Десислава Дончева 71910

СД - проект 4

Алгоритми:

1. SHA 256 (имплементиран във файлове: sha256.cpp и sha256.hpp)

Използвана е готова имплементация!
Използван е, защото:
1. Изчислената хеш стойност най-често бива използвана за проверка на цялостта на данни или защита на информация, например потребителски пароли или друга поверителна информация.
2. Сигурен хеширащ алгоритъм е.
3. 256 бита са достатъчни за променливата password (char[100])
4. Няма намерени колизии.
5. Приложен във **void Hash::calcHash(char* password)** (“Helpers.cpp”, 57 line)

2. Speck (cipher) algorithm (имплементиран във файлове: speck.hpp и speck.cpp)

Използван е, защото:
1. Макар и да е “лек” шифър, той е стабилен
2. Speck поддържа различни размери на блокове и ключове. Блокът винаги е две думи, но думите могат да бъдат с размер 16, 24, 32, 48 или 64 бита (в нашия случай работи за блокове от 64 бита)
3. Приложен във **void ArchFile::Encrypt(uint8_t *inBlock, uint8_t *outBlock, int BlockSize, char* password)** (“ArchFile.cpp”, 357 line)