Самый простой моноалфавитный шифр — аддитивный шифр, его иногда называют **шифром сдвига**, а иногда — **шифром Цезаря**, но термин аддитивный шифр лучше показывает его математический смысл.
Шифр **Цезаря** — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. Естественным развитием шифра Цезаря стал шифр Виженера. С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости.

Юлий Цезарь использовал аддитивный шифр, чтобы связаться со своими чиновниками. По этой причине аддитивные шифры упоминаются иногда как шифры Цезаря. Цезарь для своей связи использовал цифру 3.

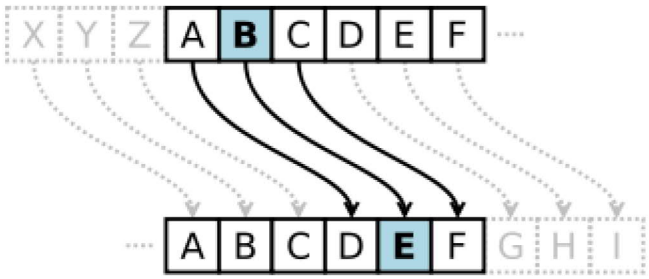

Рис. 1. Шифр Цезаря

Шифр сдвига

Исторически аддитивные шифры назывались **шифрами сдвига** — по той причине, что алгоритм шифрования может интерпретироваться как "клавиша сдвига буквы вниз", а алгоритм дешифрования может интерпретироваться как "клавиши сдвига буквы вверх". Например, если ключ = 15, алгоритм кодирования сдвигает букву на 15 букв вниз (к концу алфавита). Алгоритм дешифрования сдвигает букву на 15 букв вверх (к началу алфавита). Конечно, когда мы достигаем конца или начала алфавита, мы двигаемся по кольцу к началу (объявленные свойства операции по модулю n).

Предположим, что исходный текст состоит из маленьких букв (от a до z) и зашифрованный текст состоит из заглавных букв (от A до Z). Чтобы обеспечить применение математических операций к исходному и зашифрованному текстам, мы присвоим каждой букве числовое значение (для нижнего и верхнего регистра), как это показано на рис. 2.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Числовое значение
Зашифрованный текст
Исходный текст

Рис. 2. Представление букв исходного текста и зашифрованного текста в Z_{26}

На рисунке 2 каждому символу (нижний регистр или верхний регистр) сопоставлено целое число из Z26. Ключ засекречивания — также целое число в Zn. Алгоритм кодирования прибавляет ключ к символу исходного текста; алгоритм дешифрования вычитает ключ из символа зашифрованного текста. Все операции проводятся в Zn. Рисунок 3 показывает процесс шифрования и дешифрования

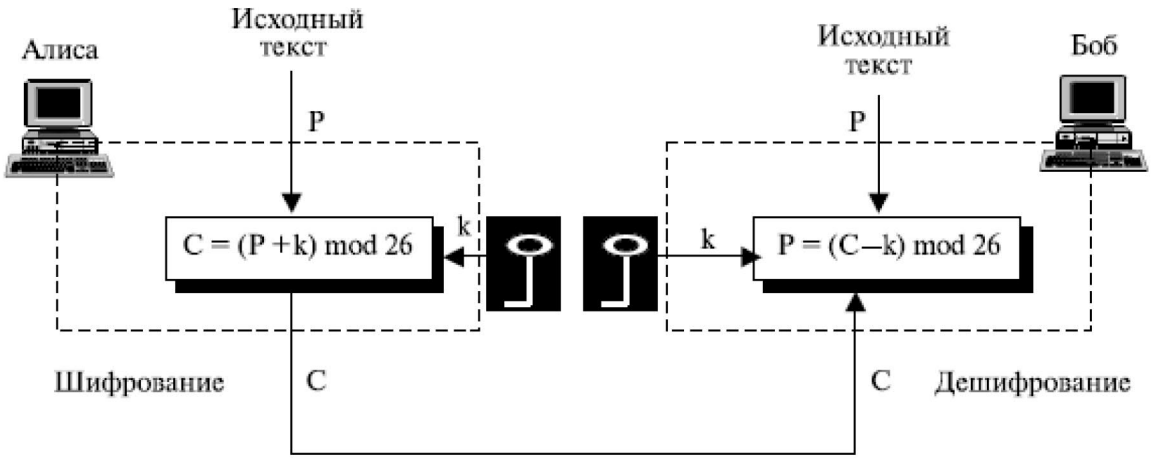

Рис. 3 Аддитивный шифр

Математическая модель

Мы можем легко показать, что шифрование и дешифрование являются инверсными друг другу.

$$P1 = (C - k) \bmod n = (P + k - k) \bmod n = P$$

Когда применяется аддитивный шифр, исходный текст, зашифрованный текст и ключ — целые числа в Z_n.

