# ***ПРАКТИКА №3***

# **КРИПТОАНАЛИЗ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ**

**Введение**

С криптографией шло развитие и **криптоанализа** – другого противоположного раздела криптологии, предметом которого является разработка методов взлома новых криптографических алгоритмов с целью выявления их надежности. Результатом возникновения каждого нового метода криптоанализа является пересмотр оценок безопасности шифров, что в свою очередь, влечет необходимость создания более стойких шифров.

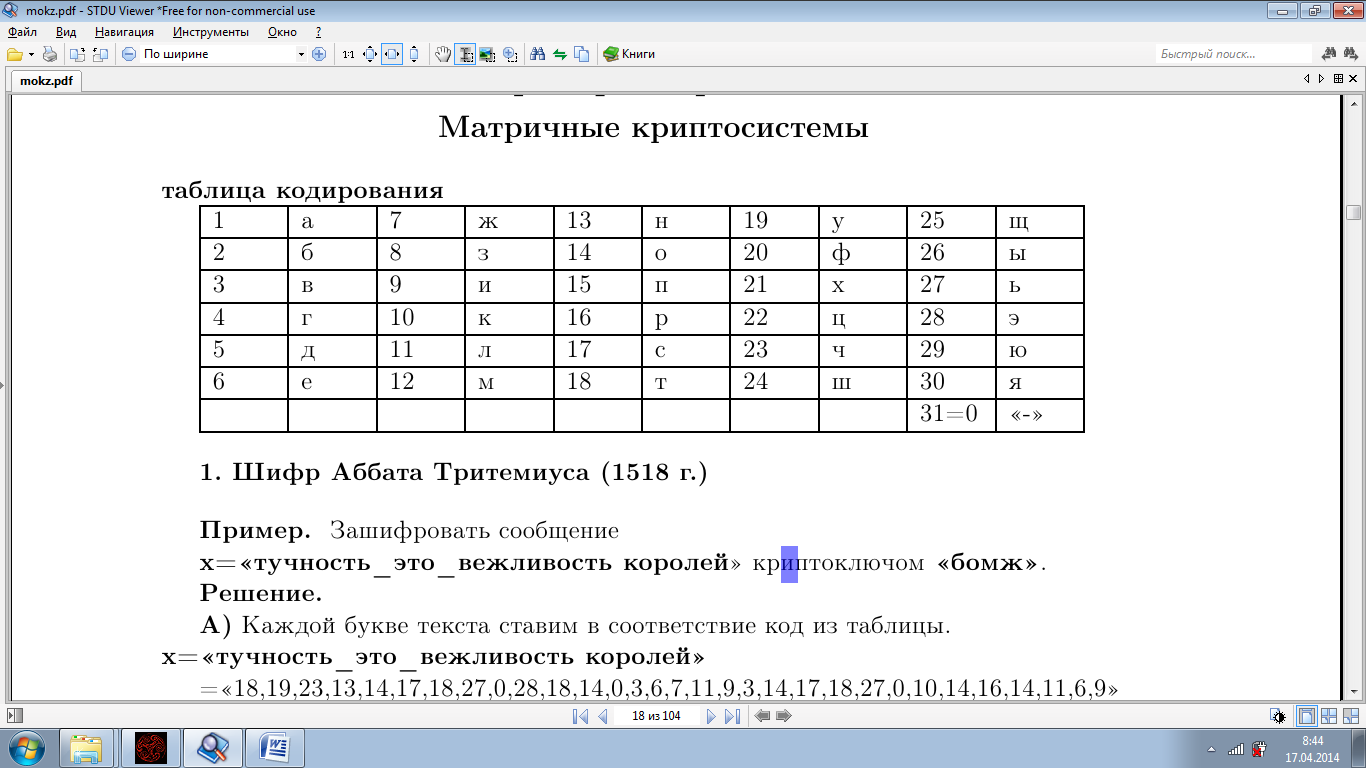
**Криптоанализ** ставит своей задачей в разных условиях получить дополнительные сведения о ключе шифрования, чтобы значительно уменьшить диапазон вероятных ключей. Результаты криптоанализа могут варьироваться по степени практической применимости. Так, криптограф Ларс Кнудсен предлагает следующую классификацию успешных исходов криптоанализа блочных шифров в зависимости от объема и качества секретной информации, которую удалось получить:

* *Полный взлом* – криптоаналитик извлекает секретный ключ.
* *Глобальная дедукция* – криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа.
* *Частичная дедукция* – криптоаналитику удается расшифровать или зашифровать некоторые сообщения.
* *Информационная дедукция* – криптоаналитик получает некоторую информацию об открытом тексте или ключе.

