

Шифрование методом гаммирования

Шифрование (зашифрование) — процесс применения шифра к защищаемой информации, т.е. преобразование исходного сообщения в зашифрованное. Под шифром понимается совокупность методов и способов обратимого преобразования информации с целью ее защиты от несанкционированного доступа (обеспечения конфиденциальности информации). Ключ – переменный параметр шифра, обеспечивающий выбор одного преобразования из совокупности всевозможных для данного алгоритма и сообщения. В общем случае, ключ – это минимально необходимая информация (за исключением сообщения, алфавитов и алгоритма), необходимая для шифрования и дешифрования сообщений.

Гамми́рование — 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. Симметри́чные криптосисте́мы (также симметричное шифрование, симметричные шифры) (англ. symmetric-key algorithm) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

$$C_i = (T_i + G_i) \bmod N$$

Примечания:

а) \bmod - операция целочисленного деления, вычисляющая остаток от деления.

Например, $18 \bmod 5 = 3$ или $48 \bmod 44 = 4$.

б) N равен количеству символов применяемого алфавита.

в) C_i , T_i и G_i - номера i -х символов, соответственно, шифрограммы, шифруемого текста и гаммы

г) если C_i будет равно нулю, то его следует приравнять N .

Создание шифрограммы завершается заменой полученных чисел C_i на соответствующие буквы алфавита.

В рассмотренном ниже примере исходное сообщение - «КАФЕДРА СИСТЕМ ИНФОРМАТИКИ», используемая гамма - «СИМВОЛ».

$$C_i = (T_i + G_i) \bmod N$$

T	К	А	Ф	Е	Д	Р	А		С	И	С	Т	Е	М		И	Н	Ф	О	Р	М	А	Т	И	К	И
G	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И
T	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10
G	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10
T+G	31	11	36	9	21	31	20	44	33	13	35	33	25	24	48	13	31	35	35	28	28	4	36	23	31	20
mod N	31	11	36	9	21	31	20	0	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20
0 → N	31	11	36	9	21	31	20	44	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20
C	Э	Й	1	З	У	Э	Т	9	Я	Л	0	Я	Ч	Ц	Г	Л	Э	0	0	Ъ	Ъ	Г	1	Х	Э	Т

Схема шифрования гаммированием по модулю N



В данной теме используется алфавит, состоящий из 44 символов
Алфавит «Русские буквы, цифры и пробел» (44 символа)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44		
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	пробел	1	2	3	4	5	6	7	8	9	0		

Дешифрирование выполняется по формуле

$$T_i = (C_i - G_i + N) \bmod N,$$

где T_i – это символы исходного сообщения, C_i – символы зашифрованного сообщения, G_i – символы гаммы.

Примечание: если $T_i = 0$, то его следует взять равным N .

C	Э	Й	1	З	У	Э	Т	9	Я	Л	О	Я	Ц	Г	Л	Э	0	0	Ъ	Ъ	Г	1	Х	Э	Т			
G	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И		
C	31	11	36	9	21	31	20	44	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20		
G	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10		
C-G	12	1	22	6	5	18	1	34	19	10	19	20	6	14	-10	10	15	22	16	18	14	1	20	10	12	10		
C-G+N	56	45	66	50	49	62	45	78	63	54	63	64	50	58	34	54	59	66	60	62	58	45	64	54	56	54		
mod N	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10		
0 → N	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10		
T	К	А	Ф	Е	Д	Р	А			С	И	С	Т	Е	М			И	Н	Ф	О	Р	М	А	Т	И	К	И

Образец текста
 Второй уровень
 Третий уровень
 Четвертый уровень
 Пятый уровень

Номер буквы Э
 Номер буквы С
 $31 - 19 = 12$
 $31 - 19 + 44 = 56$
 $56 \bmod 44 = 12$
 12 – номер буквы К

Шифрование фамилии методом гаммирования

- ▶ Расшифруйте зашифрованный текст:

9Э8Ъ7

- ▶ Используемая гамма: «ШИФР»

$$T_i = (C_i - G_i + N) \bmod N$$

С

9

Э

8

Ъ

7

G

С

G

С-G

С-G+N

Mod N

T

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44		
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	пробел	1	2	3	4	5	6	7	8	9	0		

Ответ: ПУТИН

▶ Как зашифровали:

T	П	У	Т	И	Н
G	Ш	И	Ф	Р	Ш
T	17	21	20	10	15
G	26	10	22	18	26
T+G	43	31	42	28	41
Mod N	43	31	42	28	41
T	9	Э	8	Ъ	7

Как расшифровывать:

C	9	Э	8	Ъ	7
G	Ш	И	Ф	Р	Ш
C	43	31	42	28	41
G	26	10	22	18	26
C-G	17	21	20	10	15
C-G+N	61	65	64	54	59
Mod N	17	21	20	10	15
T	П	У	Т	И	Н

Шифрование фамилии методом гаммирования

C

9 Ш А _ 1 Ш Ч С

G

C

G

C-G

C-G+N

Mod N

T

- ▶ Расшифруйте зашифрованный текст:

9Ш1_1ШЧС

- ▶ Используемая гамма: «ШИФР»

$$T_i = (C_i - G_i + N) \bmod N$$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х

24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44

Ц Ч Ш Щ Ъ Ы Ь Э Ю Я пробел 1 2 3 4 5 6 7 8 9 0

Ответ: ПОЛОЗОВА

▶ Как шифровали:

Как расшифровывать:

T	П	О	Л	О	З	О	В	А
G	Ш	И	Ф	Р	Ш	И	Ф	Р
T	17	16	13	16	9	16	3	1
G	26	10	22	18	26	10	22	18
T+G	43	26	35	34	35	26	25	19
Mod N	43	26	35	34	35	26	25	19
T	9	Ш	1	_	1	Ш	Ч	С

C	9	Ш	1	_	1	Ш	Ч	С
G	Ш	И	Ф	Р	Ш	И	Ф	Р
C	43	26	35	34	35	26	25	19
G	26	10	22	18	26	10	22	18
C-G	17	16	13	16	9	16	3	1
C-	61	60	57	60	53	60	47	45
G+N								
Mod	17	16	13	16	9	16	3	1
N								
T	П	О	Л	О	З	О	В	А