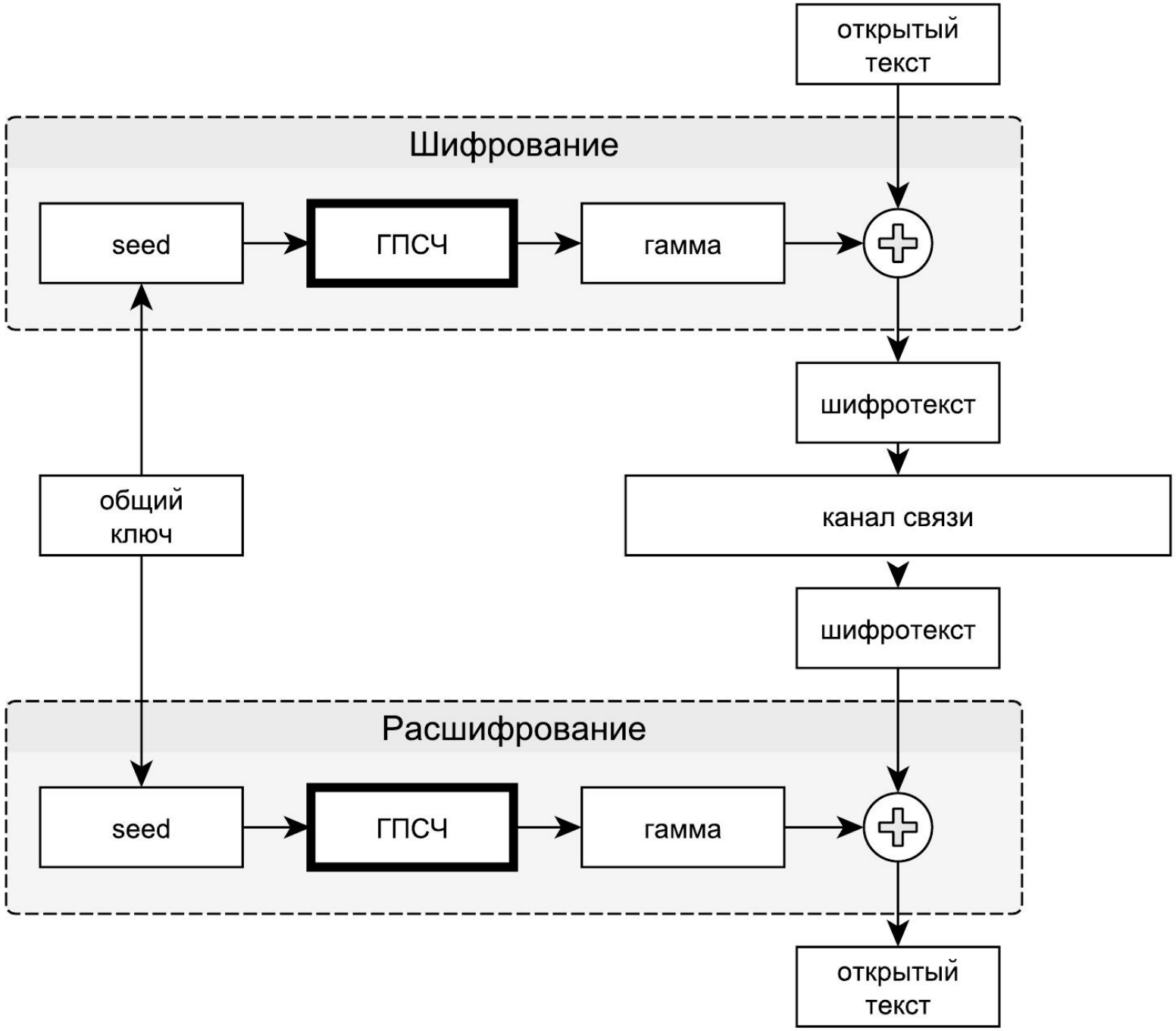
ПОТОКОВЫЕ ШИФРЫ

Описание

- Потоковые шифры осуществляют посимвольное шифрование открытого текста. Под символом алфавита открытого текста могут пониматься как отдельные биты (побитовое шифрование), так и байты (побайтовое шифрование). Поэтому можно говорить о в какой-то мере условном разделении блочных и потоковых шифров: например, 64-битная буква – один блок.

Описание


открытый текст
Шифрование
seed
ГПСЧ
гамма
шифротекст
общий ключ
канал связи
шифротекст
Расшифрование
seed
ГПСЧ
гамма
открытый текст

Описание

- Перед началом процедуры шифрования отправитель и получатель должны обладать общим секретным ключом.
- Секретный ключ используется для генерации инициализирующей последовательности генератора псевдослучайной последовательности.
- Генераторы отправителя и получателя используются для получения одинаковой псевдослучайной последовательности символов, называемой гаммой. Последовательности одинаковые, если для их получения использовались одинаковые ГПСЧ, инициализированные одной и той же инициализирующей последовательностью, при условии, что генераторы детерминированные.

Описание

- Символы открытого текста на стороне отправителя складываются с символами гаммы, используя простейшие обратимые преобразования. Например, побитовое сложение по модулю 2 (операция “исключающее или”, XOR). Полученный шифротекст передаётся по каналу связи.
- На стороне легального получателя с символами шифротекста и гаммы выполняется обратная операция (для XOR это будет просто повторный XOR) для получения открытого текста.

Шифр RC4

- Шифр RC4 был разработан Роном Ривестом (англ. Ronald Linn Rivest) в 1987 году для компании RSA Data Security. Описание алгоритма было впервые анонимно опубликовано в телеконференции Usenet sci.crypt в 1994 году.
- Генератор, используемый в шифре, хранит своё состояние в массиве из 256 ячеек S_0, S_1, …, S_{255}, заполненных значениями от 0 до 255 (каждое значение встречается только один раз), а также двух других переменных размером в 1 байт i и j. Таким образом, количество различных внутренних состояний генератора равно $255! \times 255 \times 255$.

Процедура инициализации ГПСЧ RC4

- Для заполнения байтового массива из 256 ячеек K_0, K_1, …, K_{255} используется предоставленный ключ. При необходимости (если размер ключа менее 256 байтов) ключ используется несколько раз, пока массив K не будет заполнен целиком
- Начальное значение j равно 0.
- Далее для значений i от 0 до 255 выполняется:
  - $j := (j + S_i + K_i) \bmod 256$,
  - поменять местами S_i и S_j

Процедура получения следующего псевдослучайного байта $result$ (следующего байта гаммы):

- Начальные значения i и j равны 0
- $i := (i + 1) \bmod 256$,
- $j := (j + S_i) \bmod 256$,
- поменять местами S_i и S_j,
- $t := (S_i + S_j) \bmod 256$,
- $result := S_t$

Генерируется столько значений result, сколько байт в передаваемом сообщении