УДК 378.6:519.83

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

ПРИМЕНЕНИЕ МОДУЛЯРНОЙ АРИФМЕТИКИ В КРИПТОГРАФИИ

Криптография — это искусство написания и вскрытия шифров. А шифр, в свою очередь, — это какая-либо система преобразований текста с использованием определённого секрета, который называют ключём шифрования.

Одним из наиболее изученных шифров в криптографии является Шифр Цезаря. Он появился в I в. до н. э. Шифр Цезаря заменяет каждую букву другой, находящейся в алфавите на некоторое определенное число позиций правее.

Работа шифра Цезаря может быть показана теорией, которая привычна для математики и в ещё большей степени для криптографии — модульной арифметикой. Эта теория появилась еще в работах греческого математика Евклида (325–265 гг. до н. э.) и является одной из основ современной информационной безопасности.

Рассмотрим принцип сравнения по модулю. Возьмём в качестве примера обычные часы со стрелками и сравниим их с цифровыми часами. На часах со стрелками циферблат разделен на 12 частей, которые мы обозначим числами 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, и 11. Когда мы говорим, например, что сейчас 15:00, мы также можем сказать, что сейчас три часа дня. Поделив 15 на 12 можно заметить, что остаток от деления будет равен 3. В математике это обозначается так $15 \equiv 3 \pmod{12}$, а говорится следующим образом:«15 сравнимо с 3 по модулю 12».

Мы также можем представить себе часы с отрицательными числами. Который будет час, если стрелка показывает на -9? Или, другими словами, с каким числом сравнимо число -9 по модулю 12? Давайте посчитаем, учитывая, что на наших часах с циферблатом, разделенным на 12 частей, значение 0 соответствует 12.

$$-9 = -9 + 0 = -9 + 12 = 3.$$

Математика для расчетов на наших часах со стрелками, циферблат которых разделен на 12 частей, называется арифметикой по модулю 12.

В общем случае говорят, что $a \equiv b \pmod{m}$, если остаток от деления a на m равен b, при условии что a, b и m являются целыми числами.

Шифр Цезаря является частным случаем так называемого аффинного шифра. Он определяется следующим образом

$$Z(x) = (a\times x+b) \ (\mathrm{mod} n),$$

где x — начальная позиция буквы, $Z(x)$ — позиция зашифрованной буквы, a и b — два целых числа, меньших, чем число (n) букв в алфавите. Наибольший общий делитель чисел a и n должен быть равен 1 [НОД (a,n) = 1], потому что иначе, получится несколько возможных вариантов для шифрования одной и той же буквы. Ключ шифра определяется парой (a,b).

В качестве примера возьмём слово HELLO и зашифруем его. Ключ выберем следующий: a = 7, b = 16. Таким образом, наша функция для шифрования записывается как

$$Z(x) = (7\times x+ 16) \ (\mathrm{mod}\ 26).$$

Запишем в таблице английский алфавит, добавив титульный ряд из 26 чисел.

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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Буква H стоит на позиции 7, $Z(7) = 7 \bullet 7 + 16 = 65 \equiv 13 \ (\mathrm{mod}\ 26)$, числу 13 соответствует буква N.

Буква E стоит на позиции 4, $Z(4) = 7 \bullet 4 + 16 = 44 \equiv 18 \ (\mathrm{mod}\ 26)$, числу 18 соответствует буква S.

Буква L стоит на позиции 11, $Z(7) = 7 \bullet 11 + 16 = 93 \equiv 15 \ (\mathrm{mod}\ 26)$, числу 15 соответствует буква P. Вторая буква L аналогично.

Буква O стоит на позиции 14, $Z(14) = 7 \bullet 14 + 16 = 114 \equiv 10 \ (\mathrm{mod}\ 26)$, числу 10 соответствует буква K.

Таким образом, слово HELLO, зашифрованное афинным шифром с ключем a = 7, b = 16, превратится в слово NSPPK.

Аффинный шифр имеет более высокий уровень безопасности, чем обычный шифр Цезаря, потому что ключом аффинного шифра является пара чисел (a, b). Если сообщение написано с использованием алфавита из 26 букв и зашифровано с помощью аффинного шифра, то и a, и b могут принимать любые значения от 0 до 25. Таким образом, в этой системе шифрования с алфавитом из 26 букв возможное количество ключей составит 25×25 = 625.

Это значительное улучшение, но аффинный шифр все еще возможно расшифровать методом перебора всех возможных вариантов.

