Тема 4.2

Симметричные криптосистемы

Часть 4

Шифры с гаммированием

Содержание

1. Шифрование методом гаммирования
2. Потоковые шифры

1. Шифрование методом гаммирования

Шифрование методом гаммирования

Хотя одноразовая система шифрования и оказалась неприменима на практике в силу невозможности практической реализации всех требований, обеспечивающих ее теоретическую стойкость, идея, лежащая в ее основе нашла практическое применение в методе гаммирования.

Гаммирование является также широко применяемым криптографическим преобразованием.

- ✔ На самом деле граница между гаммированием и использованием бесконечных ключей и шифров Вижинера, о которых речь шла выше, весьма условная.

Шифрование методом гаммирования

Гамма шифра – это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифровывания открытых данных и расшифровывания принятых данных.

Псевдослучайная последовательность играет роль ***ключа*** в одноразовой система шифрования.

Строго говоря, она не удовлетворяет

- ни требованию случайности,
  - ✔ т.к. используется детерминированный алгоритм для ее выработки,
- ни требованию бесконечной длины,
  - ✔ т.к. все псевдослучайные последовательности имеют конечный период.

Шифрование методом гаммирования

Но при правильно выбранном алгоритме генерации гаммы шифра можно получить метод шифрования с хорошей практической стойкостью,

- ✔ достаточной для решения реальных задач защиты информации.

Шифрование методом гаммирования

Один и тот же алгоритм генерации гаммы шифра выполняется и на стороне отправителя и на стороне получателя информации,

- ✔ оба имеют одинаковую псевдослучайную последовательность, используемую для шифрования и дешифрования.

При этом фактический (подлежащий передаче) объем ***ключевой информации*** очень мал и состоит из нескольких чисел, задающих значения

- ✔ параметров алгоритма
- ✔ и нулевого элемента последовательности.

Шифрование методом гаммирования

Процесс шифрования этим методом называют ***гаммированием***.

Он заключается

- в генерации гаммы шифра
- и её наложении на исходный открытый текст по определенному закону обратимым образом,
  - ✔ например с использованием операции сложения по модулю два.
- Шифрование ведется
  - ✔ либо посимвольно,
  - ✔ либо путем шифрования данных, объединенных в блоки.

Шифрование методом гаммирования

Различают гаммирование

- с конечной
- и бесконечной гаммами.

В первом случае источником гаммы является аппаратный или программный генератор псевдослучайной последовательности.

- Примером бесконечной гаммы может служить последовательность цифр в десятичной записи числа

$$\pi = 3{,}1415926...$$

Шифрование методом гаммирования

В том случае, если множеством используемых для шифрования знаков является алфавит, отличный от бинарного ($Z_2 = \{0,1\}$),

- ✔ например алфавит Z_{33} – русские буквы и пробел, его символы и символы гаммы заменяются цифровыми эквивалентами, которые затем суммируются по модулю 2.

Шифрование методом гаммирования

Процесс зашифровывания заключается в генерации гаммы шифра и наложении полученной гаммы на исходный открытый текст обратимым образом,

- ✔ например, с использованием операции $\oplus$ – сложения по модулю 2.

- Перед зашифровыванием открытые данные разбивают на блоки $T_0^{(i)}$ одинаковой длины,
  - ✔ обычно по 64 бита.
- Гамма шифра вырабатывается в виде последовательности блоков $Г_ш^{(i)}$ аналогичной длины.
- ***Уравнение шифрования*** можно записать в виде

$$T_ш^{(i)} = Г_ш^{(i)} \oplus T_0^{(i)},\ i = 1 \ldots M,$$

  - ✔ где $T_ш^{(i)}$ – i-й блок шифротекста;
  - ✔ $Г_ш^{(i)}$ – i-й блок гаммы шифра;
  - ✔ $T_0^{(i)}$ – i-й блок открытого текста;
  - ✔ M – количество блоков открытого текста.

Шифрование методом гаммирования

Процесс расшифровывания сводится к повторной генерации гаммы шифра и наложению этой гаммы на принятые данные.

- ***Уравнение расшифровывания*** имеет вид

$$T_0^{(i)} = \Gamma_ш^{(i)} \oplus T_ш^{(i)}.$$

Приведенные выше формулы применяются и для посимвольного гаммирования.

✔ В этом случае длина блок принимается равной одному символу.

