Российский университет дружбы народов имени Патриса Лумумбы

Факультет физико-математических и естественных наук Кафедра прикладной информатики и теории вероятностей

ДОКЛАД

на тему:

Шифры потока и блочные шифры.

Дисциплина: Информационная безопасность

Студент: Шутенко Виктория Михайловна

Группа: НФИмд-02-23

МОСКВА

2023 г.

Различают три основных способа шифрования: *поточные (потоковые) шифры, блочные шифры и блочные шифры с обратной связью*. Для классификации методов шифрования данных следует выбрать некоторое количество характерных признаков, которые можно применить для установления различий между этими методами. К таким признакам относятся:

• Выполнение операций с отдельными битами или блоками. Известно, что для некоторых методов шифрования знаком сообщения, над которым производят операции шифрования, является отдельный бит, тогда как другие методы оперируют конечным множеством битов, обычно называемым блоком.

• Зависимость или независимость функции шифрования от результатов шифрования предыдущих частей сообщения.

• Зависимость или независимость шифрования отдельных знаков от их положения в тексте. В некоторых методах знаки шифруются с использованием одной и той же функции независимо от их положения в сообщении, а в других методах, например при поточном шифровании, различные знаки сообщения шифруются с учетом их положения в сообщении. Это свойство называют позиционной зависимостью или независимостью шифра.

• Симметрия или асимметрия функции шифрования. Эта важная характеристика определяет существенное различие между обычными симметричными (одноключевыми) криптосистемами и асимметричными (двухключевыми) криптосистемами с открытым ключом. Основное различие между ними состоит в том, что в асимметричной криптосистеме знания ключа шифрования (или расшифровывания) недостаточно для раскрытия соответствующего ключа расшифровывания (или шифрования).

В табл. 2.13 приведены типы криптосистем и их основные характеристики.

Таблица 2.13

Основные характеристики криптосистем

Тип криптосистемы	Операции с битами или блоками	Зависимость от предыдущих знаков	Позиционная зависимость	Наличие симметрии функции шифрования
Поточного шифрования	Биты	Не зависит	Зависит	Симметричная
Блочного шифрования	Блоки	Не зависит	Не зависит	Симметричная или несимметричная
С обратной связью от шифротекста	Биты или блоки	Зависит	Не зависит	Симметричная

Потоковые алгоритмы преобразуют открытый текст в шифротекст по одному биту за операцию (рис. 2.27). Генератор потока ключей (иногда называемый генератором с бегущим ключом) выдает поток битов: k1, k2,..., ki. Этот поток ключей (иногда называемый бегущим ключом) и поток битов открытого

текста, p1, p2,..., pi, подвергаются операции XOR «исключающее или», и в результате получается поток битов шифротекста:

ci = pi $\oplus$ ki.

При расшифрировании операция XOR выполняется над битами шифротекста и тем же самым потоком ключей для восстановления битов открытого текста

pi = ci $\oplus$ ki.

