**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №3**

**по дисциплине «Криптографические методы защиты информации»**

**Тема:** **Изучение классических шифров Hill, ADFGVX, Playfair**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 5381 |  | Кобылянский А.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2018

**Цель работы**

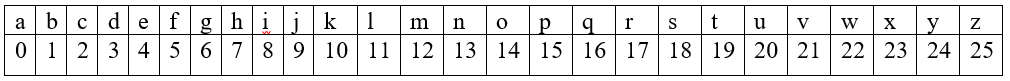
Исследовать шифры Hill, ADFGVX, Playfair и получить практические навыки работы с ними, в том числе и в программном продукте CrypTool 1 и 2.

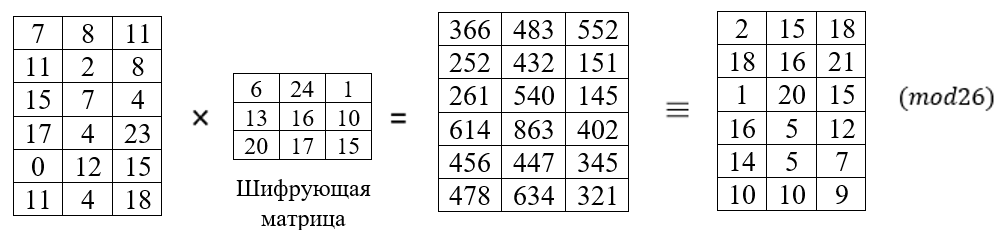
**1.** **Шифр Хилла (Hill)**

**1.1 Исходное описание шифра (как в лекции). Пример вычисления шифрующей и расшифровывающей матрицы.**

Шифр Хилла подразумевает работу с матрицами. Перед шифрованием необходимо каждому символу открытого текста сопоставить число, записать полученные значения в матрицу размера *n\*m* и сформировать шифрующую матрицу *n\*n*. Шифрующая матрица должна быть обратимой для выбранного модуля, по которому производятся вычисления (обычно для английского алфавита этот модуль 26). Для шифрования производится умножение матрицы открытого текста на шифрующую матрицу. Для дешифрации необходимо шифротекст умножить на обратную к шифрующей матрицу.

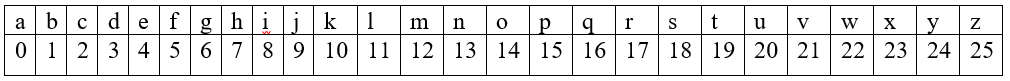
В качестве примера шифрования, зашифруем текст «*HILLCIPHEREXAMPLES*»:

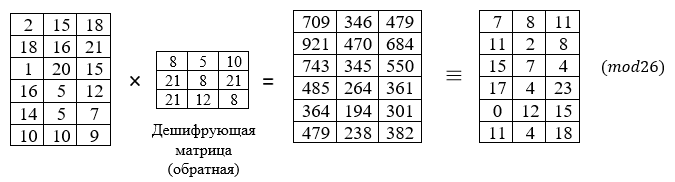




Шифротекст: *CPSSQVBUPQFMOFHKKJ*

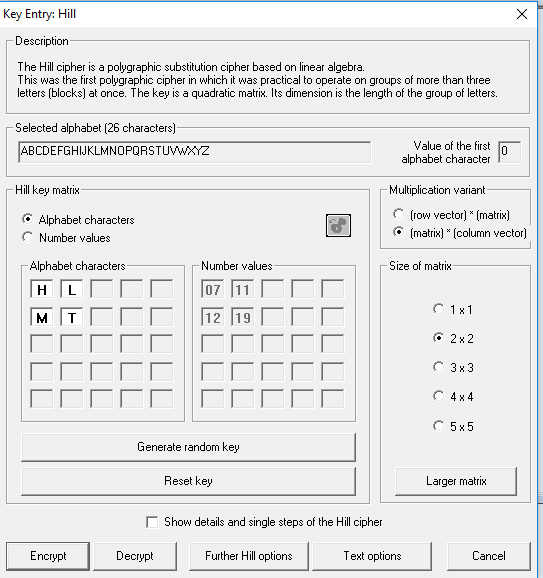
Для демонстрации дешифровки, расшифруем полученный шифротекст «*CPSSQVBUPQFMOFHKKJ*»:





Получаем открытый текст: *HILLCIPHEREXAMPLES*

**1.2 Реализация в CrypTool 1.0 (скриншот, спецификация параметров).**



Select alphabet – задание алфавита (неалфавитные символы при шифровании/дешифровании обрабатываются по особому, согласно настройкам в меню Text options)

Value of the first alphabet character – для зашифровки необходимо закодировать буквы числами. В данном поле устанавливается, с какого числа начинается нумерация букв алфавита.

В группе Hill key matrix можно задать матрицу шифрования буквами или числами. Можно сгенерировать случайную обратимую матрицу.

В группе Size of matrix задается размер матрицы шифрования.

В группе Multiplication variant можно выбрать, как будет проходить умножение, в какую матрицу будет записан исходный текст – с n столбцами или с n строками. В любом случае, текст будет заноситься в матрицу по столбцам и читаться тоже по стобцам.

