Лабораторна робота № 1 Гешування

Група КП-М922в

Автор Савичев О.В.

Мета

Дослідити принципи роботи гешування.

Завдання

Дослідити існуючі механізми гешування. Реалізувати алгоритм гешування SHA (будь-якої версії).

Довести коректність роботи реалізованого алгоритму шляхом порівняння результатів з існуючими реалізаціями (напр. утилітою sha1sum).

Хід роботи

SHA-2 (англ. Secure Hash Algorithm Version 2 — безпечний алгоритм хешування, версія 2) — збірна назва односторонніх геш-функцій SHA-224, SHA-256, SHA-384 і SHA-512. Геш-функції призначені для створення «відбитків» або «дайджестів» повідомлень довільної бітової довжини.

Початкове повідомлення після доповнення розбивається на блоки, кожен блок — на 16 слів. Алгоритм пропускає кожен блок повідомлення через цикл з 64-ма ітераціями (раундами). На кожній ітерації 2 слова перетворюються, функцію перетворення задають інші слова. Результати обробки кожного блоку складаються, сума є значенням геш-функції.

Доповнення повідомлення до довжини, що є кратною 512

```
int k = 0;
while ((msg.Length * 8 + 8 + k + 64) % 512 != 0) { k += 8; }
byte[] fitMsg = new byte[(msg.Length * 8 + 8 + k + 64) / 8];

msg.CopyTo(fitMsg, 0);
fitMsg[msg.Length] = 0x80; // 0x80 = b10000000 = the bit 1
for (int i = 1; i < (1 + (k / 8)); i++)
    fitMsg[msg.Length + i] = 0x00;
l.CopyTo(fitMsg, msg.Length + 1 + (k / 8));
```

Розбиття на блоки по 64 байти

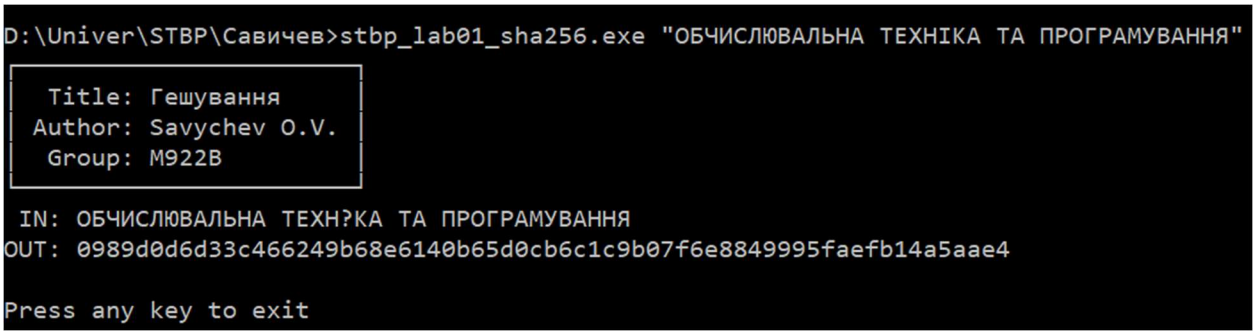
```
int n = fitMsg.Length / 64; // 64 bytes = 512 bits
var M = new byte[n][];
for (int i = 0; i < n; i++)
{
    var t = new byte[64];
    for (int j = 0; j < 64; j++)
        t[j] = fitMsg[(i * 64) + j];
    M[i] = t;
}
```

Основний цикл конвейера компрессора

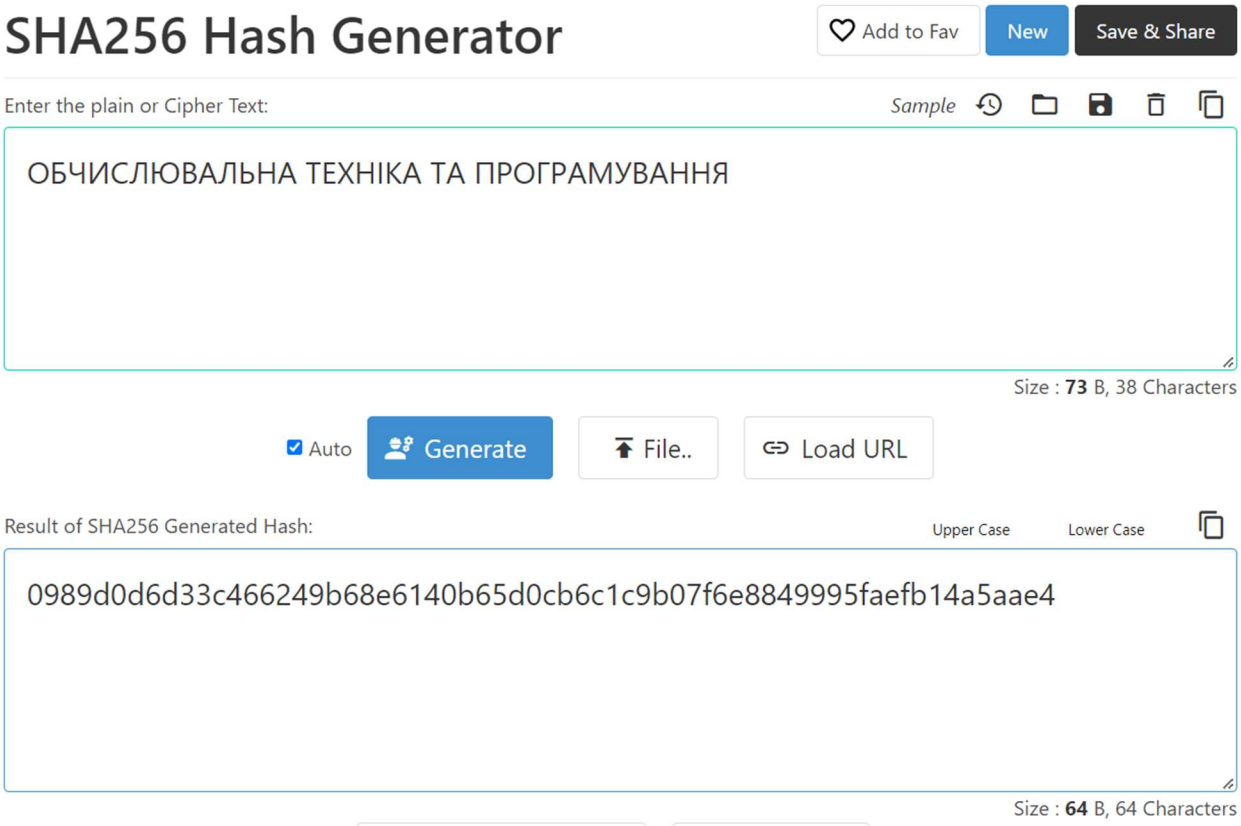
```
for (int i = 0; i < 64; i++)
{
    T1 = h + Z1(e) + Ch(e, f, g) + K[i] + W[i];
    T2 = Z0(a) + Maj(a, b, c);
    h = g;
    g = f;
    f = e;
    e = d + T1;
    d = c;
    c = b;
    b = a;
    a = T1 + T2;
}
```

Результати роботи

Результати роботи моєї реалізації Результати роботи моєї реалізації



Порівняння з онлайн-сервісом обчислення SHA-256 https://codebeautify.org/sha256-hash-generator



Висновок

Дослідив принципи роботи гешування. Реалізував алгоритм гешування SHA-256.