Лабораторная работа № 3 «Криптосистемы»

1. Необходимые теоретические сведения

Рассмотрим основные исторические криптосистемы защиты информации от несанкционированного доступа.

Шифр Цезаря

В I веке н.э. Юлий Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) - на пятую (E), наконец, 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

В русском варианте эта таблица выглядит так:

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
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

Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Ы	Ь	Э	Ю	Я	А	Б	В

Шифр Цезаря входит в класс шифров, называемых «подстановка» или «простая замена». Это такой шифр, в котором каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь их комбинация. Сообщение об одержанной победе выглядело так.

Пример 1.1. YNQL YLGL YLFL (ЛАТ.)
 ТУЛЬИО ЦЕЛЖЗО ТСДЗЖЛО (РУС.)
 Пришел, увидел, победил.
(Ю. Цезарь. Донесение Сенату о победе над понтийским царем).

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

При шифровании буквы, расположенные на одной вертикали, переходят одна в другую. Остальные буквы остаются без изменения.

Пример 1.2. Так выглядит известная пословица, записанная «тарабарской грамотой»:

МЫЩАЛ ЧОСОШЫ ЧПИЁК

Рыба с головы гниет.

Таблица Виженера (1576г.)

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

В процессе шифрования (и дешифрования) часто используется так называемая «таблица Виженера», которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число сторон которой равно числу столбцов и равно числу букв в алфавите.

Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово-лозунг и подписывается с повторением над буквами сообщения.

Чтобы получить зашифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном.

На пересечении выделенных столбца и строки находим зашифрованную букву.

Пример 1.3. Зашифруем фразу «торопись медленно» с помощью слова-лозунга «море».

м	о	р	е	м	о	р	е	м	о	р	е	м	о	р	е
т	о	р	о	п	и	с	ь	м	е	д	л	е	н	н	о
я	э	б	у	ь	ч	в	б	щ	у	ф	р	с	ь	ю	у

Постолбцовая транспозиция (XIX век)

К классу «перестановка» относится шифр «маршрутная транспозиция» и его вариант «постолбцовая транспозиция». В данный прямоугольник $[n \times m]$ вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Пример 1.4. Зашифруем фразу: «Каждая собака – хозяин у своей двери».

Решение. Фраза содержит 30 символов с учетом пробела. Ее можно записать в прямоугольнички размером 2×30 ; 3×10 ; 5×6 и т.д. Выберем прямоугольнички размером 5×6 .

1	2	3	4	5	6
---	---	---	---	---	---

к	а	ж	д	а	я
с	о	б	а	к	а
-	х	о	з	я	и
н	у	с	в	о	е
й	д	в	е	р	и

Выписываем шифрованное сообщение по столбцам:
кс-нй аохуд жбосв дазве акяор яаиеи.

Индивидуальные задания к ЛР № 1 “Криптосистемы”

1. Расшифровать криптограмму Цезаря (русский алфавит без ё и ъ)
2. Перевести текст с тарабарской грамоты
3. Расшифровать постолбцовый вариант маршрутной транспозиции
4. Используя таблицу Виженера зашифруйте фразу «А» с помощью ключевого слова «В».
5. Взломайте шифр Виженера (общее для всех)

