RGB to czerwony,zielony,niebieski i tych kolorow kodujemy reszte

BST

**Poufnosc** metoda ochrony danych

Wiaze się z ograniczeniem dostępu do informacji. Dla jednej grupy są znane, dla innej nie. **Steganografia** – ukrywanie istnienia danych, jedno z podejść do poufności. Jest mało efektywne, informacje musimy ukryc w jakiejś innej informacji. Jest dużo tego ‘tla’.

Rozwiazania steganograficzne można podzielić na 3 grupy:

Ukrywanie info w tekście

Ukrywanie info w plikach multimedialnych

Ukrywanie info w protokolach

Kryptografia klasyczna -

**Szyfrowanie** – zmiana postaci daych w ten sposób, aby ta zmieniona postac była zupełnie nieczytelna dla osob postronnych, drugie podejście do poufności.

Szyfrowanie powinno być odwracalne.

Pojecia do szyfrowania:

\_\_\_\_\_

Tekst jawny – przed zaszyfrowaniem

Szyfrogram – wiadomość już zaszyfrowana

Klucz kryptograficzny – za jego pomocą możemy ujawnić jak działa szyfrogram.

Szyfr – metoda/algorytm, poprzez który przekształcamy dane. Zazwyczaj jest jawny.

Szyfrowanie/deszyfrowanie

Kryptoanaliza – proba odczytania informacji zaszyfrowanej bez posiadania odpowiedniego klucza.

Atak silowy – brute force – sprawdzenie wszystkich możliwych kombinacji.

\_\_\_\_\_

Algorytmy szyfrujące:

NA PREZCE, POZA TYM:

Szyfry przestawieniowe, szyfry podstawieniowo-przestawieniowe (Stosowanie obecnie)

Szyfr homofoniczny polega na tym, ze kazda literka ma iles tam odpowiadających jej liczb, możemy dla tej samej litery stosować inne liczby. Tez podstawiamy jeden znak za jeden znak tyle, ze z jakiejś grupy (w tym przypadku liczb np. )

Szyfr poligramowy – mapowanie wieloznakow, np. szyfrowanie par liter. Przykład: szyfr playfair. Wpisujemy litery do macierzy 5x5. Wpisujemy jakiś klucz (na slajdzie Marcin), a następnie dopisujemy rosnąco pozostale litery. Bierzemy dwie litery w taki sposób, aby znajdowaly się po przeciwnych rogach i bierzemy dwie litery, które znajduja się po drugiej przekątnej.

Szyfr Vigenere’a – trudny xd. Robimy macierz z wszystkich liter alfabetu. Tez potrzebujemy jakiegoś wyrazu jako klucza. Chodzi o przecięcia „klucza” z literami słowa, które chcemy zaszyfrować.

Szyfr Vernama – nie da się zlamac brute-forcem. Bez znajomości klucza nie ma jednoznaczności.

Szyfry przestawieniowe: