Министерство образования Республики Беларусь

Учреждение Образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра ИИТ

Лабораторная работа № 8

По дисциплине «Криптографические методы защиты информации»

По теме «Блочные шифры. Режимы шифрования»

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| Куртумеров Д. А. |  | Шалёв Е. Г. |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_ |

Минск 2022

**1. Цель работы**

Изучить алгоритмы блочного шифрования – DES, AES; и их режимы – ECB, CBC, CTR.

**2. Ход работы**

Различия алгоритмов DES и AES:

* В DES открытый текст делится на две половины перед дальнейшей обработкой, в блоке AES нет разделения – весь блок обрабатывается целиком для получения зашифрованного текста.
* AES намного быстрее – способен шифровать большие файлы за доли секунды.
* Из-за небольшого размера разделяемого ключа, используемого в DES, он считается менее безопасным, чем AES. DES считается более уязвимым для атак методом перебора.
* AES является более гибким – допускает текст различной длины, включая 128, 192, 256 бит, тогда как DES позволяет шифровать текст с фиксированными 64 битами.

Разница между режимами шифрования:

ECB – это, по сути, первое поколение AES – самая базовая форма шифрования блочным шифром. Основная причина по которой не стоит использовать шифрование в режиме ECB заключается в том, что зашифрованные сообщения не будут являться семантически безопасными – то есть, простое наблюдение за шифротекстом, зашифрованным в режиме ECB, может привести к утечке информации об открытом тексте. В частности, проблема данного режима заключается в том, что шифрование одного и того же блока открытого текста всегда дает один и тот же блок шифрованного текста. Это может позволить злоумышленнику:

* Определить, идентичны ли два зашифрованных сообщения.
* Определить, имеют ли два зашифрованных сообщения общий префикс.
* Определить, имеют ли два зашифрованных сообщения другие общие подстроки, если эти подстроки выровнены по границам блоков.
* Определить, содержит ли одно зашифрованное сообщение повторяющиеся данные, например, длинные пробелы или нулевые байты, повторяющиеся поля заголовка или случайно повторяющиеся фразы в тексте.

|  |  |
| --- | --- |
|  |  |
| DES: ECB | AES: ECB |

Рис. 1. Изображения, зашифрованные с применением режима ECB.

CBC – это усовершенствованная форма блочного шифрования. При шифровании в режиме CBC каждый блок шифротекста зависит от всех блоков открытого текста, обработанных до этого момента. Таким образом самое большое преимущество CBC перед ECB заключается в том, что в режиме CBC одинаковые блоки не будут преобразовываться в одинаковый шифротекст. Это происходит потому, что вектор инициализации добавляет фактор случайности к каждому блоку. Хотя этот режим и является более безопасным, он не устойчив к потере блоков. Это происходит потому, что шифрование будущих блоков зависит от блоков предыдущих. Поэтому, если какой-либо блок будет потерян, шифрование всех последующих блоков будет невозможным. Также это означает, что шифрование блоков должно выполняться последовательно, а не параллельно. Однако расшифровка может выполняться параллельно.

|  |  |
| --- | --- |
|  |  |
| DES: CBC (первая попытка) | DES: CBC (вторая попытка) |

Рис. 2. Изображения, зашифрованные с применением режима CBC.

CTR – режим, в котором каждый шаг может выполняться параллельно. CTR похож на OFB, поскольку он также включает в себя XOR-пересечение последовательности векторов с блоками открытого и зашифрованного текстов. Основное различие заключается в том, как генерируются эти векторы. CTR использует случайный вектор инициализации для генерации потока ключей. Поскольку в режиме CTR блоки не зависят друг от друга, после генерации векторов можно параллельно выполнять как шифрование, так и дешифрование блоков. Отсутствие взаимозависимости также означает, что режим CTR устойчив к потере блоков. Режим CTR считается безопасным и эффективным для большинства целей. Серьезным недостатком CTR является то, что синхронный счетчик должен поддерживаться как на принимающей, так и на отправляющей стороне. Потеря этого счетчика может привести к неправильному восстановлению открытого текста.

|  |  |
| --- | --- |
|  |  |
| AES: CTR | AES: CTR |

Рис. 3. Изображения, зашифрованные с применением режима CTR.

**3. Выводы**

CTR кажется самым "безопасным" выбором из опробованных, но это не значит, что он полностью безопасен. Режим блочного шифра – это только часть общего протокола. Каждый режим имеет свои особенности и требует некоторых дополнительных систем для правильного использования, но в случае CTR разработка этих дополнительных систем несколько проще.