Шифрование методом гаммирования

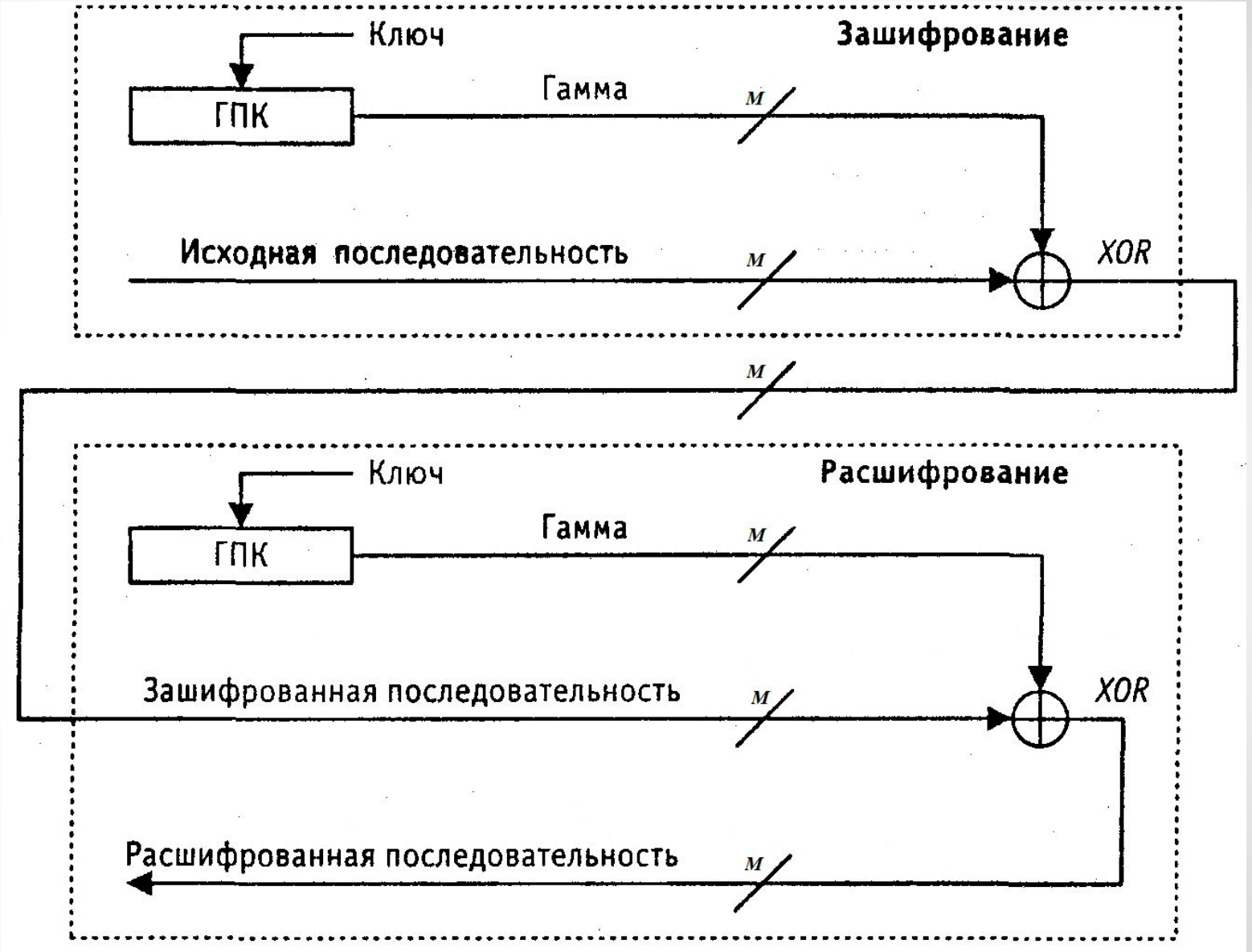


Рисунок – Шифрование информации методом гаммирования

Шифрование методом гаммирования

Получаемый этим методом шифротекст достаточно труден для раскрытия, поскольку теперь ключ является переменным.

- Гамма шифра не должна содержать повторяющихся последовательностей.
- По сути дела гамма шифра должна изменяться случайным непредсказуемым образом для каждого шифруемого блока.
- Если период гаммы превышает длину всего шифруемого текста и злоумышленнику неизвестна никакая часть исходного текста,
  - ✔ то такой шифр можно раскрыть только прямым перебором всех вариантов ключа.
- В этом случае криптостойкость шифра определяется длиной ключа.

