Шифрование методом гаммирования

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Например, в поле Галуа GF(2) суммирование принимает вид операции «исключающее ИЛИ (XOR)».

Визуальное представление

|  |  |
| --- | --- |
| Схема передатчика | Схема приёмника |

Стойкость.

Доказательство абсолютной стойкости Шеннона.

Клод Шеннон доказал, что при определённых свойствах гаммы этот метод шифрования является абсолютно стойким (то есть не поддающимся взлому).

Пусть X, Y, Z — дискретные случайные величины.

Пусть:

* X — значение бита открытого текста; то есть, переменная X (бит) способна принимать два значения: 0 и 1;
* p — вероятность события, заключающегося в том, что переменная X примет значение 0;
* (1-p) — вероятность противоположного события (то есть, вероятность того, что переменная X примет значение 1).

Запишем закон распределения значений X^

|  |  |  |
| --- | --- | --- |
| X | 0 | 1 |
| Pi | p | (1 – p) |

Используем p и (1-p), так как вероятность встретить одну букву в разных словах различна.

Пусть:

* Y — бит псевдослучайной последовательности (гаммы); то есть, переменная Y (бит) способна принимать два значения: 0 и 1;
* каждое из значений Y равновероятно; то есть, вероятности получить 0 или 1 равны 1/2.

Запишем закон распределения значений Y

|  |  |  |
| --- | --- | --- |
| Y | 0 | 1 |
| Pi | 1/2 | 1/2 |

Иными словами, в качестве гаммы (Y) подаётся одинаковое количество нулей и единиц, или значения переменной Y имеют симметричный закон распределения.

Пусть:

* Z — бит закрытого текста; то есть, переменная Z (бит) способна принимать два значения: 0 и 1;
* значение Z вычисляется на основе значений X и Y по формуле:

Z=X+Y (mod 2)

или

Z = xor(X, Y)

или

Z = X [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) Y

Найдём следующие вероятности:

* P(Z=0) — вероятность события, заключающегося в том, что переменная Z принимает значение 0;
* P(Z=1) — вероятность события, заключающегося в том, что переменная Z принимает значение 1.

Используем формулы:

* сложения вероятностей несовместных событий:

P(A+B)=P(A)+P(B);

* умножения вероятностей независимых событий:

P(A\*B)=P(A)\*P(B).

Вероятность того, что переменная Z примет значение 0:

P(Z=0)=P(X=0,Y=0)+P(X=1,Y=1)=P(X=0)\*P(Y=0)+P(X=1)\*P(Y=1)=p\*1/2+(1-p)\*1/2=1/2.

Вероятность того, что переменная Z примет значение 1:

P(Z=1)=1-P(Z=0)=1/2.

Так как P(Z=0) и P(Z=1) не зависят от p, p может принимать любое значение.

Запишем закон распределения значений переменной Z:

|  |  |  |
| --- | --- | --- |
| Y | 0 | 1 |
| Pi | 1/2 | 1/2 |

Закон распределения Z оказался симметричным, как и закон распределения гамма (Y) или шум. То есть, Z не содержит никакую информацию из X (в Z нет p). Это доказывает, что шифр является абсолютно стойким.

Требования к гамме.

* Для шифрования каждого нового сообщения нужно использовать новую гамму. Повторное использование гаммы недопустимо ввиду свойств операции «xor». Рассмотрим пример: с помощью одинаковой гаммы Y зашифрованы два открытых текста X₁ и X₂, получено две шифрограммы Z₁ и Z₂:

Z1 =X1 [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) Y}

Z2 =X2 [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) Y}

Выполним сложение двух шифрограмм, используя операцию «[xor](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2" \o "Сложение по модулю 2)»:

{\displaystyle Z1 [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) Z2 =(X1 [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) Y) [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) (X2 [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) Y)=X1 [⊕](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_2) X2}

Результат зависит от открытых текстов X₁ и X₂ и не зависит от гаммы Y. Ввиду избыточности естественных языков результат поддаётся частотному анализу, то есть открытые тексты можно подобрать, не зная гамму Y.

* Для формирования гаммы (последовательности псевдослучайных чисел) нужно использовать аппаратные генераторы случайных чисел, основанные на физических процессах. Если гамма не будет случайной, для получения открытого текста потребуется подобрать только начальное состояние генератора псевдослучайных чисел.
* Длина гаммы должна быть не меньше длины защищаемого сообщения (открытого текста). В противном случае для получения открытого текста потребуется подобрать длину гаммы, проанализировать блоки шифротекста угаданной длины, подобрать биты гаммы.