Исторические шифры

До появления компьютеров криптография состояла из алгоритмов на символьной основе. Различные криптографические алгоритмы либо заменяли одни символы другими, либо переставляли символы. Лучшие алгоритмы делали и то и другое много раз. В настоящее время алгоритмы стали работать с битами, а не с символами, поэтому размер алфавита сократился до двух элементов. При этом, многие криптографические алгоритмы до сих пор комбинирует подстановки и перестановки:

1) шифры замены (подстановки) заменяют один символ открытого текста на другой символ в зашифрованном тексте.

2) шифры перестановки меняют местами позиции символов открытого текста.

Будем использовать следующие обозначения.

K – множество ключей. Каждый ключ $k \in K$ определяет некоторую преобразование E (*encryption*) на множестве открытых текстов PT (*plaintext*) и обратное преобразование D (*deciphering*) на множестве зашифрованных сообщений CT (*ciphertext*).

$E(k, p)$ – шифртекст открытого текста p, полученный в результате использования функции шифрования E с заданным ключом k;

$D(k, c)$ – открытый текст, соответствующий шифртексту c, полученный в результате использования функции расшифрования D с заданным ключом k.

Рассмотрим применение замены и перестановки символов в криптографических алгоритмах на примере некоторых исторических шифров.

***Шифр Цезаря* (*шифр сдвига, шифр простой замены*)**. В I веке н. э. Юлий Цезарь во время войны с галлами, в переписке с Римом, заменял в сообщении первую букву латинского алфавита A на четвертую D , вторую B – на пятую E , и т.д. последнюю – на третью в соответствии со следующей таблицей

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
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

т.е. каждая буква латинского алфавита сдвигается циклически вправо на $k = 3$ позиций.

Например, донесение Ю. Цезаря Сенату об одержанной им победе над Понтийским царем выглядело так:

YHQL YLGL YLFL

("Veni, vidi, vici" – лат. "Пришел, увидел, победил").

Понятно, что выбор ключа $k = 3$ не является единственно возможным. При других ключах k имеем $E($25, IBM) = HAL, E(6, IBM) = OHS.

Нетрудно показать, что функция расшифрования $D(k, c) = E(26 – k, c)$. Исключая слабый ключ $k = 0$, множество ключей имеет мощность $|K| = 25$.

Тарабарская грамота. Первое известное применение тайнописи в России относится к XIII в. Эту систему называли «тарабарской грамотой». В этой системе согласные буквы заменяются по схеме:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Например, ШЧУ – шифр слова ВГУ.

Еще один пример шифра простой замены – ***модулярный (аффинный) шифр***. Выберем число a, взаимно простое с модулем $m = 26$. Пусть p – буква английского алфавита, отождествленная со своим порядковым номером (0, 1, ... , 25). Тогда $E((a,k), p) = ap + k (\mathrm{mod}\ m)$, где k – фиксировано. В этом случае ключом является пара чисел (a, k). Условие взаимной простоты необходимо для обратимости шифра.

Криптосхема, принадлежащая ***Л. Хиллу***, основана на линейной алгебре. При шифровании заменяются пары букв (биграммная криптосхема). Осуществим цифровую кодировку букв английского алфавита: A = 0, B = 1, C = 2, ... , Z = 25. Выберем какую-нибудь обратимую по модулю 26 квадратную матрицу M порядка 2. Это – ключ. Пусть, например,

$$M = \begin{pmatrix} 2 & 5 \\ 3 & 3 \end{pmatrix}, M^{-1} = \begin{pmatrix} 17 & 15 \\ 9 & 20 \end{pmatrix}.$$

Биграммы будем записывать в виде матриц-столбцов. Например,

$$p_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, p_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

Шифрование биграмм определим формулой $c = Mp$. Зашифруем, для примера, слово p = HELP = p_1p_2, тогда c = IHTA.

Шифр Виженера. Ключ образуется последовательностью букв $k_1k_2 \ldots k_d$ (слово-лозунг), при этом для i-ой буквы сообщения a функция шифрования $f_i(a) = (a + k_i) (\mathrm{mod}\ m)$. Для реализации этой формулы можно воспользоваться следующей таблицей, которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов и равно числу букв в алфавите.