**1.1.Матричные криптосистемы. ШИФР ТРИТЕМИУСА**

*Шифр Тритемиуса* - система шифрования, разработанная Иоганном Тритемием. Представляет собой усовершенствованный шифр Цезаря, то есть шифр подстановки. По алгоритму шифрования, каждый символ сообщения смещается на символ, отстающий от данного на некоторый шаг. Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы. Сама функция должна гарантировать целочисленное значение.

Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную. Применяется таблица кодирования, например



**ПРИМЕР 1.** Зашифровать сообщение **x= «тучность\_это\_вежливость королей»** криптоключом **«бомж».**

**Решение**

**А)** Каждой букве текста ставим в соответствие код из таблицы **x= «тучность\_это\_вежливость королей»**

= «18,19,23,13,14,17,18,27,0,28,18,14,0,3,6,7,11,9,3,14,17,18,27,0,10,14,16,14,11,6,9»

Разбиваем текст на блоки, равные размеру ключа {18,19,23,13},{14,17,18,27},{0,28,18,14},{0,3,6,7},{11,9,3,14}, {17,18,27,0},{10,14,16,14},{11,6,9,0}

Для того, чтобы заполнить последний блок мы дополнили текст пробелом\_

Каждой букве ключа ставим в соответствие код из таблицы **Q1= «бомж» = {2,14,12,7}**

Складывая поблочно исходное сообщение с ключом получим **y=x+Q1 (mod 31)**: {18,19,23,13},{14,17,18,27},{0,28,18,14},{0,3,6,7},{11,9,3,14},{17,18,27,0},{10,14,16,14},{11,6,9,0}

+

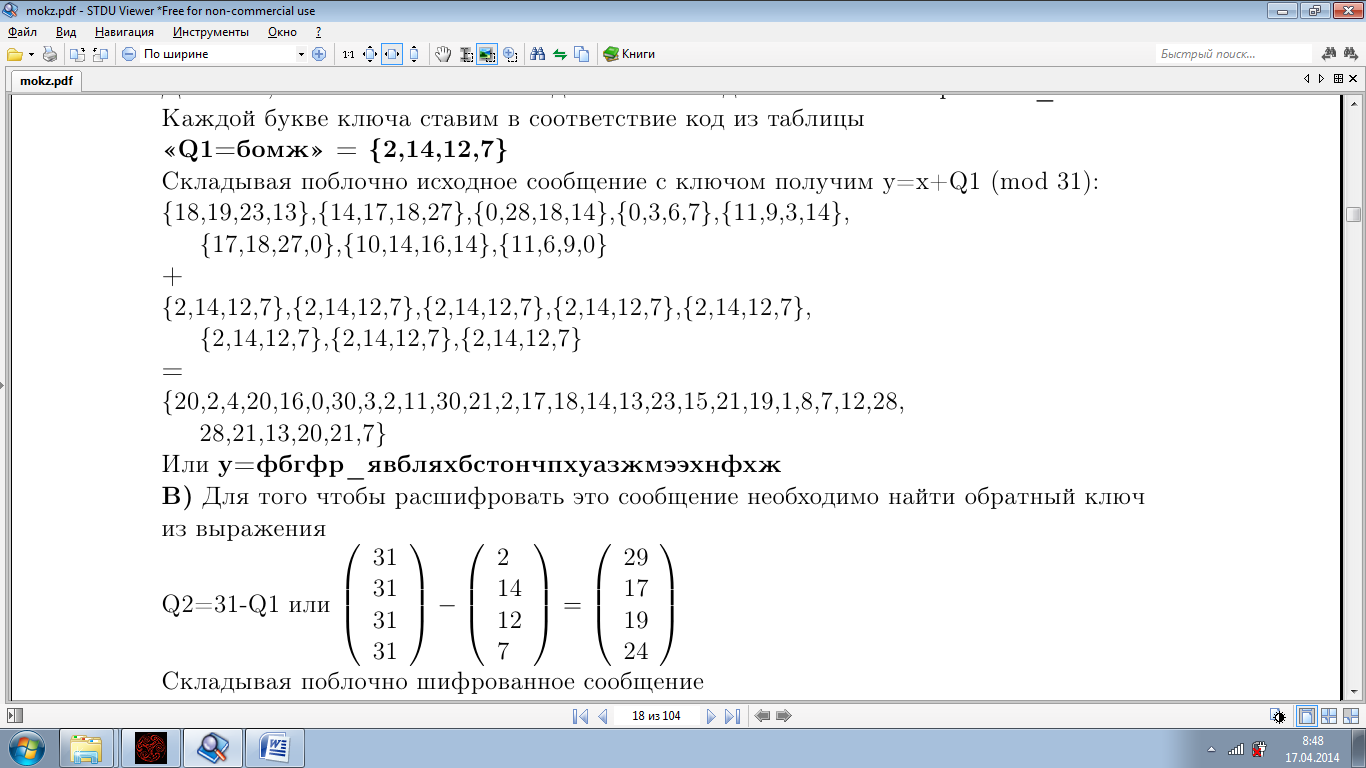
{2,14,12,7},{2,14,12,7},{2,14,12,7},{2,14,12,7},{2,14,12,7},{2,14,12,7},{2,14,12,7},{2,14,12,7}

