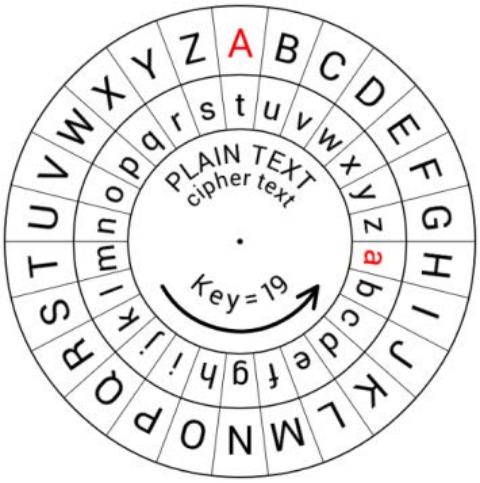
Politechnika Krakowska
im. Tadeusza Kościuszki

Programowanie dla fizyków

Raport – Algorytmy szyfrujące

Autorzy:
Bocul Rafał,
Kubański Marcin,
Stypuła Hiacynta

11 czerwca 2021



Spis treści

1. Wstęp

2. Definicja algorytmu szyfrującego

3. Rodzaje algorytmów

4. Opis problemu

5. Rozwiązanie problemu

6. Podsumowanie

7. Bibliografia

1. Plan prezentacji

Na początku prezentacji przybliżono zagadnienie algorytmu szyfrującego i wytłumaczono jego definicję, a następnie zapreentowano jego najpopularniejsze typy. W kolejnych punktach prezentacji przedstawiono problem oraz jego rozwiązanie.

2. Wstęp

Ludzie od zarania dziejów mieli potrzebę by ukryć jakieś informacje. Za jedną z najstarszych form szyfrowania uważa się hieroglify, które zdobiły ściany egipskich świątyń i grobowców. 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.

3. Definicja algorytmu szyfrującego

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

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

4. Rodzaje algorytmów

Algorytmy szyfrujące możemy podzielić ze względu na wykorzystanie typu klucza. Wyróżniamy:

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

Szyfry symetryczne, w odróżnieniu od szyfrów asymetrycznych, charakteryzują się tym, iż do szyfrowania oraz deszyfrowania używany jest identyczny klucz. Za pomocą tego klucza nadawca szyfruje wiadomość, którą następnie przesyła odbiorcy zwykle niezabezpieczonym kanałem. Problem pojawia się gdy nadawca musi przekazać odbiorcy klucz niezbędny do odszyfrowania wiadomości. To właśnie na tym kluczu opiera się bezpieczeństwo całego algorytmu, dlatego tak ważnym jest utrzymanie go w ścisłej tajemnicy i wysłanie do odbiorcy bezpiecznym kanałem. Po otrzymaniu klucza, odbiorca jest w stanie odczytać otrzymaną wiadomość. Dlatego bezpieczeństwo szyfrów symetrycznych zależy przede wszystkim od jakości bezpieczeństwa klucza.

W algorytmach blokowych jednostką przetwarzania jest grupa bitów zwana blokiem. Standardowe rozmiary bloku oraz kluczy to 64, 128, 192 lub 256 bitów, aczkolwiek we współczesnych czasach klucze o rozmiarze poniżej 128 bitów nie zapewniają już wystarczającego bezpieczeństwa.

Szyfry strumieniowe w odróżnieniu od blokowych nie wymagają oczekiwania na zaszyfrowanie całego bloku danych, lecz szyfrują pojedyncze znaki. Najczęściej jednostką przetwarzania jest 1 bit lub bajt. W szyfrach asymetrycznych używane są dwa klucze: klucz publiczny (klucz

jawny, który może zostać upubliczniony) i klucz prywatny. Wiadomość zaszyfrowaną za pomocą klucza publicznego odszyfrować można jedynie za pomocą klucza prywatnego. Analogicznie jeśli wiadomość zaszyfrowana zostanie za pomocą klucza prywatnego jej odszyfrowanie możliwe jest jedynie po użyciu klucza publicznego.

Wspólne stosowanie elementów kryptografii symetrycznej i asymetrycznej jest możliwe. Rozwiązanie to określa się mianem szyfrowania hybrydowego. Dane właściwe szyfruje się metodą symetryczną, zaś użyty do tego klucz zabezpiecza przed przechwyceniem za pomocą klucza publicznego odbiorcy.

