УДК 378.6:519.83

Студ. М. Е. Алексеев
Науч. рук. доц. И. К. Асмыкович
(кафедра высшей математики, БГТУ)

ШИФРОВАНИЕ МЕТОДОМ ГАММИРОВАНИЯ

Цель данной работы: рассмотреть алгоритм шифрования методом гаммирования по модулю 2 и его преимущества по сравнению с другими алгоритмами.

Гаммирование – метод последовательного симметричного шифрования, суть которого состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется *гаммой*. Такой метод чаще всего представляют как наложение гаммы на исходный текст, поэтому он получил название "*гаммирование*".

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые складываются по модулю k:

$$R_i = (S_i + G_i) \bmod(k),$$

где k – число символов в алфавите, а R_i, S_i и G_i – символы, соответственно, зашифрованного, исходного текста и гаммы.

При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2:

$$R_i = (S_i + G_i) \bmod(2) = S_i \oplus G_i .$$

Можно дополнительно использовать и другие логические операции. Это будет равносильно введению еще одного ключа, которым является выбор правила формирования зашифрованного сообщения из символов исходного текста и гаммы.

Процесс дешифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Операция сложения по модулю 2 в алгебре логики называется также "исключающее ИЛИ". Данная операция работает следующим образом (рис.1): при сложении двух двоичных знаков получается 0, если исходные двоичные цифры одинаковы, и 1, если цифры разные.

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Рисунок 1 – Операция сложения по модулю 2

Таким образом, при гаммировании по модулю 2 нужно использовать одну и ту же операцию как для шифрования, так и для расшифровки. Это позволяет использовать один и тот же алгоритм, а соответственно и одну и ту же программу при программной реализации, как для шифрования, так и для расшифровки.

Операция сложения по модулю 2 очень быстро выполняется на вычислительных устройствах (в отличие от многих других арифметических операций), поэтому наложение гаммы даже на очень большой открытый текст выполняется практически мгновенно.

Благодаря указанным достоинствам метод гаммирования широко применяется в современных технических системах сам по себе, а также как элемент комбинированных алгоритмов шифрования.

Гаммирование по модулю 2 в общем случае производится следующим образом:

- символы исходного текста и гамма представляются в двоичном коде исходя из выбранной кодировки и располагаются один под другим, при этом ключ (гамма) записывается столько раз, сколько необходимо;
- каждая пара двоичных знаков складывается по модулю два;
- полученная последовательность двоичных знаков кодируется символами алфавита в соответствии с выбранной ранее кодировкой.

Разберём пример шифрования слова. Символы слова будем представлять в соответствии с кодировкой Windows-1251. Ниже представлена таблица 1, которая показывает как записываются прописные буквы кириллицы в соответствии с кодировкой.

Таблица 1 – Кодировки прописных букв

Буква	Bin-код	Буква	Bin-код	Буква	Bin-код
А	1100 0000	Л	1100 1011	Ц	1101 0110
Б	1100 0001	М	1100 1100	Ч	1101 0111
В	1100 0010	Н	1100 1101	Ш	1101 1000
Г	1100 0011	О	1100 1110	Щ	1101 1001
Д	1100 0100	П	1100 1111	Ъ	1101 1010
Е	1100 0101	Р	1101 0000	Ы	1101 1011
Ж	1100 0110	С	1101 0001	Ь	1101 1100
З	1100 0111	Т	1101 0010	Э	1101 1101
И	1100 1000	У	1101 0011	Ю	1101 1110
Й	1100 1001	Ф	1101 0100	Я	1101 1111
К	1100 1010	Х	1101 0101		

Исходный текст: КОНФЕРЕНЦИЯ

Гамма (ключ): СИРЕНЬ

Исходный текст в шестнадцатеричном виде:

CA CE CD D4 C5 D0 C5 CD D6 C8 DF

Гамма в шестнадцатеричном виде: D1 C8 D0 C5 CD DC

Если гамма короче, чем сообщение, предназначенное для шифрования, гамма повторяется требуемое число раз. Так в примере длина исходного сообщения равна 11-и байтам, а длина ключа – 6-и байтам. Следовательно, для шифрования гамма должна быть повторена 1 раз полностью и еще один раз частично.

Исх.биты	1100	1010	1100	1110	1100	1101	1101	0100	1100	0101	1101	0000
Гамма	1101	0001	1100	1000	1101	0000	1100	0101	1100	1101	1101	1100
Результат	0001	1011	0000	0110	0001	1101	0001	0001	0000	1000	0000	1100

Исх. биты	1100	0101	1100	1101	1101	0110	1100	1000	1101	1111
Гамма	1101	0001	1100	1000	1101	0000	1100	0101	1100	1101
Результат	0001	0100	0000	0101	0000	0110	0000	1101	0001	0010

Закодированный текст в шестнадцатеричном виде:

1B 06 1D 11 08 0C 16 05 06 0D 12

Исх. биты	0001	1011	0000	0110	0001	1101	0001	0001	0000	1000	0000	1100
Гамма	1101	0001	1100	1000	1101	0000	1100	0101	1100	1101	1101	1100
Результат	1100	1010	1100	1110	1100	1101	1101	0100	1100	0101	1101	0000

Исх. биты	0001	0100	0000	0101	0000	0110	0000	1101	0001	0010
Гамма	1101	0001	1100	1000	1101	0000	1100	0101	1100	1101
Результат	1100	0101	1100	1101	1101	0110	1100	1000	1101	1111

Расшифрованный текст в шестнадцатеричном виде:

CA CE CD D4 C5 D0 C5 CD D6 C8 DF

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы – длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода. Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей.

Обычно разделяют две разновидности гаммирования – с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом, если длина периода гаммы превышает длину шиф-

руемого текста, то такой шифр теоретически является абсолютно стойким, т.е. его нельзя вскрыть при помощи статистической обработки зашифрованного текста, а можно раскрыть только прямым перебором (brootforce). Криптостойкость в этом случае определяется размером ключа. Это, однако, не означает, что дешифрование такого текста вообще невозможно: при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

Кроме того, для использования ключа вначале необходимо каким-либо надежным способом доставить его обеим сторонам, обменивающимся сообщениями. Это приводит к возникновению проблемы распределения ключей, сложность решения которой возрастает с увеличением длины ключа и количества абонентов в сети передачи сообщений.

В качестве гаммы может быть использована любая последовательность случайных символов, например, последовательность цифр числа π, числа e и т.п. При шифровании с помощью ЭВМ последовательность гаммы формируется с помощью ***генератора псевдослучайных чисел*** (ГПСЧ). В настоящее время разработано несколько алгоритмов работы таких генераторов, которые обеспечивают удовлетворительные характеристики гаммы.

ЛИТЕРАТУРА

1. Методы гаммирования [Электронный ресурс] – Режим доступа: https://www.intuit.ru/studies/courses/691/547/lecture/12373?page=4. – Дата обращения: 05.04.2019.

2. Шифрование методом гаммирования [Электронный ресурс] – Режим доступа: https://studfiles.net/preview/5470123/page:9/ – Дата обращения: 08.04.2019.

УДК 519.176

Студ. Р. Ю. Злобин
Науч. рук. доц. И. К. Асмыкович
(кафедра высшей математики, БГТУ)

НЕКОТОРЫЕ ПРИМЕНЕНИЯ ТЕОРИИ ГРАФОВ

Графы и теория графов представляют собой один из наиболее важных и интересных, но в тоже время один из сложных разделов в математике и информатике.

Многие структуры, представляющие практический интерес в логике, информатике, математике и других науках, могут быть представлены графами.