Математическая операция расшифровки эквивалентна нахождению неизвестного x при данном значении y по модулю n.

$$Z(x) = (ax+b) = y \ (\mathrm{mod}\ n),$$

$$(ax+b) = y \pmod{n},$$

$$ax = y - b \pmod{n}.$$

Другими словами, необходимо найти значение a-1 (обратное значению a), удовлетворяющее равенству a-1a ≡ 1 (mod n), так что

$$a^{-1}ax = a^{-1}(y - b) \pmod{n},$$

$$x = a^{-1}(y - b) \pmod{n}.$$

Следовательно, для успешной расшифровки мы должны найти число, обратное числу a по модулю n, и, чтобы не тратить зря время, мы должны заранее знать, существует ли это обратное число.

В случае аффинного шифра Z(x) = (a×x + b) (mod n), обратное значение числа a будет существовать тогда и только тогда, когда НОД (a, n) = 1.

Предположим, что нами было перехвачено зашифрованное слово: TVYXK. Мы знаем, что оно было зашифровано аффинным шифром вида Z(x) = 7x + 21 с помощью английского алфавита из 26 букв.

Как получить расшифровать сообщение?

Для начала посчитаем НОД (7, 26), который равен 1. Значит, сообщение можно расшифровать. Для этого для функции Z(x) = 7x + 21 мы должны найти обратную функцию по модулю 26:

$$7x + 21 = y \pmod{26},$$

$$7x = (y - 21) \pmod{26}.$$

Чтобы найти x, мы должны умножить обе части уравнения на число, обратное числу 7 по модулю 26, — это целое число a-1 такое, что 7×a-1 ≡ 1 (mod 26), а именно 15

$$7 \times 15 = 105 \equiv 1 \pmod{26}.$$

Итак, мы имеем x = 15 • (y - 21) (mod 26).

Теперь мы можем расшифровать сообщение TVYXK.

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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Буква T стоит на позиции 19, ей соответствует расшифрованная буква, стоящая на позиции 15 • (19 - 21) = -30 ≡ 22 (mod 26). Буква, стоящая в алфавите на позиции 22, — это W.

Буква V стоит на позиции 21, ей соответствует расшифрованная буква, стоящая на позиции 15 • (21 -21) = 0 ≡ 0 (mod 26). Буква, стоящая в алфавите на позиции 0, — это A.

Буква Y стоит на позиции 24, ей соответствует расшифрованная буква, стоящая на позиции 15 • (24 - 21) = 45 ≡ 19 (mod 26). Буква, стоящая в алфавите на позиции 19, — это T.

Буква X стоит на позиции 23 ей соответствует расшифрованная буква, стоящая на позиции 15 • (23 - 21) = 30 ≡ 4 (mod 26). Буква, стоящая в алфавите на позиции 4, — это E.

Буква K стоит на позиции 10, ей соответствует расшифрованная буква, стоящая на позиции 15 • (10 - 21) = -165 ≡ 17 (mod 26). Буква, стоящая в алфавите на позиции 17, — это R.

Расшифрованное слово – слово WATER.

Одним из существенных достоинств хорошего алгоритма шифрования является способность генерировать большое количество ключей. И шифр Цезаря, и аффинный шифр уязвимы для криптоанализа, поскольку максимальное количество ключей ограничено.

Если мы снимем какие-либо ограничения относительно порядка букв шифроалфавита, то потенциальное количество ключей резко возрастет. Количество ключей для стандартного алфавита из 26 символов (расположенных в произвольном порядке) составляет 26! = 403291461126605635584000000, то есть более 403 септиллионов ключей.

ЛИТЕРАТУРА

1. Мир математики: в 40 т. Т. 2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. / Пер. с англ. — М.: Де Агостини, 2014. — 144с.

2. Свободная энциклопедия Wikipedia.

УДК004.932

Студ. А. Н. Зайцев
Науч. рук. асс. Т. Г. Шагова
(кафедра высшей математики, БГТУ)

СЖАТИЕ ИЗОБРАЖЕНИЙ ПРИ ПОМОЩИ MRC-КОМПРЕССИИ

В современном мире человеку приходится работать с огромным количеством информации. И одной из ключевых проблем является сохранение всей информации на различных цифровых носителях. Так как объём данных растёт быстрее, чем вместимость накопителей, то сжатие данных является крайне актуальной темой.

В сфере документооборота это также актуально. Стандартом для сохранения документов в настоящий момент является формат PDF. К сожалению, PDF файлы имеют довольно большой объём. Поэтому и развиваются различные методы сжатия PDF документов.