Шифры гаммирования

Занятие 2 (лекция)

§ 1. Основная часть

Шифры гаммирования

На данной части занятия будем рассматривать шифры, которые относятся к шифрам замены, но выделяются в собственный класс в связи со своими характерными свойствами и особенностями. Эти шифры получили название *шифров гаммирования*.

В алфавите любого естественного языка буквы следуют друг за другом в определенном порядке. Это дает возможность присвоить каждой букве алфавита ее естественный порядковый номер. Так, в английском алфавите букве *A* присваивается порядковый номер 1, букве *Q* - порядковый номер 17, а букве *Z* - порядковый номер 26. Аналогичное отождествление можно осуществить и для русского алфавита, например для RUS30 (где *Ё=Е, Й=И, Ъ=Ь*). Буква *А* будет иметь порядковый номер 1, *О* - номер 14, *Я* - 30. Если в открытом сообщении каждую букву заменить ее естественным порядковым номером в рассматриваемом алфавите, то преобразование числового сообщения в буквенное позволяет однозначно восстановить исходное открытое сообщение. Например, числовое сообщение

1 11 20 1 3 9 18

в алфавите RUS30 преобразуется в буквенное сообщение:

АЛФАВИТ

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	Ы	Ь Ъ	Э	Ю	Я
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

Зададим теперь преобразования зашифрования f и преобразования расшифрования g для произвольного шифра гаммирования. Пусть:

- необходимо зашифровать сообщение $X = x_1, \dots, x_T$ в алфавите $\Omega = a_1, \dots, a_n$.

- n - мощность алфавита.
- Каждая буква отождествляется со своим порядковым номером в алфавите.
- Выберем некоторую последовательность, составленную из букв $\Omega: \gamma_1, \dots, \gamma_T$ - данная последовательность называется *гаммой* шифра, или *ключевой последовательностью*.

Тогда преобразованием зашифрования f_{k_i} будет являться преобразование, при котором i-ая буква шифртекста y_i равна:

$$y_i = f_{k_i}(x_i) = r_n(x_i + \gamma_i),$$

где $k_i = \gamma_i$ - используемый знак гаммы последовательности для шифрования i-той буквы сообщения x_i; $r_n(b)$ - остаток от деления числа числа b на n (полагаем, что $r_n(n) = n$).

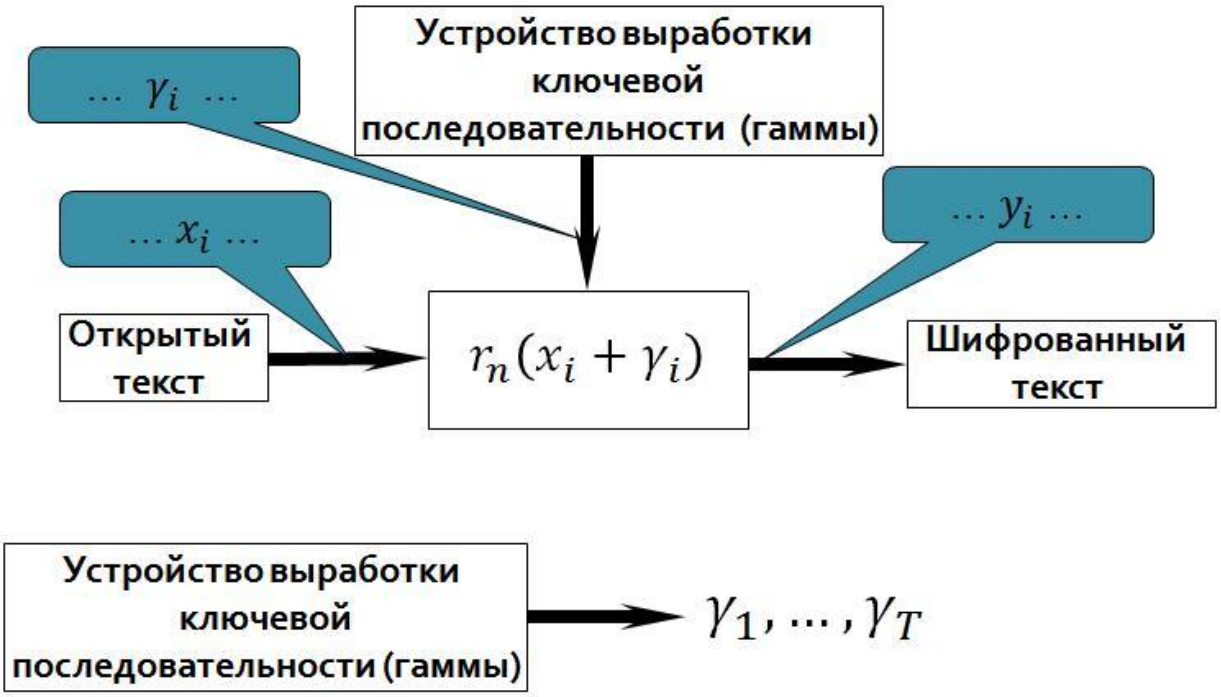
Итак, зашифрование шифром гаммирования означает «сложение» или, как говорят, «наложение» некоторой последовательности (гаммы) на знаки (буквы) открытого текста. Очевидно, что в таком случае для расшифрования нужно вычесть из букв шифртекста знаки гаммы:

$$x_i = g_{k_i}(y_i) = r_n(y_i - \gamma_i).$$

Соответственно, в силу сказанного, весь отрезок гаммы (то есть вся последовательность) является ключом данного шифра, именно поэтому ее называют ключевой последовательностью.

Отметим, что аналогичные формулы для шифрования и расшифрования мы видели на прошлом занятии, когда рассматривали сдвиговые шифры. Все дело в том, что сдвиговый шифр на самом деле является частным случаем шифра гаммирования, когда вся гамма представляется одним и тем же значением k (то есть, другими словами, когда все элементы гаммы γ_i равны k).

На данной схеме изображен процесс зашифрования сообщения шифром гаммирования.



В каждый момент времени в устройство шифрования (шифратор) подается очередная буква открытого текста x_i и подается знак гаммы γ_i, сгенерированный по некоторому правилу (закону) устройством выработки ключевой последовательности. Согласно формуле $y_i = r_n(x_i + \gamma_i)$ шифратор вырабатывает очередную букву шифрованного текста. Данный процесс продолжается до тех пор пока в через шифратор не «пройдут» все буквы открытого текста.

Зашифруем слово **АЛФАВИТ** на следующей гамме: **ИДФНТВХ.**

$$y_1 = r_{30}(\text{А} + \text{И}) = r_{30}(1 + 9) = 10 = \text{К},$$

$$y_1 = r_{30}(\text{Л} + \text{Д}) = r_{30}(11 + 5) = 16 = \text{Р},$$

$$y_1 = r_{30}(\text{Ф} + \text{Ф}) = r_{30}(20 + 20) = 10 = \text{К},$$

$$y_1 = r_{30}(\text{А} + \text{Н}) = r_{30}(1 + 13) = 14 = \text{О},$$

$$y_1 = r_{30}(\text{В} + \text{Т}) = r_{30}(3 + 18) = 21 = \text{Х},$$

$$y_1 = r_{30}(\text{И} + \text{В}) = r_{30}(9 + 3) = 12 = \text{М},$$

$$y_1 = r_{30}(\text{Т} + \text{Х}) = r_{30}(18 + 21) = 9 = \text{И}.$$

Получим шифртекст: **КРКОХМИ**.

Шифр Виженера

Одним из частных случаев шифра гаммирования является шифр Виженера, описанный в 1585 году французом Блезом де Виженером в его "Трактате о шифрах". Опишем данный шифр.

Шифр Виженера является шифром гаммирования с краткопериодической гаммой (то есть гаммой, которая является повторением некоторого короткого слова – периода).

Пусть в алфавите Ω задан открытый текст $X = x_1, \dots, x_T$. Выберем некоторое слово длины t $\gamma_1^*, \dots, \gamma_t^*$ из букв рассматриваемого алфавита. Данное слово будет являться ключом (ключевым словом). Сформируем гамму с длиной, равной длине открытого текста (то есть T) путем **повторения** ключевого слова необходимое число раз:

$$\gamma_1^*, \dots, \gamma_t^*, \gamma_1^*, \dots, \gamma_t^*, \dots$$

Наложим эту периодическую гамму (периодом которой является ключевое слово) на открытый текст $x_1, \dots, x_T$. Получим шифртекст $y, \dots, y_T$.

Математически процесс зашифрования можно описать следующей формулой:

$$y_i = f_{k_i}(x_i) = r_n(x_i + \gamma_{r_t(i)}^*),$$

где $k_i = \gamma_{r_t(i)}^*$, $r_n(b)$ – остаток от деления числа b на n.

Уравнение расшифрования:

$$x_i = g_{k_i}(y_i) = r_n(y_i - \gamma_{r_t(i)}^*)$$

Например, зашифруем слово АЛФАВИТ шифром Виженера (в алфавите RUS30). Для этого выберем ключевое слово, скажем, МИР. Поскольку открытый текст имеет длину 7, а ключевое слово – 3, то гамма шифра будет следующая:

МИРМИРМ

Сложим полученную гамму и открытый текст, получим:

АЛФАВИТ

+МИРМИРМ

НФЕНМЩЯ

Таким образом, шифртекст НФЕНМЩЯ.

§ 2. Решение задач

Задача № 7

Для передачи сообщения на русском языке Крокодил Гена и Чебурашка выполняют следующие действия. Каждый из них выбирает свою последовательность, состоящую из целых чисел в пределах от 0 до 32, длина которой равна длине сообщения. Буквы сообщения заменяются числами по табл. 2.

Таблица 2

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
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	0

Сначала Гена шифрует сообщение, используя свою последовательность. Для этого числовое значение первой буквы сообщения и первое число его последовательности складываются, а полученная сумма заменяется остатком от деления на 33 и вновь заменяется буквой по табл. 2. Затем эта процедура повторяется для вторых, третьих и т.д. чисел сообщения и последовательности. Полученный результат: **ЁЛИСУВШОЮЦОМЮВЫЗПЭЪМО** передаётся Чебурашке. После этого Чебурашка шифрует полученное сообщение с помощью своей последовательности. Получается строка **ЪЭЛВШРЕЭЭТЖЩЮИГВФБСЦХ.** Эту строку он и передает Гене.

Гена вычитает из числовых значений букв полученного сообщения числа своей последовательности (к отрицательной разнице прибавляется число 33) и передаёт результат **ЖЪЫХЙТСЖЫАШШЬЯМЫШЗЬВГ** Чебурашке**.** Какое сообщение зашифровал Крокодил Гена?

Решение:

В условии задачи имеется 3 зашифрованных сообщения:

$C_1 = M + K_Г$ = **ЁЛИСУВШОЮЦОМЮВЫЗПЭЪМО**;

$C_2 = C_1 + K_Ч = M + K_Г + K_Ч$ = **ЪЭЛВШРЕЭЭТЖЩЮИГВФБСЦХ**;

$C_3 = C_2 - K_Г = M + K_Ч$ = **ЖЪЫХЙТСЖЫАШШЬЯМЫШЗЬВГ**,

где M – исходное сообщение, $K_Г$ – последовательность, выбранная Крокодилом Геной; $K_Ч$ – последовательность, выбранная Чебурашкой.

Итак, в данной задаче идет речь о шифре гаммирования. Гена и Чебурашка вырабатывают свою гамму, а затем происходит обмен сообщениями, как это описано в задаче. Рассмотрим процесс обмена сообщениями:

1. Гена отправляет Чебурашке сообщение $C_1 = M + K_Г$.
2. Чебурашка накладывает на полученное сообщение гамму и отправляет обратно Гене: $C_2 = M + K_Г + K_Ч$.
3. Гена вычитает из полученного C_2 свою гамму и отправляет сообщение: $C_3 = C_2 - K_Г = M + K_Ч$.

Далее Чебурашка, зная свою гамму расшифровывает в итоге сообщение *M*.