Иначе говоря, если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

$$y = x + k \ (mod\ n)$$
$$x = y - k \ (mod\ n),$$

где x — символ открытого текста y — символ шифрованного текста n — мощность алфавита (кол-во символов) k — ключ. Можно заметить, что суперпозиция двух шифрований на ключах k1 и k2 — есть просто шифрование на ключе k1+k2. Более общее, множество шифрующих преобразований шифра Цезаря образует группу Z.

Алфавит:

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

Пример:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Ответ: «Пхнфчузхещнд»

Пример шифрования

Используйте аддитивный шифр с ключом = 15, чтобы зашифровать сообщение "hello".

Решение

Мы применяем алгоритм кодирования к исходному тексту, буква за буквой:

Исходный текст h -> 07 Шифрование (07 + 15) mod 26 Шифр. Текст 22 -> W

Исходный текст e -> 04 Шифрование (04+ 15) mod 26 Шифр. Текст 19 -> T

Исходный текст l -> 11 Шифрование (11 + 15) mod 26 Шифр. Текст 00 -> A

Исходный текст l -> 11 Шифрование (11 + 15) mod 26 Шифр. Текст 00 -> A

Исходный текст o -> 14 Шифрование (14 + 15) mod 26 Шифр. Текст 03 -> D

Результат — "WTAAD". Обратите внимание, что шифр моноалфавитный, потому что два отображения одной и той же буквы исходного текста (символ *l*) зашифрованы как один и тот же символ (*A*).

Пример дешифрования

Используйте шифр сложения с ключом = 15, чтобы расшифровать сообщение "WTAAD".

Решение

Мы применяем алгоритм дешифрования к исходному тексту буква за буквой:

Шифр. Текст W -> 22 Шифрование (22 - 15) mod 26 Исходный текст 07 -> h

Шифр. Текст T -> 19 Шифрование (19 - 15) mod 26 Исходный текст 04 -> e

Шифр. Текст A -> 00 Шифрование (00 - 15) mod 26 Исходный текст 11 -> l

Шифр. Текст A -> 00 Шифрование (00 - 15) mod 26 Исходный текст 11 -> l

Шифр. Текст D -> 03 Шифрование (03 - 15) mod 26 Исходный текст 14 -> 0

Результат — "hello". Обратите внимание, что операции проводятся по модулю 26 (используется английский алфавит, количество символов 26, нумерация идет с 0), отрицательный результат должен быть отображен в Z_{26} (например, –15 становится 11).

Криптоанализ

Аддитивные шифры уязвимы к атакам только зашифрованного текста, когда используется исчерпывающий перебор ключей (**атака грубой силы**). Множество ключей аддитивного шифра очень мало — их только n (где n – кол-во символов алфавита; мощность алфавита). Один из ключей, нулевой, является бесполезным (зашифрованный текст будет просто соответствовать исходному тексту). Следовательно, остается только n-1 возможных ключей. Ева может легко начать атаку грубой силы зашифрованного текста.

Пример атаки грубой силы

Пользователь перехватила зашифрованный текст "UVACLYFZLJBYL". Покажите, как он может взломать шифр, используя атаку грубой силы.

Решение

Пользователь пробует раскрыть текст и последовательно перебирает ключи начиная с первого. С помощью ключа номер 7 она получает осмысленный текст "not very secure" (не очень безопасный).

Зашифрованный текст: UVACLYFZLJBYL

K = 1 *Исходный текст: tubkxeykiaxk*

K = 2 *Исходный текст: styajwdxjhzwj*

K = 3 *Исходный текст: rsxzivewigyvi*

K = 4 *Исходный текст: qrwyhubvhfhuh*

K = 5 *Исходный текст: pqvxgtaugewtg*

K = 6 *Исходный текст: opuwfsztfdvst*

K = 7 *Исходный текст: notverysecure*

Аддитивные шифры также могут быть объектами **статистических атак**. Это особенно реально, если противник перехватил длинный зашифрованный текст. Противник может воспользоваться знаниями о частоте употребления символов в конкретном языке. Таблица 1 показывает частоту появления определенных букв для английского текста длиной в 100 символов.

Таблица 1. Частота появления букв в английском тексте							
Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
E	12,7	**H**	6,1	**W**	2,3	**K**	0,08
T	9,1	**R**	6,0	**F**	2,2	**J**	0,02
A	8,2	**D**	4,3	**G**	2,0	**Q**	0,01
O	7,5	**L**	4,0	**Y**	1,9	**X**	0,01
I	7,0	**C**	2,8	**P**	1,5	**Z**	0,01
N	6,7	**U**	2,8	**B**	1,0		
S	6,3	**M**	2,4	**V**			

Таблица 2. Частота появления букв русском тексте

Буква	*Частота*	*Буква*	*Частота*
пробел	0,175	**я**	0,018
о	0,090	**ы**	0,016
е, ё	0,072	**з**	0,016
а	0,062	**ь, ъ**	0,014
и	0,062	**б**	0,014
т	0,053	**г**	0,013
н	0,053	**ч**	0,012
с	0,045	**й**	0,010
р	0,040	**х**	0,009
в	0,038	**ж**	0,007
л	0,035	**ю**	0,006
к	0,028	**ш**	0,006
м	0,026	**ц**	0,004
д	0,025	**щ**	0,003
п	0,023	**э**	0,002
у	0,021	**ф**	0,002

Однако информации о частоте единственного символа недостаточно, и это затрудняет анализ шифрованного текста, основанный на анализе частоты появления букв. Весьма желательно знать частоту появления комбинаций символов. Мы должны знать частоту появления в зашифрованном тексте комбинаций с двумя или с тремя символами и сравнивать ее с частотой в языке, на котором написан исходный документ.

