BST wykład 3 – 15.03.2022

Szyfry numeryczne - strumieniowe, blokowe

Wlasnosci bezpiecznych szyfrow

Algorytmy DES, AES

Tryby szyfrowania

1. Szyfr symetryczny

Symetryczny proces szyfrowania danych, schemat na slajdzie,

Jeden klucz do szyfrowania i deszyfrowania, cale bezpieczeństwo opiera się na tym kluczu.

Mieszanie bitami/danymi

Algorytm jest jawny,

Zaleta: szyfry symetryczne najpopularniejsze – bo maja wielka wydajność

Dziela się na strumieniowe i blokowe (sposób przetwarzania danych) (asymetryczne – blokowe)

1. **strumieniowe**

działa tak ze mamy strumien danych i szyfrujemy bit po bicie

dodawanie modulo 2 (xor)

bit tekstu jawnego xor z bitem klucza i dostajemy bit szyfrogramu

tak samo dlugi klucz jak tekst jawny

LFSR- zestaw rejestrow, niektóre polaczone ze sobą (działanie xor), za pomocą takiego rejestru generujemy dlugi ciag binarny, jeśli projektujemy taki rejestr do generowania klucza, trzeba tak dobrac polaczenia żeby nie było jakiejś krótkiej petli i żeby ilość rejestow była dość duza, żeby ciagi żeby sekwencja nie powtarzala się za szybko, nadawca przesyla tylko pierwsze wartości rejestrow a odbiorca jest w stanie odczytac cały ciag binarny klucza,

1. **blokowe**

szyfrujemy caly blok danych/bitow,

funkcja przeksztalcajaca blok danych w szyfrogram musi być odwracalna żeby można było wiadomość odszyfrować,

bloki powinny być jak największe z punktu widzenia bezpieczeństwa,

duze bloki to także mala efektywność/wydajność

nie jesteśmy w stanie zaszyfrować kilku bajtow jeśli blok ma dlugosc 12tysiecy bitow,

trzeba znaleźć kompromis miedzy bezpieczeństwem a wydajnoscia,

typowa dlugosc bloków 128b / 256b

zjawisko „rozpraszanie” – pojedynczy element tekstu jawnego/klucza powinien mieć wpływ na wiele elementow szyfrogramu,

permutacja bitów (mieszanie bitami), klucz kryptograficzny nie może być widoczny w szyfrogramie,

przestawienia i permutacje sa w stanie zapewnić rozpraszanie i zamieszanie, jak na przykład Enigma.

zjawisko „zamieszanie” – ukrywanie związku miedzy statystyka szyfrogramu a tekstem jawnym i zastosowanym kluczem.

Co oznacza ze algorytm jest bezpieczny?

ma wieksza cyferke w nazwie, dluzsze klucze, testy testujące szyfrgramy (jak bardzo wygladaja na pseudolosowe)

Szyfrogram powinien zawierac tyle samo zer co jedynek,

Lawinowosc zmian – niewielkie zmiany na wejściu powinny skutkować wielkimi zmianami na wyjściu algorytmu,

Nieliniowosc – szyfry powinny być jak najbardziej nieliniwe

Zupełność – każdy bit wyjściowy zależy od każdego bitu wejściowego,

Niezaleznosc miedzy bitowa

Odpowiedni rozkład wartości profilu XOR

Brak korelacji, pseudolosowy ciag bitow…

Algorytm DES

- pierwszy zaliczony do współczesnych algorytmow szyfrograficznych

- algorytm blokowy

- nie jest uważany za bezpieczny

- blok 64 bity - dzielony na dwie części po 32b

- wykonywane jest 16 cykli w których dane sa mieszane, laczone kluczem szyfrograficznym, dzieje się to tylko z prawa polowka, lewa strona jest przepisywana ?? tam się dzieje cos dalej jeszcze…

- 56 bitowy klucz (bardzo krotki) – można złamac brut forcem

Szyfr AES

- symetryczny, bardzo szybki, wydajny

- jest odpowiedzia na szyfr DES, sa bardziej bezpieczne,

- klucz 128 bitow (stabilnie), możliwe inne dlugosci kluczy – 192, 256

- tekst jawny – 128 bitow, szyfrogram – 128 bitow

- w zaleznosci od wyboru dlugosci klucza, im dluzszy tym więcej rund algorytmu będzie stiosowane im więcej tym bardziej bezpiecznie,

- shiftroats = permutacja,

- 4 proste funkcje powtarzane cyklicznie daja super algorytm

Jak szyfrować duze ilości danych??

- ECB – electronic codebook (zdradza tekst jawny)

- CBC – Cipher Block Chaining (dodatkowe dzialania xor)

- dzielimy tekst jawny na bloki o dlugosci klucza

- szyfrujemy a przy odczytywaniu składamy do kupy i mamy - włala