-z-wykorzystaniem-bitlockera-3/
[2]http://ekryptografia.pl/kryptografia/szyfry-asymetryczne/
[3]http://ekryptografia.pl/kryptografia/szyfry-symetryczne/
[4]https://mfiles.pl/pl/index.php/Algorytmy_szyfrowania
[5]https://www.politykabezpieczenstwa.pl/pl/a/
jakie-sa-najpopularniejsze-metody-szyfrowania-danych
[6]http://www.pg17.idl.pl/projekty/kryptografia/rsp/www/
historia.html
[7]https://www.emojipng.com/preview/787938

Dziękujemy za uwagę!