Наиболее употребляемые группы с двумя символами (диаграмма (diagrams)) и группы с тремя символами (триграмма (trigrams)) для английского текста показаны в таблице 3.

Таблица 3. Группы диаграмм и триграмм, основанные на их частоте появления в английском языке	
Диаграмма	TH,HE,IN,ER,AN,RE,ED,ON,ES,ST,EN,AT,TO,NT,HA,ND,OU,EA,NG,AS,OR, TI,IS,ET,IT,AR,TE,SE,HI,OF
Триграмма	THE,ING,AND,HER,ERE,ENT,THA,NTH,WAS,ETH,FOR,DTH

Пример статистической атаки

Ева перехватила следующий зашифрованный текст. Используя статистическую атаку, найдите исходный текст.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Решение. Когда злоумышленник составит таблицу частоты букв в этом зашифрованном тексте, он получит: I = 14, V = 13, S = 12, и так далее. Самый частый символ – «I» — имеет 14 появлений. Это показывает, что символ «I» в зашифрованном тексте, вероятно, соответствует символу «e» в исходном тексте. Тем самым, ключ = 4. Расшифровывая текст получаем:

«the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers»
«дом теперь продается за четыре миллиона долларов, стоит поспешить, пока продавец не получил больше предложений»

Пример реализации шифра Цезаря на языке С (шифрование, английский алфавит, строчные буквы)

```
#include <stdio.h>
int main()
{
char string4[80];
int rotatorN;
printf("Enter String: ");
gets(string4);
printf("Enter Number: ");
scanf("%i", &rotatorN);
int n = 0, rotateSwap = 0;
int i;
for(i=0; string4[i] != '\0'; i++)
{if(string4[i] >='a' && string4[i] <='z')
{n = 'z' - string4[i];
if( rotatorN > n )
{rotateSwap = rotatorN - n - 1;
string4[i] = 'a';
string4[i] += rotateSwap;}
else
string4[i] += rotatorN;}}
int j;
for(j = 0; string4[j] !='\0'; j++)
{printf("%c", string4[j]);}
printf("\n");
return 0;
}
```

Задание на практическую работу

1) Зашифровать открытый текст:
«Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message»
Ключ k = 17.

2) Дешифровать шифротекст:

Вариант 1.
«Yzkmgtumxgvne otirajky znk iutikgrsktz ul otluxsgzout coznot iusvazkx lorky»
Ключ k = 6.
Вариант 2.
«Aol johunl pz zv zbiasl aoha zvtlvul dov pz uva zwljpmpjhssf svvrpun mvy pa pz busprlsf av uvapjl aol johunl»
Ключ k = 7.
Вариант 3.
«Cqn orabc anlxamnm dbn xo cqn cnav fjb rw (1499) kh Sxqjwwnb Carcqnvrdb rw qrb Bcnpjwxpajyqrj»
Ключ k = 9. Число незашифрованное.
Вариант 4.
«Yqeemsqe iduffqz uz Yadeq oapq az kmdz mzp ftqz wzuffqp uzfa m buqoq ar oxaftuzs iadz nk m oagduqd»
Ключ k = 12.

3) Провести статистическую атаку на шифротекст. Предоставить подробное описание

Вариант 1.
«Пэпыютшжэкь юрапчюь юяафуфыофвбо жпбвювэюбвл уыо ргъс».
Вариант 2.
«Сжтдвб йвскую ог кусонюйодвпкк уфжевпоетвцкк дуфтжщвжфуб д фтвмфвфж Ежтрёрфв «Куфрткб»».
Вариант 3.
«Йлсэйкълцк кшгяэ пэиёбдш й нбебпэйгб ёэйкшщбдфёуе збыеэёкже».
Вариант 4.
«И фжшщхёалл ичлуё цхк шщлйжфхйчжыплр южал ишлйх цхфпужещ шсчвщпл пфыхчужэпп и щлсшщхивь йчжыпюлшспь тпзх жъкпхыжртжь».

4) Подробно описать процесс шифрования и дешифрования сообщения «(Имя_Фамилия_Отчество) лучший криптоаналитик планеты Земля».

*5) Дописать процесс дешифрования в программе на языке С, представленной выше. Разрешается ПОЛНОСТЬЮ переписать программу. В отчете предоставить листинг и скриншоты работы программы.
* - дополнительное задание. (!)Не обязательно, но рекомендуемо(!)