Гаммирование

Шифры гаммирования (аддитивные шифры) являются самыми эффективными с точки зрения стойкости и скорости преобразований (процедур шифрования и дешифрования).

По стойкости данные шифры относятся к классу совершенных (неподдающихся вскрытию).

Для шифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (**mod**).

Например: 5+10 mod 4 = 15 mod 4 = 3

В шифрах гаммирования может использоваться:

- сложение по модулю N (общий случай)
- сложение по модулю 2 (частный случай, ориентированный на программно-аппаратную реализацию)

Сложение по модулю N

При замене букв исходного сообщения и ключа на числа справедливы формулы:

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

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

N - количество символов в алфавите;

K_i - i-ый символ гаммы (ключа).

Данные формулы позволяют выполнить зашифрование / расшифрование 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

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:

Символ								
	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
	шифрограммы, C_i	**Ж**	**Ф**	**Б**	**И**	**В**	**Ч**	**П**
		7	21	1	9	2	24	16

Сложение по модулю 2 (шифр Вернама)

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 «+ + – + +» означала перехода от букв к цифрам.

На бумажной ленте, используемой при работе телетайпа, знаку «+» соответствовало *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.

Шифровальная машина

Вернам: складывать «импульсы» знаков открытого текста с «импульсами» гаммы, предварительно нанесенными на ленту. Сложение «по модулю 2» (⊕, для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»).

Если «+», то 1, если «–», то 0.

сложение определяется двоичной арифметикой:

⊕	0	1
0	0	1
1	1	0

Процедуры шифрования и дешифрования выполняются по следующим формулам:

$$C_i = P_i \oplus K_i,$$

$$P_i = C_i \oplus K_i.$$

Коды символов Windows 1251 и их двоичное представление

Буква	Dec-код	Bin-код	Буква	Dec-код	Bin-код	Буква	Dec-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			

Пример шифрования по модулю 2

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

Так как длина ключа меньше длины открытого сообщения, то для генерации гаммы он циклически повторяется.

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

Упражнения для самопроверки

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	∑
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №1

И.РЮУ.ЪФОБГНО

СЛХГ.ЪЛХО.ФОО.ЩВ

Упражнения для самопроверки

2. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	∑
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №2

▽*!(∞♦№ > ♯⊕

@♠ – ♡∞ ▽ *!(–)♯ * Δ

Упражнения для самопроверки

3. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:

- ЖЕЛТЫЙ_ОГОНЬ
- МЫ_НАСТУПАЕМ

4. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:

- СЛПИЬНАЕ
- РОИАГДВН

5. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:

- МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР
- СИГНАЛ БОЯ – НИСАГО ЛЯБ

Упражнения для самопроверки

6. Зашифруйте сообщения методом перестановки по таблице 5*5. Ключ указывает порядок считывания столбцов при шифровании.
   - ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)
   - ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)
7. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.
   - ЕАУПД_КЕАЗАРЧВ (ключ: 4123)
   - А_НСЫИЛБСАЛЙГ (ключ: 3142)