=

{20,2,4,20,16,0,30,3,2,11,30,21,2,17,18,14,13,23,15,21,19,1,8,7,12,28,28,21,13,20,21,7}

или **y=фбгфр\_явбляхбстончпхуазжмээхнфхж**

**B)** Для того чтобы расшифровать это сообщение необходимо найти обратный ключ из выражения.



Складывая поблочно шифрованное сообщение

{20,2,4,20,16,0,30,3,2,11,30,21,2,17,18,14,13,23,15,21,19,1,8,7,12,28,28,21,13,20,21,7}

с обратным ключом Q2 получим

{x=18,19,23,13,14,17,18,27,0,28,18,14,0,3,6,7,11,9,3,14,17,18,27,0,10,14,16,14,11,6,9,0}

Или **«x=тучность\_это\_вежливость королеи».**

**ЗАДАНИЕ №1.** Расшифровать сообщение зашифрованное протоколом **y=x+Q (mod n)**

|  |  |  |
| --- | --- | --- |
| Вариант | Ключ | Сообщение |
| 1 | Q= «один» | y= сдырннтн\_дьюпшщьыдшючпкхизклофпюфзпяаоир\_лищ этт\_эхгнсдщухохнелщыэдлущуньоосьрхкффттм\_ |
| 2 | Q= «ангел» | y= фютуфгнхищжнифэуьнуэуртеэеупжфуугифеньшщакц флоугимщугел |
| 3 | Q= «курсант» | y= у\_цяоьтбфщякчькгсщгцхлсвстояюсрькэебжосе усэщьноьгэпрсант |
| 4 | Q= «тигр» | y= бфтеьпгхащтфьицашлчодищявчэщзиуааятхьхыц |
| 5 | Q=«яблоко» | y= оррпнщю\_дфроарцквчмуюсшок\_рфуозосфэоарцкв фяуьфпьдуюпэчрффер\_ирпэкшннфер\_сдмочэвблоко |
| 6 | Q=«мячик» | y= трвткгдвчнтишичткусимилшуяычьшмдьчкьпеолксчик |
| 7 | Q=«машина» | y=ттгтндысщицетушунннджхуе\_аацошхушходыняоааь пикнингчсзгнуфияащбиуьухлщхца |
| 8 | Q=«слон» | y= юсьмплшьюшп\_яямнвщроихбнямотфягч\_чьогшбл |
| 9 | Q=«кура» | y= беявду\_сшдььэпрорцятщэвбчалнкшятэфвпбаяаьюс илемащгсгпжра |
| 10 | Q=«мышка» | y= эхылахфяэар\_якдчоысжмьшбжчиьрлмяюрапдмь оташуаоакщмннеша |
| 11 | Q=«боцман» | y= гфзцпызегыт\_юоуяпнофзяпнеуэмрюрчзбптлацяпн щфыыаызошжгозацман |
| 12 | Q=«мент» | y= упх\_зекдыеьктцучзехумчщшэширмуьтяфшоцфн\_трьд ыцзшмсуы\_шнфтонагмюшспнт |
| 13 | Q= «рубль» | y= зэуюкразлос\_бпацухндаф\_юьсуфмзрчжсьуфчюбауулмгыюсз |
