Szyfr Cezara - (zwany szyfrem przesuwającym ) . Jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego (niezaszyfrowanego) zastępowana jest inną, oddaloną od niej o stałą liczbę pozycji w alfabecie,

SCHEMAT SZYFROWANIA SYMETRYCZNEGO:

(Nadawca) Orginalna informacja --> Klucz symetryczny --> Zaszyfrowana informacja --> Klucz symetryczny --> Orginalna informacja (Odbiorca)

Klucz - w szyfrowaniu stanowi informacje, dzięki której można zaszyfrować lub odszyfrować informacje właściwą lub dane.

Kryptografia symetryczna - wykorzystują klucze znane nadawcy i odbiorcy.

SCHEMAT SZYFROWANIA ASYMETRYCZNEGO:

(Nadawca) Orginalna informacja --> Szyfrowanie kluczem publicznym --> Zaszyfrowana informacja --> Odszyfrowywanie kluczem prywatnym --> Orginalna informacja (Odbiorca)

W szyfrowaniu asymetrzycznym używa się kluczy publicznych i prywatnych. Klucz prywatny pełni funkcję swoistego podpisu nadawcy i powinnien być znany tylko jemu.

Klucz prywatny i publiczny stanowią unikatową parę. Funkjce kluczy mogą byc łączone, np. informacja najpierw jest podpisywana kluczem prywatnym nadawcy apotem szyfrowanym

kluczem publicznym odbiorcy. Metoda ta jest zazwyczaj stosowana dla zwiększenia bepieczeństwa, kiedy dla każdego połączenia generuje się nowy klucz.

ASCII jest to standard kodowania znaków w komputerach i w Internecie. (7 bitowy system kodowania znaków).

Generowanie losowych liczb:

rand()%15+5 = (wynik i zakres losowania) = % wyznacza zakres (0-(n-1) = n to 15) (0+5 i 14+4 zakres 5-19)

Szyfrowanie zachłanne czyli kody Huffmana:

Kompresja ta polega na zastępowanie znaków kompresowanego pliku krótszymi kodami, dzięki czemu wynikowy ciąg bitów jet znacznie krótszy od wejściowego.

Litera A w ASCII:

A = 01000001

po zakodowaniu A = 000

mamy zmniejszenie o około -50%.

Zakoduj wiadomość EDBCB, stosując kodowanie Hafftmana wiedząc że prawdopodobieństwo wystąpienia liter wiadomośći to: A-10% B-10% C-15% D-20% E-45%.

1 011 001 010 001

Szyfrowanie przestawieniowe + przestawieniowe z tablicą(wzór: n^2 <= |a|)

Tablica - w jednej zmiennej pare wartości

int nazwa\_tablicy[] = {wartosc1,wartosc2,wartosc3, ...}

int nazwa\_tablicy[x]; // x tyle ile wartosci zaczynaja od zera.

value round floor ceil

2.3 2.0 2.0 3.0

3.8 4.0 3.0 4.0

5.5 6.0 5.0 6.0

-2.3 -2.0 -3.0 -2.0

-3.8 -4.0 -4.0 -3.0

-5.5 -6.0 -6.0 -5.0

Błąd bezwzględny: Δx=|x−x0|

gdzie:

x - to dokładna wartość

x0 - to zmierzona wartość

Błąd względny: δ=(Δx/x)\*100%=(|x−x0|/x)\*100% , i δ=Δx/x=|x−x0|/x

gdzie:

Δx - to błąd bezwzględny pomiaru

x - to dokładna wartość

x0 - to zmierzona wartość

Przkład:

Na początku liczymy błąd bezwzględny:

Δx=|x−x0|=|122,5−120|=2,5

Teraz obliczymy błąd względny:

δ=Δx/x=2,5/122,5=1/49

Wyrazimy jeszcze błąd względny w procentach:

δ=Δx/x\*100%=1/49\*100%=100/49%≅2,04%