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 mod 4 = 15 mod 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

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

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

где P_i, C_i - i-ый символ открытого и шифрованного сообщения; N - количество символов в алфавите; K_i - i-ый символ гаммы (ключа). Если длина гаммы меньше, чем длина сообщения, то она используется повторно.

Данные формулы позволяют выполнить зашифрование / расшифрование по Виженеру 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

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 1. Пример аддитивного шифрования по модулю N = 33

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

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

Т.е., 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

$$C_i = P_i \oplus K_i$$

$$P_i = C_i \oplus K_i.$$

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 **шифрблокноты**. 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 2. 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			

[Примечание. Dec-код – десятичный код символа, Bin-код – двоичный код символа]

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

Таблица 3. Пример аддитивного шифрования по модулю 2

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

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

Таблица 4. Пример использования ложной гаммы

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

Ярким примером шифра гаммирования по модулю 2 является RC4.

RC4 (от англ. Rivest cipher или Ron’s code) является синхронным потоковым шифром. Был создан сотрудником компании «RSA Security» Рональдом Ривестом в 1987 г. В течение семи лет шифр являлся коммерческой тайной, и точное описание алгоритма предоставлялось только после подписания соглашения о неразглашении, но в сентябре 1994 г. его описание было анонимно отправлено в список рассылки «Cypherpunks».

Шифрование выполняется гаммированием по модулю 2.

Этап 1. Инициализация S-блока.

Перед генерацией гаммы выполняется инициализация **S-блока** длиной L_s. Обычно L_s выбирается кратно 8 битов ($2^8 = 256$, $2^{16} = 65536$ и т.п.). Для инициализации используется ключ **K** длиной L_K от 40 до 2048 битов по следующему алгоритму.

1. Цикл A. Для i := 0 до L_s - 1

    1.1. S[i] := i

2. j := 0

3. Цикл B. Для i := 0 до L_s - 1

    3.1. j := (j + S[i] + K[i mod L_K]) mod L_s

    3.2. Поменять местами S[i] и S[j]

Этап 2. Генерация гаммы.

Непосредственная генерация гаммы выполняется циклически блоками по $\mathbf{L_s}$ битов до достижения необходимой длины псевдослучайной последовательности $\mathbf{L_g}$. Алгоритм генерации следующий.

1. i := 0

2. j := 0

3. L := 0

4. Цикл. Пока L < L_g

    4.1. i := (i + 1) mod L_s

    4.2. j := (j + S[i]) mod L_s

    4.3. Поменять местами S[i] и S[j]

    4.4. t := (S[i] + S[j]) mod L_s

    4.5. Блок гаммы := S[t]

    4.6. L := L + L_s

Внутреннее состояние генератора гаммы описывается **S-блоком**, строки 4.1 - 4.3 представляют собой **функцию переходов**, а строки 4.4 - 4.5 — **выходную функцию**.

RC4 получил широкое распространение в криптосистемах и протоколах, в частности:

- WEP (англ. Wired Equivalent Privacy) — алгоритм для обеспечения безопасности сетей Wi-Fi;

- WPA (англ. Wi-Fi Protected Access) — обновленный алгоритм сертификации устройств сетей Wi-Fi;

- BitTorrent protocol encryption — протоколы пиринговых файлообменных сетей;

- SSL (англ. Secure Sockets Layer) — криптографический протокол передачи данных в сети;

- Kerberos — сервер аутентификации Kerberos;

- PDF (англ. Portable Document Format) — межплатформенный формат электронных документов, разработанный фирмой Adobe Systems;

- Skype — программное обеспечение IP-телефонии;

- и др.

Обнаруженные уязвимости в стандартной реализации RC4 привели к отказу от его использования в некоторых криптосистемах и протоколах, а также появлению различных его модификаций: RC4A, RC4+, VMPC, Spritz.

Комбинированные (составные) шифры.

Предполагают использование для шифрования сообщения сразу нескольких методов (например, сначала замена символов, а затем их перестановка).

Два самых известных полевых шифра в истории криптографии - ADFGX и ADFGVX. Шифр ADFGX впервые был использован во время решающих этапов Первой мировой войны, когда в марте 1918 г. кайзеровские генералы начали крупное наступление. Шифр ADFG(V)X был разработан полковником Фрицем Небелем, офицером связи, служившим в штабе германской армии. Оба шифра предполагают вначале применение к буквам исходного сообщения замену, после чего для получения окончательной шифрограммы выполняется перестановка.

Таблица шифрозамен ADFGX представляет собой матрицу 5 х 5, а для ADFGVX – 6 х 6. Строки и столбцы обозначаются буквами, входящими в название шифра. Пример таблицы шифрозамен для шифра ADFGVX применительно к русскому алфавиту показан на следующем рисунке.

	A	D	F	G	V	X
A	Ю	У	И	Ч	К	Б
D	В	Г	Е	Ф	Ж	З
F	Й	А	Л	М	О	П
G	Р	Щ	Т	Я	Ё	Х
V	Ц	Н	Ш	С	Ъ	Ы
X	Ь	Э	Д	-	-	-

Рис.1. Пример таблицы шифрозамен для шифра ADFGVX

Шифрозамена для буквы исходного текста состоит из букв, обозначающих строку и столбец, на пересечении которых она находится (см. шифр «Полибианский квадрат»). Например, для сообщения «АБРАМОВ» набор шифрозамен будет «FD AX GA FD FG FV DA».

На втором этапе для выполнения перестановки полученный набор шифрозамен вписывается построчно сверху-вниз в таблицу, количество столбцов в которой строго определено (ADFGX) или соответствует количеству букв в ключевом слове (ADFGVX). Нумерация столбов либо оговаривается сторонами (ADFGX) либо соответствует положению букв ключевого слова в алфавите, как в шифре вертикальной перестановки (ADFGVX). Например, для полученного выше набора шифрозамен перестановочная таблица с ключевым словом «ДЯДИНА» показана на следующем рисунке.

Д	Я	Д	И	Н	А
2	6	3	4	5	1
F	D	A	X	G	A
F	D	F	G	F	V
D	A				

Рис.2. Перестановочная таблица шифра ADFGVX с ключевым словом «ДЯДИНА»

На третьем этапе буквы выписываются из столбцов в соответствии с их нумерацией, при этом считывание происходит по столбцам, а буквы объединяются в пятибуквенные группы. Таким образом, окончательная шифрограмма для рассматриваемого примера будет выглядеть «AVFFD AFXGG FDDA».

Задание на практическую работу

В работе необходимо зашифровать свою «фамилию_имя_отчество» и «фамилию_имя_отчество» заведующего кафедры с помощью шифров гаммирования по **модулю N** и **модулю 2** и с помощью **шифра ADFGVX**.

При оформлении отчета необходимо привести

- исходное сообщение (фамилию_имя_отчество), гамму и таблицы зашифрования/дешифрования [гаммирование].
- привести исходное сообщение (фамилию_имя_отчество), таблицу шифрозамен, ключевое слово, перестановочную таблицу и зашифрованное сообщение [комбинированные].