5. Typy algorytmów szyfrujących

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**)

DES był jednym z najpopularniejszych blokowych szyfrów symetrycznych. Został wynaleziony już we wczesnych latach ’70 w IBM i został uznany za standard federalny w USA. Obecnie już od kilku lat uznawany jest za algorytm, który nie zapewnia odpowiedniego bezpieczeństwa, a to głównie ze względu na niewielką długość klucza (56 bitów).

AES to szyfr symetryczny, który jest oparty na algorytmie Rijndaela, czyli rodzinie szyfrów o różnych długościach klucza oraz różnych wielkościach bloków. Algorytm ten używa klucza o długości 128, 192 lub 256 bitów. W procesie szyfrowania tekst jawny jest dzielony na bloki 128-bitowe. Bloki przedstawiane są jako szeregowane kolumnami macierze 4 bajty $\times$ 4 bajty.

RSA to algorytm asymetryczny, umożliwia więc utworzenie dwóch powiązanych kluczy: klucza publicznego oraz klucza prywatnego w celu ochrony treści przekazywanych wiadomości. Klucz ma zwykle długość od 1000 do 4000 bitów.

MD5 to algorytm haszujący, wykorzystujący proces tworzenia danych wyjściowych o stałym rozmiarze z danych wejściowych o zmiennym rozmiarze. I choć stosowanie go w nowych rozwiązaniach nie jest zalecane, to nadal może zapewniać satysfakcjonujący poziom bezpieczeństwa.

SSL jest protokołem sieciowym używanym do bezpiecznych połączeń internetowych. Certyfikat SSL zapewnia poufność transmisji danych przesyłanych przez Internet. Został przyjęty jako standard szyfrowania na stronach WWW. Długość klucza wynosi 2048 bitów.

6. 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.

Jednym z dostępnych rozwiązań jest zastosowanie algorytmu szyfru-

jącego. 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.

7. Rozwiązanie problemu

Szyfr Cezara jest to szyfr podstawieniowy, w którym każda litera tekstu jawnego zostaje zamieniona na literę oddaloną od niej o trzy pozycje. Każdą zaszyfrowaną wiadomość trzeba kiedyś rozszyfrować. W szyfrze Cezara znajduje się literę stojącą w alfabecie trzy miejsca bliżej, czyli stosujemy ten sam algorytm szyfrowania, ale z innym kluczem. Do szyfrowania używamy klucza +3, natomiast do rozszyfrowania klucza -3. Dlatego gdy jest znany klucz szyfrowania, to znany jest również klucz rozszyfrowania. Można więc powiedzieć, że jest to ten sam klucz, pod warunkiem, że pominiemy jego znak.

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. W ogromnym uproszczeniu długość klucza to liczba możliwych kombinacji klucza. Jeśli przestrzeń możliwych kluczy jest niewielka, haker może wypróbować kolejno wszystkie klucze. W szyfrowaniu przy użyciu komputera można ustalić długość klucza na podstawie liczby bitów (np. klucz 40-bitowy, 56-bitowy, 128-bitowy, 256-bitowy). Wraz z długością klucza wzrasta liczba możliwych kombinacji – zupełnie jak w wypadku hasła. Szyfrowanie 128-bitowe jest bilion razy silniejsze od szyfrowania 40-bitowego.

Algorytm **RSA**, jak już wspomniano wcześniej, 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.

Spośród wykorzystanych w naszym programie algorytmów szyfrujących, najprostszym do złamania okazał się Szyfr Cezara, a nieco trudniejszym ROT13. Najbezpieczniejszym okazał się algorytm RSA. Potwierdziły się więc nasze założenia odnośnie siły ich zabezpieczeń.

8.Podsumowanie

Szyfr Cezara przewiduje tylko 26 kluczy. Wypróbowanie ich (nawet metodą ręczną) zajmuje bardzo mało czasu. Dlatego można szybko odczytywać szyfrogramy stworzone tą metodą bez konieczności mozolnego poszukiwania klucza. 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). Współcześnie złamanie szyfru RSA o dwa tysiące czterdziesto ośmio bitowym kluczu, przy pomocy domowego komputera zajęłoby miliardy lat, natomiast gdyby użyto do tego zadania komputera kwantowego byłoby to już zaledwie 8 godzin.

Reasumując, w dobie wszech dostępnej wiedzy, znajdującej się w zaso-

bach 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.

9. Bibliografia

Literatura

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