Введение в криптографию. Шифры замены

Занятие 1 (лекция)

§ 1. Основная часть

Зачем нужна криптография?

Как передать нужную информацию нужному адресату в тайне от других? Размышляя над задачей тайной передачи сообщений, нетрудно прийти к выводу, что есть три возможности:

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.
2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.
3. Использовать общедоступный канал связи, но передавать по нему информацию в преобразованном виде, чтобы восстановить ее мог только адресат.

Прокомментируем их.

1. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для неоднократной передачи больших объемов информации практически нереально.
2. Разработкой средств и методов скрытия факта передачи сообщения занимается ***стеганография***. Первые следы стеганографических методов теряются в глубокой древности. Например, известен такой способ скрытия письменного сообщения: голову раба брили, на коже головы писали сообщение и после отрастания волос раба отправляли к адресату. Из детективных произведений хорошо известны различные способы тайнописи между строк обычного, незащищаемого текста. В настоящее время в связи с широким распространением компьютеров известно много тонких методов сокрытия защищаемой информации внутри больших объемов информации, хранящейся в компьютере.

Наглядный пример сокрытия текстового файла в графический можно найти в Интернете.

3. Разработкой методов преобразования информации с целью ее защиты от незаконных пользователей занимается ***криптография***. Такие методы и способы преобразования информации называются *шифрами*.

Что такое криптография?

Криптография («криптос» - тайна, «графэйн» - писать) - *наука о методах обеспечения*

- *конфиденциальности (невозможности прочтения информации посторонним)*
- *аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства)*

информации.

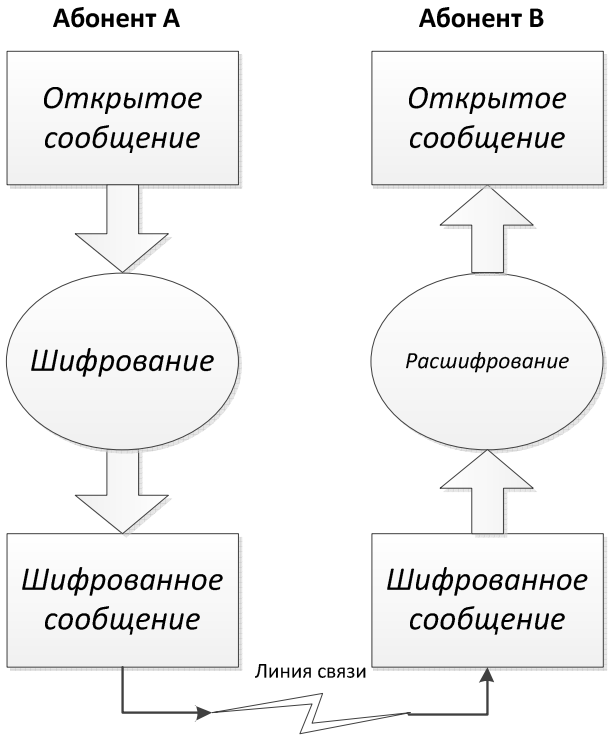
Дословно термин «криптография» означает «тайнопись». Смысл этого термина выражает основное предназначение криптографии - защитить или сохранить в тайне необходимую информацию.

В отличие от стеганографии криптография не «прячет» передаваемые сообщения, а преобразует их в форму, недоступную для понимания противником. Преобразованное сообщение будем называть *шифрованным сообщени*ем (или зашифрованным сообщением). Другое название зашифрованного сообщения – *криптограмма*, или *шифртекст*.

Основные термины, используемые в криптографии

Рассмотрим типичную схему обмена сообщениями между абонентами, которые хотят защитить передаваемую информацию от посторонних.

1. Сообщение, которое передается адресату, называется *открытым сообщением*.



2. Преобразованное криптографическими методами сообщение называется *шифрованным сообщением*, или *шифртекстом*.
3. Процесс преобразования открытого сообщения в шифрованное называется *шифрованием*, или *зашифрованием*.
4. Процесс преобразования шифртекста абонентом-получателем в открытое сообщение называется *расшифрованием* (не следует данный термин путать с термином «дешифрование»)

Формализуем математически процесс зашифрования и расшифрования. Для этого введем следующие обозначения:

- X - открытое сообщение,
- Y - шифрованное сообщение,
- f - правило шифрования (функция, определенная на множестве всех открытых текстов),
- g - правило расшифрования (функция, определенная на множестве всех шифртекстов).

Тогда зашифрование X в Y можно записать в виде

$$f(X) = Y.$$

Обратное преобразование (то есть получение открытого сообщения X путем расшифрования Y) запишется в виде соотношения

$$g(Y) = X.$$

Отметим, что правило зашифрования f не может быть произвольным. Оно должно быть таким, чтобы по шифртексту Y с помощью правила расшифрования g можно было однозначно восстановить открытое сообщение X, иначе адресат просто не поймет, какое именно сообщение передавалось. При этом надо отметить, что при выборе правила шифрования f надо стремиться к тому, чтобы посторонние лица, не знающие правила расшифрования g, не смогли восстановить по криптограмме открытое сообщение. В случае же, если противнику удастся это сделать, то говорят о *дешифровании* сообщения.

Однотипные правила зашифрования можно объединить в классы. Внутри класса правила зашифрования различаются между собой по значениям некоторого параметра, которое может быть числом, таблицей и т.д. В криптографии конкретное значение такого параметра обычно называют *ключом*. По сути дела, ключ выбирает конкретное правило зашифрования из данного класса правил.

Зачем понадобилось вводить понятие *ключа*? Есть, по крайней мере, два обстоятельства, которые позволяют понять необходимость этого. Во-первых, обычно шифрование производится с использованием специальных устройств. У вас должна быть возможность изменять значение параметров устройства, чтобы зашифрованное сообщение не смогли расшифровать даже лица, имеющие точно такое же устройство, но не знающие выбранного вами значения параметра. Во-вторых, многократное использование одного и того же правила зашифрования f для зашифрования открытых текстов создает предпосылки для получения открытых сообщений по шифрованным без знания правила расшифрования g. Поэтому необходимо своевременно менять правило зашифрования.

Используя понятие *ключа*, процесс зашифрования можно описать в виде соотношения:

$$f_k(X) = Y,$$

в котором k - выбранный ключ, известный отправителю и адресату.

Для каждого ключа k шифрпреобразование f_k должно быть обратимым, то есть должно существовать обратное преобразование g_k, которое при выбранном ключе k однозначно определяет открытое сообщение Y по шифрованному сообщению X, то есть выполняется равенство $g_k(Y) = X$.

Совокупность преобразований f_k и набор ключей, которым они соответствуют, будем называть *шифром*.

Простейшие шифры

Среди всех шифров можно выделить два больших класса: *шифры замены* и *шифры перестановки*. На данном занятии будем рассматривать только шифры замены.

Шифрами замены называются такие шифры, преобразования в которых приводят к замене каждого символа открытого сообщения на другие символы - *шифробозначения*, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения.

Рассмотрим далее основные примеры таких шифров (в том числе и исторические).

Примеры шифров замены

1. ***Шифр Цезаря.*** Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, применял следующее шифрпреобразование: он заменял в тексте каждую букву A (первую в алфавите) на D (на четвертую в алфавите), букву B (вторую в алфавите) – на E (пятую в алфавите) и т.д. Таким образом нижняя строка замены (см. таблицу) образовывалась циклическим сдвигом алфавита открытого текста на 3 буквы влево.

Например, слово CAESAR шифровалось бы как:

FDHVDU

2. ***Шифр простой замены.*** Шифр простой замены подразумевает замену букв алфавита на буквы алфавита (в общем случае, не обязательно того же), при этом разным буквам ставятся в соответствие разные буквы. Формально шифр буквенной простой замены в алфавите $\Omega = \{a_1, \dots, a_n\}$ можно описать таблицей, которая является его ключом, вида

a_1	a_2	a_3	…	a_n
a_{i_1}	a_{i_2}	a_{i_3}	…	a_{i_n}

где

$(i_1, i_2, i_3, \dots, i_n)$ – некоторая перестановка чисел $(1,2,3, \dots, n)$. Таблица указывает на то, что шифрование должно осуществляться следующим образом: каждая буква a_k в открытом тексте заменяется на букву a_{i_k}. Чтобы расшифровать полученный шифртекст, нужно произвести обратную процедуру: каждую букву a_{i_k} заменить на a_k. В качестве примера данного шифра можно привести шифр Цезаря. Отметим, что нижняя строка таблицы может представлять собой и некоторые символы нового алфавита, например сочетание цифр. Скажем, каждая буква ОТ рассматриваемого алфавита может переходить в пару цифр.

Рассмотрим шифр простой замены, соответствующий таблице:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
11	98	33	42	19	13	87	54	43	49	48	50	69	32	73	18	81	29	76	74	22	31	90	59	67	77	91	12	52	45

В этом случае, например слово «ПОБЕДА» перейдет в криптограмму:

73 32 98 13 19 11

Такой шифр называется шифром *цифровой простой замены*.

Еще один интересный пример шифра простой замены был описан в рассказе А. Конан Дойла «Пляшущие человечки», где каждый символ изображает пляшущего человечка в определенной позе.

Также, например, в романе Ж. Верна «Путешествие к центру Земли» в руки профессора Лиденброка попадает пергамент с рукописью из знаков рунического письма. Каждый рунический знак был заменен на соответствующую букву немецкого языка, что облегчило восстановление открытого сообщения.

3. ***Шифр Полибия.*** В Древней Греции (II в. до н.э.) был известен шифр, называемый «квадрат Полибия» (в нашем примере будет прямоугольник). Шифр Полибия является оригинальным шифром простой замены. Приведем пример этого шифра для русского языка. Буквы алфавита в **произвольном** порядке вписываются в прямоугольник 5x6 (заполнение квадрата и является *ключом*), например, так как показано на рисунке.

	1	2	3	4	5
1	К	Р	Б	Ю	Ы
2	Ф	Т	А	Щ	О
3	Д	Н	Я	И	Е
4	С	Ь	В	М	Ш
5	Э	Г	Л	Ц	П
6	Ж	У	Х	З	Ч

Тогда каждой букве алфавита однозначно соответствует пара чисел – номер строки и номер столбца в этой таблице. Процедура шифрования

текста представляла собой замену каждой буквы на пару чисел в соответствии с таблицей. Например, при шифровании слова «Греция» на данном ключе получим следующую криптограмму:

52 12 35 54 34 33

4. ***Сдвиговый шифр.*** Пусть X - сообщение, которое необходимо зашифровать, $X = x_1, \dots, x_T$, где T – длина сообщения, а буквы сообщения x_i, $i \in \{1, \dots, T\}$ выбираются из некоторого алфавита $\Omega = \{a_1, \dots, a_n\}$, n - мощность алфавита. Каждая буква отождествляется со своим порядковым номером в алфавите. Зашифрование сообщения X осуществляется побуквенно: сначала шифруется 1-ая буква x_1, затем 2-ая x_2 и т.д. до x_T. Преобразование зашифрования f i-ой буквы сообщения x_i в данном случае будет иметь вид:

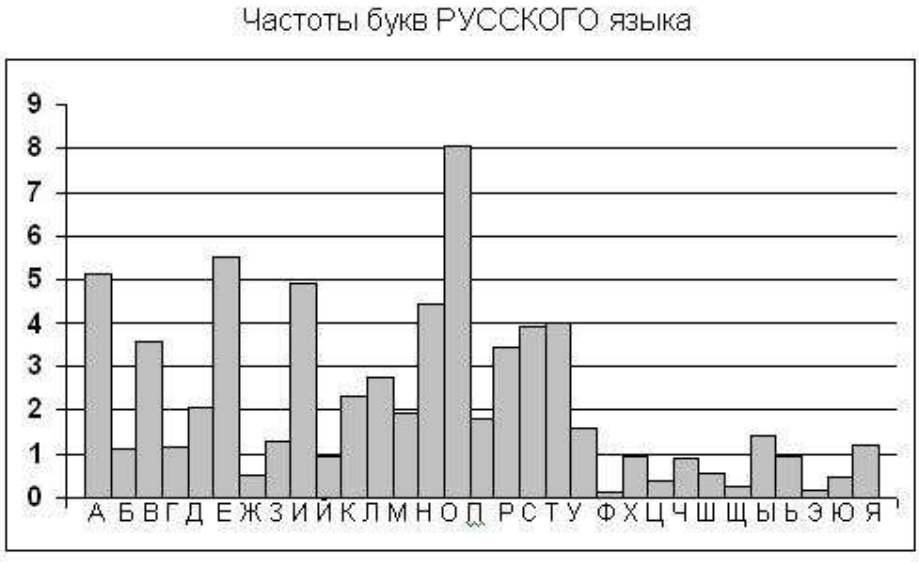
$$f_k(x_i) = r_n\,(x_i + k)\,,$$

где $r_n(b) -$ остаток от деления b на n, k – ключ шифра, некоторое целочисленное значение от 1 до n-1. Отметим одну особенность данного шифра: если остаток от деления $x_i + k$ на n равен нулю, то буква x_i заменяется на a_n, то есть считается, что в таком случае значение $f_k(x_i)$ равно n. Можно проверить, что уравнение расшифрования в данном случае будет следующим:

$$g_k\,(y_i) = r_n(y_i - k)\,.$$

Уязвимость шифров вида простой замены

Дело в том, что буквы любого открытого текста, написанного на любом языке, использующим алфавит, встречаются в тексте разное количество раз. Если взять произвольный открытый текст достаточно большой длины, написанный на русском языке и подсчитать в нем число букв *А*, затем *Б*, *В* и так до *Я*, то получиться примерно следующая картинка (см. рисунок).



Высота темного столбца каждой буквы говорит о процентном содержании в тексте этой буквы. Из этой таблицы (*гистограммы*) находим, что самой частой буквой в русском открытым тексте является буква *О*, а самыми редкими - *Ф*, *Щ*, *Э*.

Данное наблюдение позволяет предложить следующий подход к вскрытию шифра простой замены. Если в открытом сообщении часто встречается какая-либо буква, то в сообщении, зашифрованном с помощью такого шифра, часто будет встречаться соответствующий ей символ или буква. Поэтому, в случае шифра простой замены, целесообразно выделить из шифртекста самую частую букву (подсчитав предварительно частоты встречаемости всех букв в шифртексте) и найти сопоставление этой буквы букве языка (в соответствии с гистограммой частот, изображенной выше). И продолжить далее эту процедуру сопоставления частот букв шифртекста частотам букв языка (тем самым сопоставляя буквы шифртекста и буквы открытого текста) и таким образом, вскрыть данный шифр.

Отметим, что из-за специфики некоторых текстов или небольшой их длины самому частому символу шифртекста не обязательно соответствует самый частый символ языка, а возможно символ с меньшей частотой встречаемости.

§ 2. Решение задач

Задача № 1.

Известно зашифрованное сдвиговым шифром сообщение

РГЖС ЕФХУЗХЛХЯФВ

Также известны параметры этого шифра: $k = 3$, использовался русский 33-х буквенный алфавит. Расшифровать данное сообщение.

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:

Зададим числовое соответствие данному шифртексту (используя таблицу):

18 4 8 19 6 22 23 21 9 23 13 23 33 22 3

Поскольку $k = 3$, то согласно уравнению расшифрования нужно вычесть из каждого значения 3, а затем взять остаток от деления на 33:

15 1 5 16 3 19 20 18 6 20 10 20 30 19 0(33)

Отметим, что последнее числовое значение равно нулю, поэтому его (согласно сделанному ранее замечанию) мы должны заменить на значение 33. Далее осталось полученной числовой последовательности поставить в соответствие последовательность букв, согласно таблице и придем к следующему ответу.

Ответ: *НАДО ВСТРЕТИТЬСЯ.*

Задача № 2.

В какое из представленных слов может перейти слово:

B E N E F I T

при использовании сдвигового шифра в английском алфавите?

- WZIZADO;
- SVEWHZK;
- QTCTAXI;

- GJSJKN.

Решение:

- 4-ый вариант отвергается из-за того, что зашифрованное слово GJSJKN имеет меньшую, чем исходное слово длину;
- 3-ий вариант не подходит по причине того, что соседние буквы (идущие друг за другом в алфавитном порядке) должны переходить в соседние буквы при использовании такого типа шифрпреобразования, а в данном примере соседние буквы *E* и *F* переходят в *T* и *A*;
- 2-ый вариант - из-за того, что при использовании сдвигового шифра одинаковые буквы должны переходить в одинаковые символы, а в данном ответе SVEWHZK символы, стоящие на 2 и 4 местах - разные, тогда как в исходном слове BENEFIT - одинаковые.

Остается только один возможный вариант – первый.

Ответ: *в первое*.

Задача № 3.

Имеется криптограмма

HFPSHJB

Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x_1, x_2 - корни трехчлена $x^2 + 5x + 4$. К порядковому номеру каждой буквы в английском алфавите прибавлялось значение многочлена

$$f(x) = x^6 + 5x^5 + 4x^4 + x^3 + 6x^2 + 9x + 5$$

вычисленное либо при $x = x_1$, либо при $x = x_2$ (в неизвестном порядке), а затем полученное число заменялось соответствующей ему буквой.

Решение:

Для данного многочлена верно разложение:

$$f(x) = (x^2 + 5x + 4)(x^4 + x + 1) + 1.$$

Это легко проверить просто разделив «столбиком» $f(x)$ на $x^2 + 5x + 4$ с остатком.

Поэтому, и при $x = x_1$, и при $x = x_2$ значение $f(x) = 1$. Таким образом, данное преобразование осуществляет не что иное, как сдвиговый шифр с параметром k=1. Если теперь шифрованное сообщение представить в виде цифровом виде, получим

8 6 16 19 8 10 2

Отнимем от каждого значение 1, получим:

7 5 15 18 7 9 1,

приводим обратно к буквенному виду, получаем

Ответ: *GEORGIA.*

Задача № 4.

В таблице приведена переписка двух абонентов (Godzillы и Фунтика) в чате.

Дата/время	Отправитель	Сообщение
10:11 28.11.2010	Godzilla	**Привет. Как дела? Пришли пароль для почты.**
10:14 28.11.2010	Фунтик	**И усцрмс щюуьсэ ц Яспар-Дюрюмгщмт пс вцю пювючж. Дсмычз: Гщмтщпвжи.**
10:21 28.11.2010	Godzilla	**Когда доберешься до Питера, позвони.**

Фунтик отвечает Godzille и для конспирации каждую букву заменяет другой буквой (при этом разные буквы заменяются разными, а одинаковые – одинаковыми). Восстановите зашифрованное сообщение и пароль.

Решение:

Отметим, что восстановить исходный текст короткого сообщения, зашифрованного с использованием такого шифра не так-то просто. Помогает здесь то, что в сообщении сохранена разбивка на слова, оставлены знаки препинания и заглавные буквы. Если обратить внимание на сочетание **Яспар-Дюрюмгщмт** и содержащееся в ответе Godzillы упоминание города **Питера,** то можно предположить, что речь идёт о **Санкт-Петербурге**. Составим таблицу соответствий:

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
К			Б	П									Р			Н	Т	А	Г						У						Е	С

В соответствии с этими заменами некоторые буквы в шифрованном тексте можно восстановить:

. .А.ТРА УЕ..А. . САНКТ-ПЕТЕРБУРГ НА ..Е НЕ.Е.. . ПАР...: БУРГУН...

Далее подбираем некоторые слова по смыслу. Весьма вероятно, что **.А.ТРА** -- это **ЗАВТРА**, **ПАР...** - это **ПАРОЛЬ**. С учётом этих предположений сообщение примет вид:

. ЗАВТРА УЕЗ.А. В САНКТ-ПЕТЕРБУРГ НА .ВЕ НЕ.ЕЛ. . ПАРОЛЬ: БУРГУН... .

Затем по смыслу окончательно получаем искомое сообщение.

Ответ: *Я завтра уезжаю в Санкт-Петербург на две недели. Пароль: Бургундия.*

Задача № 5.

Рассмотрим преобразование цифрового текста (алфавит $\Omega = \{0,1,2,3,4,5,6,7,8,9\}$), в котором каждая цифра заменяется остатком от деления значения многочлена

$$F(x) = 3(x^3 + 7x^2 + 3x + 13)$$

на число 10. Может ли это преобразование использоваться в качестве шифрпреобразования (т.е. допускать однозначное расшифрование)?

Решение:

Для однозначного расшифрования необходимо и достаточно, чтобы разным значениям x соответствовали различные значения $f(x)$. Проверим это.

Обозначим через $f(x)$ - остаток от деления значения многочлена $F(x)$ на 10.

- $x = 0,\ F(0) = 3 \cdot 13;\ f(0) = 9$
- $x = 1,\ F(1) = 3(1 + 7 + 3 + 13) = 3 \cdot 24;\ f(1) = 2;$

- $x = 2,\ F(2) = 3(8 + 28 + 6 + 13) = 3 \cdot 55;\ f(2) = 5;$
- $x = 3,\ F(3) = 3(27 + 63 + 9 + 13) = 3 \cdot 112;\ f(3) = 6;$
- $x = 4,\ F(4) = 3(64 + 112 + 12 + 13) = 3 \cdot 201;\ f(4) = 3;$
- $x = 5,\ F(5) = 3(125 + 175 + 15 + 13) = 3 \cdot 20;\ f(5) = 4;$
- $x = 6,\ F(6) = 3(216 + 252 + 18 + 13) = 3 \cdot 201;\ f(6) = 7;$
- $x = 7,\ F(7) = 3(343 + 343 + 21 + 13) = 3 \cdot 720;\ f(7) = 0;$
- $x = 8,\ F(8) = 3(512 + 448 + 24 + 13) = 3 \cdot 997;\ f(8) = 1;$
- $x = 9,\ F(9) = 3(729 + 567 + 27 + 13) = 3 \cdot 1336;\ f(9) = 8.$

Получились все 10 различных значений, значит правильный

Ответ: *да*, *может*.

Задача № 6

Если слово СРОЧНО зашифровать простой заменой с помощью ключа:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
Ч	Я	Ю	Э	Ы	Ь	Щ	Ш	Ц	Х	Ф	У	Б	Д	Т	З	В	Р	П	М	Л	К	А	И	О	Ж	Е	С	Г	Н

то получится слово ВЗДАБД. Зашифровав полученное слово с помощью того же ключа еще раз, получим слово ЮШЫЧЯЫ. Сколько всего различных слов можно получить, если указанный процесс шифрования продолжать неограниченно?

Решение:

Несложно заметить, что рассматриваемый шифр обладает тем свойством, что при зашифровании разные буквы заменяются разными. Следовательно, при зашифровании разных слов получаются разные слова. С другой стороны, одинаковые буквы заменяются на одинаковые независимо от цикла шифрования, так как используется один и тот же ключ. Следовательно, при зашифровании одинаковых слов получаются одинаковые слова. Таким образом, число различных слов, которые можно получить в указанном процессе шифрования с начальным словом СРОЧНО, совпадает с наименьшим номером цикла шифрования, дающем это начальное слово.

Как определить номер такого цикла? Рассмотрим первую букву слова СРОЧНО – букву С. Исходя из ключа шифра (таблицы), составим цикл по которому данная буква будет «передвигаться» при последовательном применении шифрования. Обозначим его так: (СВЮГЭ) – данная запись означает, что буква С перейдет в В, В перейдет в Ю, Ю перейдет в Г и, наконец, Г – в Э, а далее мы опять возвращаемся в букву С. Длина такого цикла равна 5. Значит, если число последовательно примененных шифрований кратно 5, то первой буквой полученной криптограммы будет – С.

Найдем длины циклов, на которых «лежат» все остальные буквы данного слова.

- Цикл, на котором «лежит» буква С:

  (СВЮГЭ), длина 5.
- Цикл, на котором «лежит» буква Р:

  (РЗШИЦКХЛФМУПТ), длина 13.
- Цикл, на котором «лежит» буква О:

  (ОДЫЕЬЖЩ), длина 7.
- Цикл, на котором «лежит» буква Ч:

  (ЧА), длина 2.
- Цикл, на котором «лежит» буква Н:

  (НБЯ), длина 3.

Теперь, легко видеть, что первое повторение слова СРОЧНО произойдет тогда, когда все перечисленные буквы снова повторятся одновременно. А это произойдет тогда, когда число последовательно примененных шифрований кратно длинам всех перечисленных циклов, но мы ищем наименьшее число с таким свойством, поэтому ответ – НОК{5, 13, 7, 2, 3} = 2730.

Ответ: *2730*.

Задача № 7

Зашифрование сообщения состоит в простой замене букв на пары цифр. Криптографу дали задание восстановить зашифрованный текст. В каком случае ему будет легче выполнить задание: если известно, что первое слово второй строки - "термометр" или что первое слово третьей строки - "ремонт"? Обоснуйте свой ответ. (Предполагается, что таблица зашифрования криптографу неизвестна).

Решение:

Во втором случае известны пары цифр, которыми шифруются буквы "р", "е", "м", "о", "н", "т", а в первом - пары цифр для тех же букв, за исключением буквы "н".

Таким образом, зная второе слово, криптограф обладает большим знанием о соответствии букв парам цифр, а следовательно в этом случае ему проще *дешифровать* криптограмму (отметим, что в данной задаче перед криптографом стоит задача именно дешифрования, а не расшифрования, поскольку ключа шифра, которым в случае простой замены является таблица, ему не известно).

Ответ: *во втором случае*.

Задача № 8

Перед шифрованием буквы некоторого текста отождествлялись с числовыми значениями согласно табл. 1.

Таблица 1

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	Ь	Ы	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

Затем к числовым значениям было прибавлено некоторое число от 1 до 30 и от полученных значений взят остаток от деления на 30. Полученные

числовые остатки переводились обратно к буквенному виду, используя таблицу 1. Получилось:

ЦЭСЯСИУДХГОЧШОНЩЫИЛСЫОУСЩОЛОШХЦСТЦШОС.

Прочитайте исходный текст.

Решение:

Прочитав внимательно условие задачи легко понять, что в ней идет речь о сдвиговом шифре. Постановка задачи заключается во вскрытии данного шифра. Отличительной особенностью сдвигового шифра среди шифров простой замены является возможность его вскрытия путем полного перебора ключей, число который равно в точности мощности алфавита (что сравнительно не так много), поскольку число ключей – это в точности число возможных вариантов сдвига, то есть возможных значений параметра *k*. Но в тоже время для его вскрытия достаточно установить какое-либо соответствие между буквой шифртекста и буквой открытого текста. Поскольку тогда легко вычислить ключ данного шифра – *k* – параметр сдвига, он будет равен

$$k = \text{БШТ} - \text{БОТ},$$

где БШТ – буква шифрованного текста, а БОТ – буква открытого текста.

В нашем случае попробуем установить какая из букв представленного шифртекста соответствует наиболее часто встречающейся в русском языке букве О (см. гистограмму частот, представленную ранее). Для этого подсчитаем частоты встречаемости букв в шифртексте (см. таблицу).

С	О	Ц	Ш	Щ	И	Л	У	Ы	…
6	6	3	3	2	2	2	2	2	…

1. Предположим, что буква О переходит при зашифровании в букву С, тогда ключ *k* = С – О = 17-14 = 3. Попробуем расшифровать данный шифртекст на таком ключе. Получим следующее начало открытого текста: УЩОЫ… Очевидно, что ничего осмысленного нет, значит О не переходит в С и *k* не равен 3.

2. Смотрим на следующую наиболее частую букву шифртекста. Это буква О. Но очевидно, что О не могла перейти в саму себя, поскольку иначе параметр сдвига k = 0, а такого быть не может (иначе текст остается нешифрованым).
3. Следующая по встречаемости буква Ц. Если О переходит в Ц, то k = Ц – О = 22-14 = 8. Попробуем расшифровать текст на данном ключе. Получим начало: ОФИЦИА… Как видим текст получается читаемым, остается расшифровать оставшуюся часть шифртекста и убедиться, что k = 8 действительно ключ рассматриваемого шифра.

Ответ: *Официальные представители Северной Кореи.*