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**
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	а
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	а	б
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	а	б	в
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	а	б	в	г
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	а	б	в	г	д
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	а	б	в	г	д	е
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	а	б	в	г	д	е	ё
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	а	б	в	г	д	е	ё	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ъ	ы	ь	э	ю	я	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
щ	ъ	ы	ь	э	ю	я	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
ъ	ы	ь	э	ю	я	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	э	ю	я	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	э	ю	я	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
э	ю	я	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
ю	я	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
я	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

Чтобы зашифровать сообщение, слово-лозунг подписывается с повторением над буквами сообщения. Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого, в вертикальном алфавите, а соответствующий ему знак сообщения в горизонтальном. На пересечении выделенных столбца и строки находим зашифрованную букву.

Например, зашифруем фразу «криптографические методы» с помощью слова-лозунга «вгу»:

в	г	у	в	г	у	в	г	у	в	г	у	в	г	у	в	г	у	в	г	у	в	г
к	р	и	п	т	о	г	р	а	ф	и	ч	е	с	к	и	е	м	е	т	о	д	ы
м	у	ь	с	х	в	е	у	у	ц	л	к	ж	ф	ю	к	з	а	ж	х	в	ё	ю

Наряду с подстановочными шифрами известны так называемые перестановочные (транспозиционные) шифры. При этом буквы сообщения остаются прежними, но меняют свое расположение в тексте.

Постолбцовая транспозиция **(XIX век).** К классу «перестановка» относится шифр «постолбцовая транспозиция». В данный прямоугольник [$m \times n$] вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Например, зашифруем фразу «Без труда не выловишь рыбку из пруда».

Решение. Фраза содержит 30 символов с учетом тире. Ее можно записать в прямоугольники размером 2×15, 3×10, 5×6 и т. д. Выберем прямоугольник 5×6.

б	е	з	т	р	у
д	а	н	е	в	ы
л	о	в	и	ш	ь
р	ы	б	к	у	и
з	п	р	у	д	а

Выписываем шифрованное сообщение по столбцам:

бдлрз еаоып знвбр теику рвшуд уыьиа.

Лабораторная работа 1

Цель работы: изучить алгоритмы, используемые в классических криптосистемах.

Задания. 1. Расшифровать криптограмму Цезаря (неалфавитные символы (пробелы, знаки препинания, цифры) – не преобразуются.).

2. Расшифровать криптограмму Виженера, если для шифрования было использовано слово-лозунг «шифр».

3. Реализовать схему шифрования посредством постолбцового варианта маршрутной транспозиции.

Входные параметры: сообщение, ключ (количество строк и столбцов в прямоугольнике, используемом для шифрования).

Выходные параметры: шифртекст.

4. Реализовать схему расшифрования посредством постолбцового варианта маршрутной транспозиции.

Входные параметры: шифртекст, ключ (количество строк и столбцов в прямоугольнике, используемом для шифрования).

Выходные параметры: открытый текст.

Вариант 1

1. Нгн ргцнг нултхсёугчлв ескрлног тсфоз чцржгпзрхгоярюш угдсх гпзулнгрфнсёс пгхзпгхлнг л аознхусхзшрлнг Носжг Ызррсрг (1916–2001).

2. Ачаякч шящдцрцы эш анбьб, и ьюшцэп – бр яюблэ.

Вариант 2

1. Е угдсхгш Носжг Ызррсрг «Пгхзпгхлъзфнгв хзсулв февкл» л «Хзсулв февкл е фзнузхрюш флфхзпгш» (1949) фсжзуйлхфв сдсдьзрлз дсояысёс стюхг фскжгрлв ылчусе, ргнстозррсёс жс рзёс, л угкугдгхюегзхфв тсорсщзррюм пгхзпгхлъзфнлм гттгугх жов нултхсёугчлъзфнлш кгжгъ.

2. Есе яйкщйшнжвч ъгьёящэ, ш ащьжкщы — ацфюбнб.

Вариант 3

1. Грголклуцв угрзз фцьзфхесегеылз ылчую, Носж Ызррср тулыио н еюесжц, ъхс дсояылрфхес лк рлш (жгйз фгпюз фосйрюз ылчую) фнсрфхуцлусегрю лк тусфхюш хлтлърюш нсптсрзрх, сфцьзфхеовбьлш кгпзрц л тзузфхгрсенц.