| 14 | Q= «закон» | y= лтртьзолорщж\_оыоа\_соыкэоэцушыазшээнлтрть знлщьзбксяоцкыыцдшон |
| 15 | Q= «патрон» | y= хтющоюкчуаннвеуач\_лабяошхгащожхлшраьп п\_рбэрешвоырабапрккттэч |
| 16 | Q= «шериф» | y= мтюгышсооюшоюктле\_щюеэщшпшжрозижытфаж\_ч абусжжшысужуериф |
| 17 | Q=«штраф» | y= кьюкюшдгнхет\_пкжщрохшатнхетблзиьуаяжгпшввт блхауьабщвыпащ\_раф |
| 18 | Q= «цель» | y= гмхкифьцэеоцыскахшлсжжнмстфьефюквщлуифлюддюн хеяюэнмотель |
| 19 | Q=«налог» | y= эсмсн\_жцкх\_гщоуюкшнпьашфт\_мщхсзжлыкюьлютн фхякэмсьнлаыээоушбжежф\_внгсяяномяттблсгтпцщд |
| 20 | Q= «лидер» | y= вьуечлечфрчгдиярушевщитмррчфпьфифцщчпчжрыфу ьскидер |
| 21 | Q= «ордер» | y= цсэмэочлевясчпьчбаеуиртжрюякжашщдилобетщоьшю ифржарьцдхачцннсщщдер |
| 22 | Q= «орден» | y= яяцчцнрбшьобчцоьсдчньцфцуубпжхбцсащо\_хфещлсен |
| 23 | Q=«турне» | y= \_фб\_фснщцефгс\_ж\_увьштлмцебфьиэнубьчдфушдрер пжыэбнитвп\_пящаыфяу\_юфгеаоугеууе |
| 24 | Q= «жмурки» | y= рщбфпкжюлсььвтубнктхцсрьшлувлужщщястмнаюшияя брчпж\_д\_рмзтммкчщююябтщзуукыщыгячэ |
| 25 | Q= «шкурка» | y= яцюяьуфкбвршяьеуроедирнкебщбэжишцруидргпруки уукхбофтлкллирка |
| 26 | Q= «диск» | y=хэвьпкркхпиедлчтдхтэеиаылмблякчэцзсндо\_фркцк |
| 27 | Q= «ролик» | y=ючхьшрьсиьээтпэрьмснсажинс\_ллрштькцяашгцрфэф урьмиьвфшпкучэтэргщьерэрцлртькцяамик |
| 28 | Q= «нолик» | у=ыпхччудльшнчэархщмищюфэьюэьщыенряунощжцшнсвпыооычьшфрцрсэлшыу\_юэщычхккхпьптощфифошфпк\_элхлыккуу |
| 29 | Q= «один» | y= сдырннтн\_дьюпшщьыдшючпкхизклофпюфзпяаоир\_лищ этт\_эхгнсдщухохнелщыэдлущуньоосьрхкффттм\_ |
| 30 | Q= «ангел» | y= фютуфгнхищжнифэуьнуэуртеэеупжфуугифеньшщакц флоугимщугел |

**2. КРИПТОАНАЛИЗ ШИФРА СТОЛБЦОВОЙ ПЕРЕСТАНОВКИ**

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 1. Сочетаемость букв русского языка