Шифрование методом гаммирования

Чтобы получить линейные последовательности элементов гаммы, длина которых превышает размер шифруемых данных, используются генераторы псевдослучайных последовательностей.

Шифрование методом гаммирования

Слабое место метода гаммирования в том, что он становится бессильным, если злоумышленнику становится известен

- ✔ фрагмент исходного текста длиной более чем период гаммы,
- ✔ и соответствующая ему шифрограмма.

- Простым вычитанием по модулю 2
  - ✔ получается ключ
  - ✔ и по нему восстанавливается вся последовательность.

Шифрование методом гаммирования

Криптоаналитик также может частично или полностью восстановить ключ на основе догадок о содержании исходного текста.

- Так, если большинство посылаемых сообщений начинается со слов "СОВ. СЕКРЕТНО",
  - ✔ то криптоанализ всего текста значительно облегчается.
- Также многие текстовые редакторы, например Word, вставляют в начало файла стандартную служебную информацию,
  - ✔ что понижает криптостойкость при шифровании этих файлов методом гаммирования.

2. Потоковые шифры

Понятие ключевого потока

Обратим внимание на одно из **различий между шифром простой замены и гаммирования**:

- в шифре простой замены один и тоже элемент открытого текста перейдет в фиксированный знак шифртекста в любом такте шифрования,
- а в шифре гаммирования это не так:
  - ✔ этот шифр преобразует элемент открытого текста в зависимости от значения гаммы (т.е. ключа) на каждом такте шифрования.
- Можно сказать, что упомянутый ключ задает последовательность шифрпреобразований,
  - ✔ в отличие от шифра простой замены, где все шифрпреобразования одинаковы.

Основные типы шифров

Указанное различие приводит к понятиям основных типов шифров:

- блочных
- и потоковых шифров

соответственно.

Последовательность выбора шифрпреобразований

Рассмотрим пронумерованный список Δ всех различных шифрпреобразований, которые могли бы возникнуть в процессе шифрования сообщений с помощью данной криптосистемы.

- Процесс зашифрования можно записать как последовательность номеров шифрпреобразований, выбранных на соответствующих тактах.
- Обозначим эту последовательность через Г и назовем ключевым потоком.

Свойства этой последовательности во многом отражают качество шифра и определяют его классификацию.

- Например, если список Δ содержит только шифрпреобразования, являющиеся сложением по модулю 2, каждое с фиксированным числом c_i, то шифр является шифром гаммирования по модулю 2.

Потоковый шифр

Потоковым шифром называется система, в которой на каждом такте используется переменный, выбираемый с помощью элементов ключевого потока, алгоритм шифрования.

Ключевой поток определяется

- исходными ключевыми данными
- и, в общем случае, номерами тактов шифрования, вплоть до рассматриваемого.

Потоковый шифр

Потоковые шифры, очевидно, более чувствительны к нарушениям синхронизации (вставка, пропуск), чем блочные.

- Для некоторой компенсации данного недостатка используются потоковые шифры с обратной связью.
  - ✔ В этих шифрах значение элемента ключевого потока на такте *t* вычисляется с помощью фиксированной функции *f* от ключа и нескольких знаков шифртекста, полученных на *m* предыдущих тактах.

