

12. Шифрование методом гаммирования. Потокосые шифры

В аддитивных шифрах используется сложение по модулю (mod) исходного сообщения с гаммой, представленных в числовом виде. Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, $5+10 \bmod 4 = 15 \bmod 4 = 3$).

В литературе шифры этого класса часто называют потоковыми, хотя к потоковым относятся и другие разновидности шифров. Стойкость закрытия этими шифрами определяется, главным образом, качеством гаммы, которое зависит от длины периода и случайности распределения по периоду. При этом символы в пределах периода гаммы являются ключом шифра.

Длиною периода гаммы называется минимальное количество символов, после которого последовательность цифр в гамме начинает повторяться. Случайность распределения символов по периоду означает отсутствие закономерностей между появлением различных символов в пределах периода.

По длине периода различаются гаммы с конечным и бесконечным периодом. Если длина периода гаммы превышает длину шифруемого текста, гамма является истинно случайной и не используется для шифрования других сообщений, то такое преобразование является абсолютно стойким (совершенный шифр).

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы

$$C_i = (P_i + K_i) \bmod N, \quad (6.1)$$

$$P_i = (C_i + N - K_i) \bmod N, \quad (6.2)$$

где P_i , C_i - i -ый символ открытого и зашифрованного сообщения;

N - количество символов в алфавите;

K_i - i -ый символ гаммы (ключа). Если длина гаммы меньше, чем длина сообщения, то она используется повторно.

Данные формулы позволяют выполнить зашифрование / расшифрование по Вижнеру при замене букв алфавита числами согласно следующей таблице (применительно к русскому алфавиту):

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Рис.6.1. Таблица кодирования символов

Например, для шифрования используется русский алфавит ($N = 33$), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква А будет представлена как 0, Б – 1, ..., Я – 32. Результат шифрования показан в следующей таблице.

Таблица 6.1. Пример аддитивного шифрования по модулю $N = 33$

С и м в о л	открытого сообщения, P_i	А	Б	Р	А	М	О	В
		0	1	17	0	13	15	2
	гаммы, K_i	Ж	У	Р	И	Х	И	Н
		7	20	17	9	22	9	14
	шифrogramмы, C_i	Ж	Ф	Б	И	В	Ч	П
		7	21	1	9	2	24	16

Сложение по модулю 2. Значительный успех в криптографии связан с именем американца Гильберто Вернама. В 1917 г. он, будучи сотрудником телеграфной компании AT&T, совместно с Мейджором Джозефом Моборном предложил идею автоматического шифрования телеграфных сообщений. Речь шла о своеобразном наложении гаммы на знаки алфавита, представленные в соответствии с телетайпным кодом Бодо пятизначными «импульсными комбинациями». Например, буква А представлялась комбинацией («- - - +

+»), а комбинация («+ + – + +») представляла символ перехода от букв к цифрам. На бумажной ленте, используемой при работе телетайпа, знаку «+» отвечало наличие отверстия, а знаку «–» - его отсутствие. При считывании с ленты металлические щупы проходили через отверстия, замыкали электрическую цепь и, тем самым, посылали в линию импульс тока.

Вернам предложил электромеханически покоординатно складывать «импульсы» знаков открытого текста с «импульсами» гаммы, предварительно нанесенными на ленту. Сложение проводилось «по модулю 2». Имеется в виду, что если «+» отождествить с 1, а «–» с 0, то сложение определяется двоичной арифметикой:

\oplus	0	1
0	0	1
1	1	0

Таким образом, при данном способе шифрования символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по модулю 2 (\oplus , для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»). Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C_i = P_i \oplus K_i, (6.3)$$

$$P_i = C_i \oplus K_i. (6.4)$$

Вернам сконструировал и устройство для такого сложения. Замечательно то, что процесс шифрования оказывался полностью автоматизированным, в предложенной схеме исключался шифровальщик. Кроме того, оказывались слитыми воедино процессы зашифрования / расшифрования и передачи по каналу связи.

В 1918 г. два комплекта соответствующей аппаратуры были изготовлены и испытаны. Испытания дали положительные результаты. Единственное неудовлетворение специалистов - криптографов было связано с гаммой. Дело в том, что первоначально гамма была нанесена на ленту, склеенную в кольцо. Несмотря на то, что знаки гаммы на ленте выбирались случайно, при зашифровании длинных сообщений гамма регулярно повторялась. Этот недостаток так же отчетливо осознавался, как и для шифра Виженера. Уже тогда хорошо понимали, что повторное использование гаммы недопустимо даже в пределах одного сообщения.

Попытки удлинить гамму приводили к неудобствам в работе с длинным кольцом. Тогда был предложен вариант с двумя лентами, одна из которых шифровала другую, в результате чего получалась гамма, имеющая длину периода, равную произведению длин исходных периодов.

Шифры гаммирования стали использоваться немцами в своих дипломатических представительствах в начале 20-х гг., англичанами и американцами – во время Второй мировой войны. Разведчики-нелегалы ряда государств использовали шифроблокноты¹. Шифр Вернама (сложение по модулю 2) применялся на правительственной «горячей линии» между Вашингтоном и Москвой, где ключевые материалы представляли собой перфорированные бумажные ленты, производившиеся в двух экземплярах.

Перед иллюстрацией использования шифра приведем таблицу кодов символов Windows 1251 и их двоичное представление.

