Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование блочных шифров

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Теоретическая часть**

В симметричных системах отправитель и получатель используют один и тот же ключ. К блочным шифрам относятся DES, FEAL, RC2, Blowfish, TEA, RC5, CAST-128, XTEA, XXTEA, RC6 и AES. Эти алгоритмы блочных шифров (БШ) основаны на подстановках и перестановках, являясь комбинационными и симметричными. Блочное шифрование разбивает исходный текст на равные блоки, к которым применяется одинаковая процедура шифрования или расшифрования, состоящая из повторяющихся раундов преобразований.

Основные требования к блочным шифрам:

* Незначительное изменение исходного сообщения должно значительно изменять зашифрованное сообщение.
* Устойчивость к атакам по выбранному тексту.
* Возможность реализации на различных платформах.
* Простота алгоритмов и низкая вероятность программных ошибок.
* Возможность модификации для повышения криптостойкости.

Сеть Фейстеля подразумевает ячеистую топологию, где одна ячейка соответствует одному раунду шифрования или расшифрования. При шифровании сообщение делится на блоки фиксированной длины (64 или 128 бит), каждый из которых делится на два подблока: левый (L0) и правый (R0).

Блоки преобразований:

* Блок подстановок (S-блок): преобразует n-разрядное двоичное число в одноразрядный сигнал.
* Блок перестановок (P-блок): изменяет положение цифр.

Симметричная криптография. Алгоритм DES: Алгоритм DES использует подстановку и перестановку данных в 16 раундах. Один блок данных длиной 64 бита обрабатывается 16 раз с новым ключом на каждом этапе, где биты ключа сдвигаются, а из 56 бит выбираются 48 бит. Блок перестановок изменяет положение цифр, являясь линейным устройством.

Существуют несколько реализаций алгоритма 3DES:

* DES-EEE3: шифрование трижды с тремя разными ключами (шифрование-шифрование-шифрование).
* DES-EDE3: 3DES с операциями шифрование-расшифрование-шифрование с разными ключами.
* DES-EEE2 и DES-EDE2: аналогично предыдущим, но на первом и третьем шагах используется один и тот же ключ.

1. **Практическая часть**

Ниже представлены функции для шифрования и дешифрования DES. На рисунке 2.1 изображен алгоритм шифрования.



Рисунок 2.1 – метод множественной перестановки

Метод EncryptFile шифрует данные с использованием алгоритма DES и возвращает зашифрованные данные в формате Base64. Он принимает ключ и данные в виде байтового массива. Внутри метода создается MemoryStream для хранения зашифрованных данных и DESCryptoServiceProvider для выполнения шифрования. Ключ и вектор инициализации устанавливаются с использованием ASCII-кодировки ключа. Затем создается CryptoStream, через который данные записываются и шифруются. После завершения шифрования зашифрованные байты преобразуются в строку Base64 и возвращаются.

На рисунке 2.2 представлен код для расшифрования.

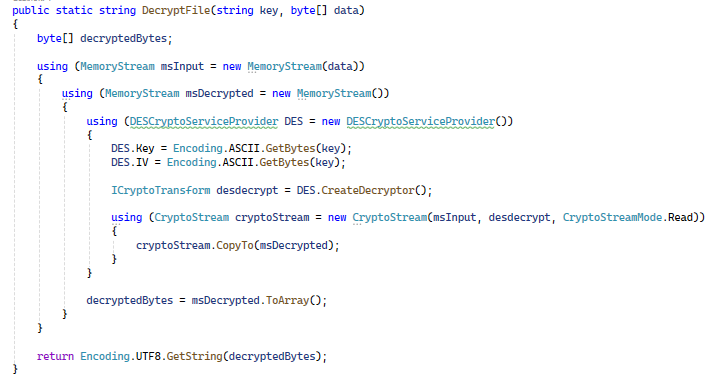


Рисунок 2.1 – метод множественной перестановки

Метод DecryptFile расшифровывает данные, зашифрованные алгоритмом DES, с использованием указанного ключа. Он принимает ключ и зашифрованные данные в виде байтового массива. Внутри метода создается MemoryStream для чтения зашифрованных данных и еще один MemoryStream для хранения расшифрованных данных. Затем создается DESCryptoServiceProvider для выполнения расшифровки. Ключ и вектор инициализации устанавливаются с использованием ASCII-кодировки ключа. Затем создается CryptoStream, через который данные копируются и расшифровываются. После завершения расшифровки расшифрованные байты преобразуются в строку UTF-8 и возвращаются.