БЮОУ ЖЬЪЫГ ЦГТЧГЖГФ ДБФЦЗЯХТГВЮБ У ТХВШКНЫМЬ, РУАЧСТ
АБТЭЭМЧС ЪЕЪЪФЪЭЦ СЪЧРШ ТЪРЬШЦКВЮЗС АЪНЖГЪЕЖГФКБ Ф
ЪХЪЕЧМШ ИУЧКМЦЩНЪЭ: ВСЭСЬЦН ЮМЙ АСХЧМШ
ГВЦУЕТЧДУГ, Х ЩЕЩ ОЧГБЗС УЬЦДБФТЭЭМГЗВЛ
ЦЪМИГВЦРГЮЩУ. СЦЗН ХХШЧНМЦЛ Ч УЕБЦГЕВЦЛЬ,
ЦЕЖСКЮЭЖЭД ГСРЬВЦАК ЦКЦЯЭЧХГЦУЧ. ИГБНУВЯЭАЮ ФРЭ
ЦШЕЮЬЦРЬ ЧГЪИПГ ЯЦБЦБТЬГЭД, СЦАЩ ФГХДШЗЩЮБ ЮМЙ ЦПУ
ЮЬЦГЭ... М ЧЯЮ ВСШКЯ ЩЕ ХЯХВЯХ ЪСЫЕК ФМ ЮЬЦХ ФРЭ ЪЧХ
ЦХХЬЦК ГЛИГВЮКВ. РРВЗК ВЦНЖЖЬЙЭГСРСЮБ ГГЩУЖРЮЦФ Ц
ДЯРЭИИФЗХЮФГ ЮМЙ ЩБ ВЦРУЖГМЧЯЯШ, С НБЦКЮЭЦ ИАСУТГЦ
ШЧЦГБЬ – ВЦЫХЭРУТЬЮЩУ... Э ОУГТЕК БММАЩГТГ БЧВЯДКВЦС
АПРКЮ Ц ЖУЬНБ ОТЬИЩНБ ЦКЦЯЭЧХГЦЕБ: УЩЮБИГ ЮДШЯЮНЗ
БЙВЯ, ЩБЯИГФЬ ЩБЯИГЦ...

БЮТГЬСИ ЦЧГ БУМЦЮ, ИЮУЦМ КШЯ ФГУСЙЬЮФК У УЦКСЦЗУС
ЦМЧУ АЪНФГЩУ ЯЦХИЧМГОЩШ, ХЬРЫЦЦ ИИФЧРУМЧС ФЬ
ЖМХХЬЮКЕ Ф ВБМЗР О ЖУЬНК ДШЗЫМЬ.

ЩЕЩЯ ШМЩЮАЧСЮБ Ц ЦГВЮЕЧ БХЭВЯЧЖГОШУКФЬ: ЮУ, ГЧГ
ОАЪЯОКЗ Я ЧМДШМЩОЕЪЭИГ ЭСЬЖ З ЯНЮБВЮЗЬ РХИШСО Ц
ЦЧЦЬЦЮФПГУ, ЦДРКЗ ЦКДБФДЗЮБ ИВЧАНСЮБ У
ФЕЩЭШЗВЮЗЭЩ ЛЬЮЗ, ЩЧН ЯЮБХ, НАЩ ШМЩЮКАР...