Таблица 6.2. Коды символов Windows 1251 и их двоичное представление

Буква	Дес-код	Bin-код	Буква	Дес-код	Bin-код	Буква	Дес-код	Bin-код
А	192	1100 0000	Л	203	1100 1011	Ц	214	1101 0110
Б	193	1100 0001	М	204	1100 1100	Ч	215	1101 0111
В	194	1100 0010	Н	205	1100 1101	Ш	216	1101 1000
Г	195	1100 0011	О	206	1100 1110	Щ	217	1101 1001
Д	196	1100 0100	П	207	1100 1111	Ъ	218	1101 1010
Е	197	1100 0101	Р	208	1101 0000	Ы	219	1101 1011

Ж	198	1100 0110	С	209	1101 0001	Ь	220	1101 1100
З	199	1100 0111	Т	210	1101 0010	Э	221	1101 1101
И	200	1100 1000	У	211	1101 0011	Ю	222	1101 1110
Й	201	1100 1001	Ф	212	1101 0100	Я	223	1101 1111
К	202	1100 1010	Х	213	1101 0101			

Примечание. Дес-код – десятичный код символа, Bin-код – двоичный код символа.

Пример шифрования сообщения «ВОВА» с помощью гаммы «ЮЛЯ» показан в следующей таблице.

Таблица 6.3. Пример аддитивного шифрования по модулю 2

Открытое сообщение, P_i	Буква	В	О	В	А
	Дес-код	194	206	194	192
	Bin-код	1100 0010	1100 1110	1100 0010	1100 0000
Гамма, K_i	Буква	Ю	Л	Я	Ю
	Дес-код	222	203	223	222
	Bin-код	1101 1110	1100 1011	1101 1111	1101 1110
Шифрограмма, C_i	Дес-код	28	5	29	30
	Bin-код	0001 1100	0000 0101	0001 1101	0001 1110

Шифрование по модулю 2 обладает замечательным свойством, вместо истинной гаммы противнику можно сообщить ложную гамму, которая при наложении на шифрограмму даст осмысленное выражение.

Таблица 6.4. Пример использования ложной гаммы

Шифрограмма, C_i	Дес-код	28	5	29	30
	Bin-код	0001 1100	0000 0101	0001 1101	0001 1110
Ложная гамма, K'_i	Буква	Ю	Е	М	Б
	Дес-код	222	197	204	193
	Bin-код	1101 1110	1100 0101	1100 1100	1100 0001
Ложное открытое сообщение, P'_i	Дес-код	194	192	209	223
	Bin-код	1100 0010	1100 0000	1101 0001	1101 1111
	Буква	В	А	С	Я

В 2013 г. ученые Корнельского университета предложили использовать для генерации ключей (шифроблокнотов) куски полупрозрачного стекла [42]. Кратко принцип нового метода шифрования заключается в том, что отправитель и получатель (Алиса и Боб) во время встречи формируют общий ключ, облучая кусочки стекла изображением-паттерном с IDi (внешне он напоминает QR-код).

В результате отражения и преломления, характер которого индивидуален для каждого куска стекла, у Алисы и Боба получаются собственные случайные изображения, которые затем оцифровываются (получаются ключи $keyA_i$ и $keyB_i$). Из этих изображений и составляется общий ключ ($keyAB_i = keyA_i \oplus keyB_i$).

Потоковые шифры

Потоковый шифр - симметричный тип шифра, где каждый элемент открытого текста переводится в зашифрованный вид, в зависимости от применяемого ключа и его позиции в текстовом потоке. Особенность поточного шифра - иной подход к процессу шифрования в сравнении с блочным типом шифра.

Потоковый шифр - вид шифра, в котором каждый бит данных зашифровывается посредством гаммирования. Процесс гаммирования подразумевает наложение на

информацию гамм кода по строго определенным правилам. Чтобы расшифровать данные, требуется наложение той же гаммы на зашифрованный текст.

Первые потоковые шифры были использованы еще во времена Второй мировой войны (до появления электроники). Более чем через два десятка лет (в 1965 году) норвежский криптограф Эранст Селмер разработал свою теорию последовательности регистровых сдвигов. Еще через время Соломон Голомб написал книгу о последовательности сдвиговых регистров. При этом популярность потоковым шифрам пришла раньше - в 1949 году, когда миру была представлена работа Клода Шеннона о стойкости шифра Вернама.

Принцип потокового шифрования

Генератор случайных чисел выдает определенную гамму (числовую последовательность). Последняя накладывается на шифруемую информацию с применением операции XOR. На выходе получаются зашифрованные данные. Наиболее популярный потоковый шифр - RC4, признанный органами стандартизации. Надежность потокового шифрования зависит от числовой последовательности, выдаваемой генератором.

Сфера применения потоковых шифров - военные, сетевые, телефонные и другие системы, где необходимо преобразование речевой информации в цифровую форму и надежное шифрование данных. Причина популярности - простота реализации и конструирования генераторов, надежность шифрования, отсутствие ошибок в потоковом шифре.

В проектировании поточных шифров применяется один из следующих подходов:

- **системно-теоретический** - основан на создании проблемы, которая еще не известна и не исследована криптоаналитиком;
- **информационно-технический** - базируется на попытке спрятать разгадку от криптоаналитика;
- **сложно-теоретический** - подход, базирующийся на известной, хоть и сложной проблеме;
- **рандомизированный** - подход, где создается объемная задача, решение которой выглядит невозможным.