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Г** | **С** | **Слева** |  | **Справа** | **Г** | **С** |
| 3 | 97 | л, д, к, т, в, р, н | **А** | л, н, с, т, р, в, к, м | 12 | 88 |
| 80 | 20 | я, е, у, и, а, о | **Б** | о, ы, е, а, р, у | 81 | 19 |
| 68 | 32 | я, т, а, е, и, о | **В** | о, а, и, ы, с, н, л, р | 60 | 40 |
| 78 | 22 | р, у, а, и, е, о | **Г** | о, а, р, л, и, в | 69 | 31 |
| 72 | 28 | р, я, у, а, и, е, о | **Д** | е, а, и, о, н, у, р, в | 68 | 32 |
| 19 | 81 | м, и, л, д, т, р, н | **Е** | н, т, р, с, л, в, м, и | 12 | 88 |
| 93 | 17 | р, е, и, а, у, о | **Ж** | е, и, д, а, н | 71 | 29 |
| 98 | 11 | о, е, а, и | **З** | а, н, в, о, м, д | 51 | 49 |
| 27 | 73 | р, т, м, и, о, л, н | **И** | с, н, в, и, е, м, к, з | 25 | 75 |
| 55 | 45 | ь, в, е, о, а, и, с | **К** | о, а, и, р, у, т, л, е | 73 | 27 |
| 77 | 23 | г, в, ы, и, е, о, а | **Л** | и, е, о, а, ь, я, ю, у | 75 | 25 |
| 80 | 20 | я, ы, а, и, е, о | **М** | и, е, о, у, а, н, п, ы | 73 | 27 |
| 55 | 45 | д, ь, н, о, а, и, е | **Н** | о, а, и, е, ы, н, у | 80 | 20 |
| 11 | 89 | р, п, к, в, т, н | **О** | в, с, т, р, и, д, н, м, | 15 | 85 |
| 65 | 35 | в, с, у, а, и, е, о | **П** | о, р, е, а, у, и, л | 68 | 32 |
| 55 | 45 | и, к, т, а, п, о, е | **Р** | а, е, о, и, у, я ,ы, н | 80 | 20 |
| 69 | 31 | с, т, в, а, е, и, о | **С** | т, к, о, я, е, ь, с, н | 32 | 68 |
| 57 | 43 | ч, у, и, а, е, о, с | **Т** | о, а, е, и, ь, в, р, с | 63 | 37 |
| 15 | 85 | п, т, к, д, н, м, р | **У** | т, п, с, д, н, ю, ж | 16 | 84 |
| 70 | 30 | н, а, е, о, и | **Ф** | и, е, о, а, е, о, а | 81 | 19 |
| 90 | 10 | у, е, о, а, ы, и | **Х** | о, и, с, н, в, п, р | 43 | 57 |
| 69 | 31 | е, ю, н, а, и | **Ц** | и, е, а, ы | 93 | 7 |
| 82 | 18 | е, а, у, и, о | **Ч** | е, и, т, н | 66 | 34 |
| 67 | 33 | ь, у, ы, е, о, а, и, в | **Ш** | е, и, н, а, о, л | 68 | 32 |
| 84 | 16 | е, б, а, я, ю | **Щ** | е, и, а | 97 | 3 |
| 0 | 100 | м, р, т, с, б, в, н | **Ы** | л, х, е, м, и, в, с, н | 56 | 44 |
| 0 | 100 | н, с, т, л | **Ь** | н, к, в, п, с, е, о, и | 24 | 76 |
| 14 | 86 | с, ы, м, л, д, т, р, н | **Э** | н, т, р, с, к | 0 | 100 |
| 58 | 42 | ь, о, а, и, л, у | **Ю** | д, т, щ, ц, н, п | 11 | 89 |
| 43 | 57 | о, н, р, л, а, и, с | **Я** | в, с, т, п, д, к, м, л | 16 | 84 |

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 — 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 105 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 2. Чередование гласных и согласных

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Г** | **С** | **Всего** |
| **Г** | 6588 | 38310 | 44898 |
| **С** | 38296 | 16806 | 55102 |

**ПРИМЕР 2.** Дан шифр-текст: СВПООЗЛУЙЬСТЬ\_ЕДПСОККАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **С** | **В** | **П** | **О** | **О** |
| **З** | **Л** | **У** | **Й** | **Ь** |
| **С** | **Т** | **Ь** | **\_** | **Е** |
| **Д** | **П** | **С** | **О** | **К** |
| **К** | **А** | **Й** | **З** | **О** |