БЬБЮИ ЧСТТГ ЮЕЯЧС ЖЬСЙЭГИ ЪС ЧЬЭ, МГЬЖР ЩЕЖЭСЭЯС
ФЕЩДРХВИ ЯВЮЕЗЩ З ЯНЦЗСЩУЧЫС ГТЕКШЯ ХХШПУЧЯЪЕ У

УЗУСЧ ЮМ МЦХ-АЩНУ УЪФЕЯЭ ЭЪФ НДЮПИ, Е ЮС ЧГЪХШЪМЦС О
ЪСЭЧГЪИК ЫМП ЮСЪЗЯ ЪИЧРУЪ Ф ЪСЪЕВЦС ДЯРИГГЪЗАЦЦТГЦ

ЫЮУЖЪЪЫГЦГТЧГЖГФДБФЦЗЯХТГВЮБУТХВШКНЫМЪРУАЧСТАБТЭ
ЭМЧСЪЕЪЪФЪЭЦСЪЧРШТЬРЬШЩКВЮЗСАЪНЖГЪЕЖГФКБФЪХЪЕЧМ
ШИУЧКМЦЦНЬЭВСЭСЪЙЦНЮМЙАСХЧМШГВЦУЕТЧДУГХЩЕЩОЧГ
БЗСУЪЦДБФТЭЭМГЗВЛЦЪМИГВЦРГЮЩУСЦЗНХХШЧНМЩЛЧУЕБЦГЕ
ВЩЛЪЦЕЖСКЮЭЖЭДГСРЪВЩАКЦЦКЩЯЭЧХГЦУЧИГБНУВЯЭАЮФРЭ
ЦШЕЮЪЦРЪЧГЪИПГЯЦБЦБТЬГЭДСЦАЩФГХДШЗЩЮБЮМЙЦПУЮБЦ
ГЭМЧЯЮВСШКЯЩЕХЯХВЯХЪСЫЕКФМЮБЦХФРЭЪЧХЦХХЪЩКГЛИГ
ВЮКВРРВЗКВЩНЖЖЪЙЭГСРСЮБГГЩУЖРЮЦФЦДЯРЭИИФЗХЮФГЮ
МЙЩБВЦРУЖГМЧЯЯШСНБЦКЮЭЦИАСУТГЦШЧЦГБЪВЦЫХЭРУТЬЮ
ЩУЭОУГТЕКБММАЦГТГЪЧВЯДКВЩСАПРКЮЦЖУЪНБОТЬЙЩНБЩК
ЩЯЭЧХГЦЕБУЩЮБИГЮДШЯЮНЗЪЙВЯЩБЯИГФЪЩБЯИГЦЫУТГЪСИ
ЦГБУМЦЮИЮУЦМКШЯФГУСЙЪЮФКУУЦКСЦЗУСЦМЧУАЪНФГЩУ
ЯЦХИЧМГОЩШХЪРЫЦЩИИФЧРУМЧСФЪЖМХХЪЮОКЕФВБМЗРОЖУЪ
НКДШЗЫМЫЩЕЩЯШМЩЮАЧСЮБЩЦГВЮЕЧЫХЭВЯЧЖГОШУКФЪЮ
УГЧГОАЪЯОКЗЯЧМДШМЩОЕЪЭИГЭСЪЖЗЯНЮЪВЮЗЪРХИШСОЩЦЧ
ЦЪЦЗЮФПГУЦДРКЗЦКДБФДЗЮБИВЧАНСЮБУФЕЩЭШЗВЮЗЭЩЛЪЮ
ЗЩЧНЯЮОХНАЩШМЩЮКАРЪЪЮИЧСТТГЮЕЯЧСЖЪСЙЭГИЪСЪЭ
МГЪЖРЩЕЖЭСЭЯСФЕЩДРХВИЯВЮЕЗЩЗЯНЦЗЩУЧЫСГТЕКШЯХХ
ШПУЧЯЪЕУУЗУСЧЮММЦХАЩНУУЪФЕЯЭЭЪФНДЮПИЕЮСЧГЪХШЪ
МЦСОЪСЭЧГЪИКЫМПЮСЪЗЯЪИЧРУЪФЪСЪЕВЦСДЯРИГГЪЗАЦЦТГЦ

Между БФ 70

Между ЯИ 7

Между БУ 41

Между СЪ 49

6. Составьте алгоритмическое и программное обеспечение: процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста.

7. Составьте алгоритмическое и программное обеспечение: процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.

Вариант 1

1. Ефвнгв злччиуиршлуципгв ччрнщлв ритууиюерг
2. Хифпъ нметмалпа цшуря шебари – ифугепиер ракеракити и её нменоцашапиер

3. тояаиовпдтлррлньеиеакмнжм
4. А=«Если запастись терпением и проявить старание, то посеянные семена знания непременно дадут добрые всходы. Леонардо да Винчи», В=«знание».

Вариант 2

1. Рлыхс ри еиырс тсз оцрсб
2. Паута лкапошикля ноцсиппой паутой ш кой лкенепи, ш татой носьфуекля ракеракигелтири рекоцари
3. стллёбеотъьпексыкешаснидаченпишикаепыемьчпмотчоселбтентясаормен
4. А=«Учиться и, когда придет время, прикладывать усвоенное к делу — разве это не прекрасно! Конфуций», В=«время».