2. Ъъуыжн дядьыюшцрх ныых ъъуыжлг юэрврёеу.

Вариант 4

1. Дсозз ёоцдснсз тсрлпгрлз хсёс, нгн жсойрю фхуслхяфв ргжийрюз ылчую, тулезос Ызррсрг н еюжзозрлб жецш сдьлш тулрщлтсе тсфхусзрлв нултхсёугчлъзфнлш тузсдугксегрлм: тзузпзылегрлз л угффзлегрлз.

2. Еьшбух вщгыг юэ щгфбфёп, ш цфдпсавч.

Вариант 5

1. Тзузпзылегрлз скргъгзх цфосйрзрлз ефзескпсйрюш февкзм пзйжц длхгпл схнуюхсёс л ылчусегррсёс хзнфхсе. Угффзлегрлз тсжугкцпзегзх угфтусфхугрзрлз еолврлв сжрсёс длхг схнуюхсёс хзнфхг рг дсояысз ълфос длхсе ылчусегррсёс хзнфхг.

2. Ымщ вбфф юэ хгчэы, жре ьб ажхгчэы.

Вариант 6

1. Носж Ызррср етзуеюз пгхзпгхлъзфнл фхусёс фчсупцолусего естусфю с хзсузхлъзфнсм фхсмнсфхл ылчусе. Г лпзррс, ргфнсоянс цфхсмълесм веовзхфв ылчуфлфхзпг жов косцпюыозррлнг, сдогжгбьзёс рзсёугрлъзррюпл узфцуфгпл (еузпзрзп, тгпвхяб л х. ж.)?

2. Лхщюфн э гиьш тйн дхинжблы.

Вариант 7

1. Г фцьзфхецбх ол ылчуфлфхзпю, е нсхсуюш косцпюыозррлн рз тсоцълх рлнгнсм лрчсупгщлл, фнсоянс дю ср рл тзузшегхюего ылчухзнфх? Схезх снгкгофв тсосйлхзоярюп. Ылчуфлфхзпю, сдогжгбълз хгнлп фесмфхесп, ргкюегбхфв фсезуызррс фзнузхрюпл.

2. Ён чяъчещ, пыг фэффь, ш лгтжщэ, зкч ёфэффь.

Вариант 8

1. Флппзхулъргв ылчуфлфхзпг — флфхзпг ылчусегрлв, е нсхсусм нобъл кгылчусегрлв л угфылчусегрлв фсетгжгбх, олдс озёнс стузжзовбхфв сжлр тс жуцёспц. Тзузж лфтсояксегрлзп флппзхулърсм ылчуфлфхзпю гдсрзрхгп рзсдшсжлпс кгугрзз жсёсегулегхяфв с зжлрсп фзнузхрсп нобъз.

2. Анбьц уерйсж вжфвжэ, и лхдчцхги жблм.

Вариант 9

1. Гфлппзхулъргв ылчуфлфхзпг — флфхзпг ылчусегрлв, е нсхсусм лфтсоякцбхфв нобъл жецш елжсе — схнуюхюз нобъл л фзнузхрюз нобъл. Схнуюхюм нобъ тулпзрвзхфв е тусщзффз кгылчусегрлв л, нгн тугелос, веовзхфв сдьзжсфхцтрюп.

2. Ацфюфн вх ъчшщои - ц бжы ёреч вх йыфюэы ащкеёп.

Вариант 10

1. Нултхсёугчлъзфнгв фхсмнсфхя гфлппзхулърсм флфхзпю стузжзовзхфв хуцжсзпнсфхяб, ф нсхсусм косцпюыозррлн псйзх еюълфолхя фзнузхрюм нобъ лфшсжв лк кргрлв схнуюхсёс нобъг л жуцёсм жстсорлхзоярсм лрчсупгщлл с ылчуфлфхзпз. Сфрсерюп тузлпцьзфхесп гфлппзхулърсм ылчуфлфхзпю веовзхфв хс, ъхс гдсрзрхгп рз рцйрс кгугрзз жсёсегулегхяфв сд сдьзп фзнузхрсп нобъз.

2. Лаъсш с жблм я ажйщфшх цхььж.