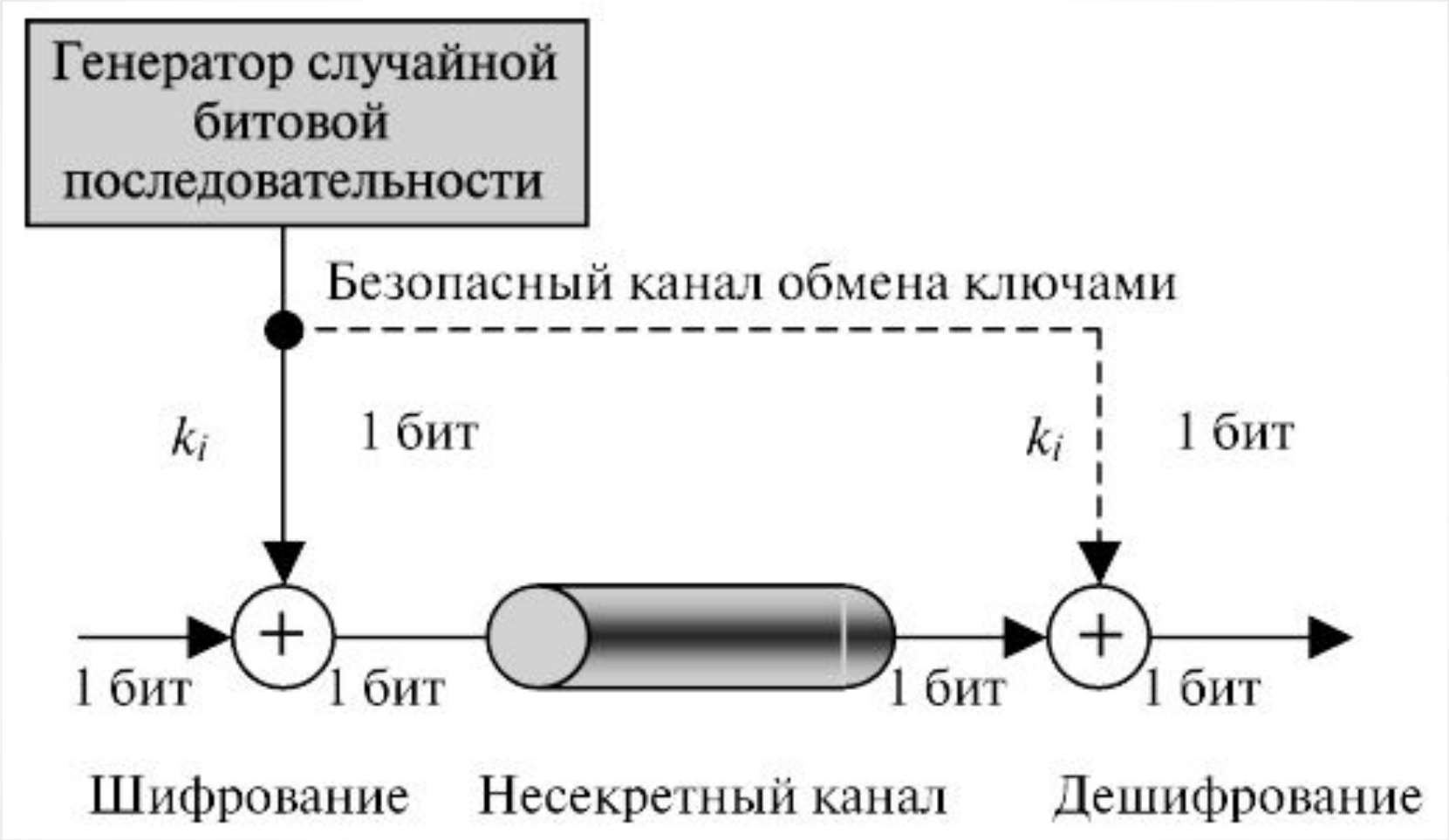
Потоковый шифр

В криптографической литературе под ***потоковым шифром*** очень часто понимают так называемый двоичный аддитивный потоковый шифр, представляющий собой шифр гаммирования по модулю два с псевдослучайной гаммой.

- Для такого шифра ключевой поток можно записать с помощью нулей и единиц и непосредственно использовать для гаммирования открытого текста.

Потоковый шифр

Рисунок – Принцип работы поточного шифра



Потоковый шифр

К **достоинствам** поточных шифров относятся высокая скорость шифрования, относительная простота реализации и отсутствие размножения ошибок.

Недостатком является необходимость передачи информации синхронизации перед заголовком сообщения, которая должна быть принята до расшифрования любого сообщения.

- ✔ Это обусловлено тем, что если два различных сообщения шифруются на одном и том же ключе, то для расшифрования этих сообщений требуется одна и та же псевдослучайная последовательность.

Потоковый шифр

Такое положение может создать угрозу криптостойкости системы.

- Поэтому часто используют дополнительный, случайно выбираемый ключ сообщения, который
  - ✔ передается в начале сообщения
  - ✔ и применяется для модификации ключа шифрования.
- В результате разные сообщения будут шифроваться с помощью различных последовательностей.

Потоковый шифр

Поточные шифры широко применяются для шифрования преобразованных в цифровую форму речевых сигналов и цифровых данных, требующих оперативной доставки потребителю информации.

- ✔ 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.