Вариант 3

1. Лфхсулв цылх, ыхс рлнгнгв еогфхя ри дюегих еиырсм
2. Паута щэф ракеракити – пе паута
3. ммауамрычнчеуапееттчдолпоаеузоопменвтноутаеозтосёкмноня
4. А=«Наука есть наилучший путь для того, чтобы сделать человеческий дух героическим. Джордано Бруно», В=«наука».

Вариант 4

1. Лфхсулыифнл тиуеюи еюдсую тусьол е Лцзии тул Тсрхлл Тлогхи
2. Тшапкошый торнюкем шфсораек сющую лошмереппую тминкочмазигелтую лилкеру
3. сеяелодднутегнчклоьяратейыноунттвмыиплы
4. А=«В одном просвещении найдем мы спасительное противоядие для всех бедствий человечества! Карамзин Н. М», В=«учение».

Вариант 5

1. Нултхсжугчлв угкугдгхюегих пихсзю кгэлхю лрчсупгщлл сх рифгрнщлсрлусегррежс зсфхцтг
2. Аццикишпая чмунна л цоноспикесьпой онемадией урпохепия, лшяфаппой ло лсохепиер фатопари цилкмищукишполки, пафишаекля тосьдор
3. сзветмглаельаеемлоньялдыивазьоскеуанвлоккнааягааиятмоесмьичсаа
4. А=«Хуже всего то, что кто смолоду плохо обучен, тот до старости в этом не сознается. Петроний», В=«время».

Вариант 6

1. Хисулв ылфио фимыгф схрсфлхфв н угкувзц тулногзрюш ргцн
2. Гер пешехелкшеппей гесошет, кер щосее оп ушемеп, ГКО илкипа у нечо ш тамрапе
3. ундитимиеътнклевбеаёреыикнязтмонедьейотенюойсзищпцянгиребад

йельче

4. А=«Тот, кто, обращаясь к старому, способен открывать новое, достоин быть учителем. Конфуций», В=«школа».

Вариант 7

1. Нгйзюм еютцфнрлн ДЖЦЛУ цеиуиррс еогзиих нсптябхиусп
2. Пи оцип шекем пе щуцек нонукпыр цся томащя, токомый пе шывес из чашапи
3. клшуетслтрояяронртувааьдаузтнтчмообьиымв
4. А=«Частый и громкий смех есть признак глупости и дурного воспитания. Честерфилд Ф», В=«смех».

Вариант 8

1. ПУХЛ – ецк хесим пиыхю
2. Чмарр шоси шелик кяхесее, гер депкпем малллухцепия и ущехцепия
3. уооримтрдтгпецаирчеебоиитнтймсеисиятвеп
4. А=«На человека, которого довели до того, что он даже не боится быть смешным, столь же мало можно положиться, как и на преступника. Цвейг С.», В=«смысл».

Вариант 9

1. Носз Ъ иррср веовихфв сфрсестсосйрлнсп фсеуипиррсм кгэлхю лрчсупгщлл
2. Рыльс ифмегеппая елкь сохь
3. хнядеозурррардобыщнршлибуиутхгечаомшоаг аатно
4. А=«Человек не может быть неисправимо плохим, если он хотя бы раз от души смеялся. Карлейль Т.», В=«душа».

Вариант 10

1. Перслз, ц юсхсусжс ефи аоипирхю сдугхлпю схрсфлхиоярс стуизиоиррсм е рип гождуглыифнсм стиугщлл, ргкюегихфв жуцттсм
2. Къры пифтиж илкип пар цомохе Пал шофшываюбий оштрап
3. ссхгйрлолцеедаадпнзриыоыь
4. А=«Есть люди настолько сухие, что вы можете вымачивать их в шутках целый месяц, и ни одна из них не попадет им под кожу. Бигер Г», В=«кожа».