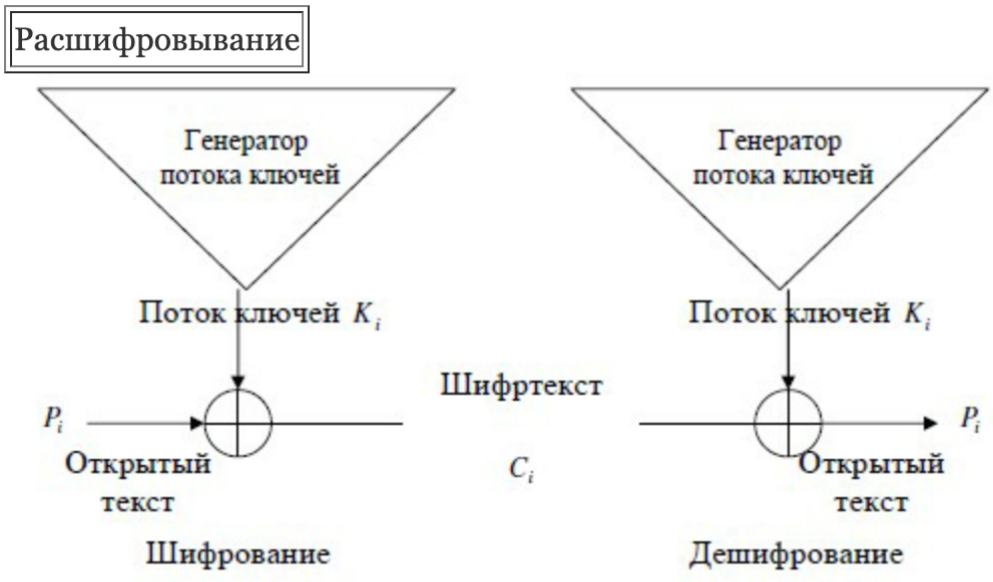

Рис. 2.27. Потоковый алгоритм

К достоинствам поточных шифров относятся высокая скорость шифрования, относительная простота реализации и отсутствие размножения ошибок. Недостатком является необходимость передачи информации синхронизации (синхропосылки) перед заголовком сообщения, которая должна быть принята до расшифровывания любого сообщения. Передачи информации синхронизации может создать угрозу криптостойкости системы. Поэтому часто используют дополнительный, случайно выбираемый ключ сообщения, который передается в начале сообщения и применяется для модификации ключа шифрования.
Поточные шифры широко применяются для шифрования преобразованных в цифровую форму речевых сигналов и оцифрованных данных, требующих оперативной доставки потребителю. До недавнего времени такие применения были преобладающими для данного метода шифрования. Это обусловлено, в частности, относительной простотой проектирования и реализации генераторов хороших шифрующих последовательностей. Но самым важным фактором, конечно, является отсутствие размножения ошибок в поточном шифре. Примером эффективного метода генерирования последовательностей для поточного шифрования является метод, применяемый в стандарте шифрования DES в режиме обратной связи по выходу (режим OFB).

При блочном шифровании открытый текст сначала разбивается на равные по длине блоки, затем применяется зависящая от ключа функция шифрования для преобразования блока открытого текста длиной m бит в блок шифротекста такой же длины. Достоинством блочного шифрования является то, что каждый бит блока шифротекста зависит от значений всех битов соответствующего блока открытого текста, и никакие два блока открытого текста не могут быть представлены одним и тем же блоком

шифротекста. Алгоритм блочного шифрования может использоваться в различных режимах. Четыре режима шифрования алгоритма DES фактически применимы к любому блочному шифру: режим прямого шифрования или шифрования с использованием электронной книги кодов ECB (Electronic code Book), шифрование со сцеплением блоков шифротекста CBC (Cipher block chaining), шифрование с обратной связью по шифротексту CFB (Cipher feedback) и шифрование с обратной связью по выходу OFB (Output feedback).

Наиболее часто блочные шифры применяются в системах шифрования с обратной связью. Системы шифрования с обратной связью встречаются в различных практических вариантах. Как и при блочном шифровании, сообщения разбивают на ряд блоков, состоящих из m бит. Для преобразования этих блоков в блоки шифротекста, которые также состоят из m бит, используются специальные функции шифрования. Однако, если в блочном шифре такая функция зависит только от ключа, то в блочных шифрах с обратной связью она зависит как от ключа, так и от одного или более предшествующих блоков шифротекста.
Практически важным шифром с обратной связью является шифр со сцеплением блоков шифротекста CBC алгоритма DES. В этом случае m бит предыдущего шифротекста суммируются по модулю 2 со следующими m битами открытого текста, а затем применяется алгоритм блочного шифрования под управлением ключа для получения следующего блока шифротекста. Еще один вариант шифра с обратной связью получается из стандартного режима CFB алгоритма DES, т.е. режима с обратной связью по шифротексту.

Достоинством криптосистем блочного шифрования с обратной связью является возможность применения их для обнаружения манипуляций сообщениями, производимых активными перехватчиками. При этом используется факт размножения ошибок в таких шифрах, а также способность этих систем легко генерировать код аутентификации сообщений. Поэтому системы шифрования с обратной связью используют не только для шифрования сообщений, но и для их аутентификации.

На практике поточные шифры или шифры с обратной связью применяют для шифрования длинных сообщений. Выбор конкретного типа шифра зависит от назначения системы и предъявляемых к ней требований.