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского и английского алфавита, а также таблицы частот биграмм представлена выше). В первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **В** | **О** | **С** | **П** | **О** |
| **Л** | **Ь** | **З** | **У** | **Й** |
| **Т** | **Е** | **С** | **Ь** | **\_** |
| **П** | **О** | **Д** | **С** | **К** |
| **А** | **З** | **К** | **О** | **Й** |

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ\_ПОДСКАЗКОЙ

**ЗАДАНИЕ №2.** Расшифровать фразу, зашифрованную столбцовой перестановкой

|  |  |
| --- | --- |
| Вариант | Фраза |
| 1 | ОКЕСНВРП\_ЫРЕАДЕЫН\_В\_РСИКО |
| 2 | ДСЛИЕЗТЕА\_Ь\_ЛЬЮВМИ\_ \_АОЧХК |
| 3 | НМВИАИ\_НЕВЕ\_СМСТУОРДИАНКМ |
| 4 | ЕДСЗЬНДЕ\_МУБД\_УЭ\_КРЗЕМНАЫ |
| 5 | СОНРЧОУО\_ХДТ\_ИЕИ\_ВЗКАТРРИ |
| 6 | \_ОНКА\_БНЫЕЦВЛЕ\_К\_ТГОАНЕИР |
| 7 | НЗМАЕЕАА\_Г\_НОТВОССОТЬЯАЛС |
| 8 | РППОЕААДТВЛ\_ЕБЬЛНЫЕ\_ПА\_ВР |
| 9 | ОПЗДЕП\_ИХРДОТ\_И\_ВРИТЧ\_САА |
| 10 | ВКЫОСИРЙУ\_ОЬВНЕ\_СОАПНИОТС |
| 11 | ПКТИРАОЛНАОИЧ\_З\_ЕСЬНЕЛНЖО |
| 12 | ИПКСОЕ\_ТСМНАЧИ\_ОЕН\_ГДЕЛА\_ |
| 13 | АМВИННЬТЛЕАНЕ\_ЙОВ\_ОПХАРТО |
| 14 | АРЫКЗЫ\_КЙТНЛ\_ААЫ\_ОЛБКЫТРТ |
| 15 | \_ПАРИИВИАРЗ\_БРА\_ИСТЬЛТОЕК |
| 16 | П\_ЛНАЭУВКАА\_ЦИИВР\_ОКЧЕДРО |
| 17 | ЖВНОАН\_АТЗОЬСН\_ЫО\_ФВИИКИЗ |
| 18 | ОТВГОСЕЬЬТАДВ\_С\_ЬЗАТТЕЫАЧ |
| 19 | ЯАМРИТ\_ДЖЕХ\_СВЕД\_ТСУВЕТНО |
| 20 | УЬБДТ\_ОЕГТВ\_ОЫКЭА\_ВКАИУЦИ |
| 21 | ЛТБЕЧЛЖЫЕ\_ \_ОАПТЖРДУ\_ЛМНОА |
| 22 | ИТПРКРФАГО\_АВЯИА\_ЯНЖУАКАН |
| 23 | ПКЕЕРРПО\_ЙУСТ\_ИТПСУТЛЯЕИН |
| 24 | ИЬЖЗНСД\_ТДН\_ЕТ\_НУВЕУРЫГОЫ |
| 25 | ЕОУРВА\_НЬРИАДИЦЕПИ\_РНШВЫЕ |
| 26 | П\_ЛНАЭУВКАА\_ЦИИВР\_ОКЧЕДРО |
| 27 | ОПЗДЕП\_ИХРДОТ\_И\_ВРИТЧ\_САА |
| 28 | СОНРЧОУО\_ХДТ\_ИЕИ\_ВЗКАТРРИ |
| 29 | РППОЕААДТВЛ\_ЕБЬЛНЫЕ\_ПА\_ВР |
| 30 | ИПКСОЕ\_ТСМНАЧИ\_ОЕН\_ГДЕЛА\_ |

**Контрольные вопросы**

1.Понятие криптоанализа.

2.Задача криптоанализа.

3.Предположения криптографа Ларса Кнудсена.

4.Шифр Тритемиуса.

5.Что следует иметь в виду при анализе сочетаемости букв.

6.Что доказал А.А.Марков.