Не смотря на казалось бы, сложный протокол обмена сообщениями, сторонний наблюдатель, обладая всеми тремя сообщениями (но не зная гаммы) так же может определить М. Итак, зная $C_1,\ C_2, C_3$ наблюдатель может по следующей формуле найти М:

$$M = C_1 - C_2 + C_3 = M + K_Г - \ M + K_Г + K_Ч \ + M + K_Ч.$$

Раскрыв скобки, несложно убедиться, что это действительно верно.

Найдем по указанной формуле исходное сообщение. В итоге, можно получить следующее предложение:

ТИШЕ ЕДЕШЬ ДАЛЬШЕ БУДЕШЬ.

Ответ: *ТИШЕ ЕДЕШЬ ДАЛЬШЕ БУДЕШЬ***.**

Задача № 8

Осмысленная фраза на русском языке записана **два раза подряд** без пробелов и знаков препинания и зашифрована шифром Виженера. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

МХЛЩЛИФЦБДЮГИШСПТАИВПБЬДЮОЛДЬУЭЮЫЙЕМХЛ

Восстановите исходное сообщение и ключевое слово, если известно, что его первой буквой является одна из четырех: Л, П, К, Р.

Табл. 2

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
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	33

Решение:

Убеждаемся, что шифрованный текст имеет длину 38. Осмысленное предложение имеет тогда длину 19.

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}
γ_1	γ_2	γ_3	γ_4	γ_5	γ_1	γ_2	γ_3	γ_4	γ_5	γ_1	γ_2	γ_3	γ_4	γ_5	γ_1	γ_2	γ_3	γ_4
м	**х**	**л**	**щ**	**л**	**и**	**ф**	**ц**	**б**	**д**	**ю**	**г**	**и**	**ш**	**с**	**п**	**т**	**а**	**и**

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}
γ_5	γ_1	γ_2	γ_3	γ_4	γ_5	γ_1	γ_2	γ_3	γ_4	γ_5	γ_1	γ_2	γ_3	γ_4	γ_5	γ_1	γ_2	γ_3
в	**п**	**б**	**ь**	**д**	**ю**	**о**	**л**	**д**	**ь**	**у**	**э**	**ю**	**ы**	**й**	**е**	**м**	**х**	**л**

$$r_{33}(x+\gamma)=y$$

Табл. 2

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
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	33

в	**п**	**б**	**ь**	**д**
м	**х**	**л**	**щ**	**л**
22	27	22	3	25

Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв, исходя из отождествления, указанного в таблице.

в п б ь д

м х л щ л

22	27	22	3	25

Получаем: 22 27 22 3 25 ... . Если $\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$ - ключевое слово, то при первом шифровании использовалось оно само, а при втором - $\gamma_5, \gamma_1, \gamma_2, \gamma_3, \gamma_4$. Таким образом, найденные разности равны соответственно:

$$r_{33}(\gamma_5 - \gamma_1), r_{33}(\gamma_1 - \gamma_2),\ r_{33}(\gamma_2 - \gamma_3),\ r_{33}(\gamma_3 - \gamma_4), r_{33}(\gamma_4 - \gamma_5).$$

$$\begin{cases} \gamma_5 - \gamma_1 = 22 \\ \gamma_1 - \gamma_2 = 27 \\ \gamma_2 - \gamma_3 = 22 \\ \gamma_3 - \gamma_4 = 3 \\ \gamma_4 - \gamma_5 = 25 \end{cases} \Rightarrow \begin{cases} \gamma_2 = \gamma_1 + 6 \\ \gamma_3 = \gamma_1 + 17 \\ \gamma_4 = \gamma_1 + 14 \\ \gamma_5 = \gamma_1 + 22 \end{cases}$$

Тогда при известной 1-ой букве гаммы γ_1 остальные вычисляются по формулам, указанным выше. Далее перебирая все 4 варианта для первой буквы γ_1 (указанных в условии задачи), приходим к одному осмысленному слову КРЫША.

Далее остается расшифровать текст на данном слове, получим:

В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р .

Ответ: *В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р, КРЫША.*