**1.3. Пример работы шифра для выбранных параметров и текста сообщения.**

Везде ниже мы умножаем шифрующую матрицу на матрицу с текстом . Нумерация алфавита начинается с 0.

|  |  |  |
| --- | --- | --- |
| **Открытый текст** | **KEY** | **Результат шифрования** |
| KOBILIANSKY |  | UOWHYRNNMGKY |
| KOBILIANSKY |  | UAWZYJNAMWKY |
| ABCDEFGHI |  | FQFYFGFOMI |

**1.4 Тип шифра**

Тип шифра – блочный.

**1.5 Ключ шифра**

Ключ шифра – матрица шифрования.

**1.6 Оценка сложности атаки “грубой силы”**

Если длина текста равна , то выбрав соответствующую матрицу шифрования размером мы можем получить из любого текста любой другой (Почти из любого. Если рассматривать алфавит в 26 символов, то если все символы текста кратны 2 или 13, то и все символы зашифрованного текста будут кратны 2 или 13 соответственно).

Тогда для полного перебора потребуется , где – размер алфавита.

Если знать размер шифрующей матрицы - , то потребуется

шагов.

**1.7 Описание атаки на шифр с использованием утилит CrypTool 1.0.**

Атака производится со знанием части исходного текста. Так как шифр блочный, то можно расшифровывать отдельные блоки. Если блоков достаточно, то зная исходный и зашифрованный фрагменты можно составить и решить СЛАУ на коэффициенты шифрующей матрицы. В Cryptool 1.0. перебираются размеры шифрующей матрицы (=размеры блоков) и ищутся возможные решения системы для каждого размера.

**1.8 Результат расшифровки перехваченного от коллеги текста.**

Известное обращение:

what up dawg

Перехваченный текст:

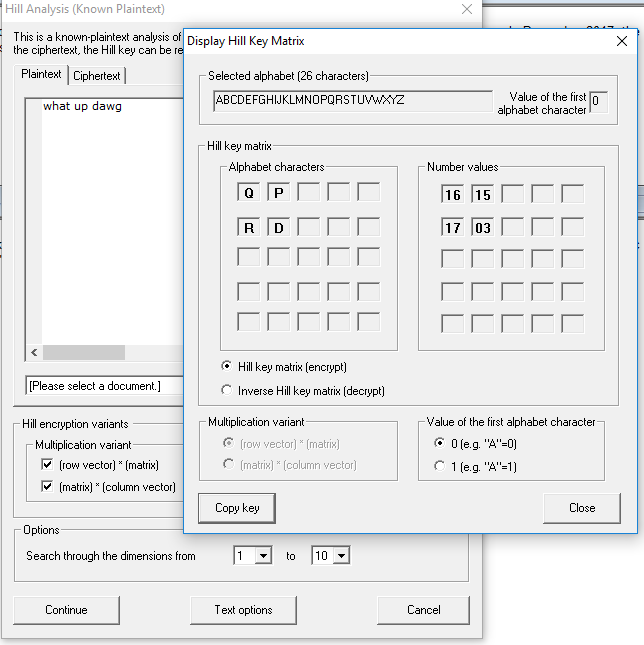
pfzf zv wzac

Tghpn ldlb tuca nrqkafab zl ddjufou tgl vhpaucdwvos eitg eksitgltl hvvktupzs ydgisel vqb axkna "ekcaxm" dtw "lbdlu" cajma tgd jmdfncmo gm jufgfix. Lt Elouzzhp 2017, tgc Ozshpizc Neuaxuy Iykpldijgm elwgelv eq edmis tge eldgb "buwqvzu" stw "kgiytwvzu" sc u qcatijgtax exk nkcaxw/fufgf axknltzlcwk qz sqbtf JMM whpgfw fntkzvzb TLTW.

Расшифровка и ключ:

what up dawg

There have been attempts to replace the terminology with something different because the terms "master" and "slave" evoke the practice of slavery. In December 2017, the Internet Systems Consortium decided to allow the words "primary" and "secondary" as a substitute for master/slave terminology in their DNS server software BINO.



**2. 2. Комбинированный шифр ADFGVX**

**2.1. Исходное описание шифра (как в лекции).**

Шифр ADFGVX — один из самых известных шифров времён Первой мировой войны, который использовался немецкой армией. Особенность шифра заключается в том, что он построен на соединении базовых операций замены и перестановки.

Шифрование осуществляется в два этапа. На первом этапе задается матрица, заполненная символами алфавита, а также цифрами от 0 до 9. Далее каждый символ кодируется парой символов, на пересечении которых он находится. На втором этапе производится перестановка столбцов, заданная кодовым словом.

Например, зашифруем текст «*CIPHEREXAMPLE*» с кодовым словом «OURKEY»:

1. Составляем матрицу и кодируем каждый символ открытого текста

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | a | d | f | g | v | x |
| a | a | b | **c** | d | e | f |
| d | g | h | i | j | k | l |
| f | m | n | o | p | q | r |
| g | s | t | u | v | w | x |
| v | y | z | 0 | 1 | 2 | 3 |
| x | 4 | 5 | 6 | 7 | 8 | 9 |

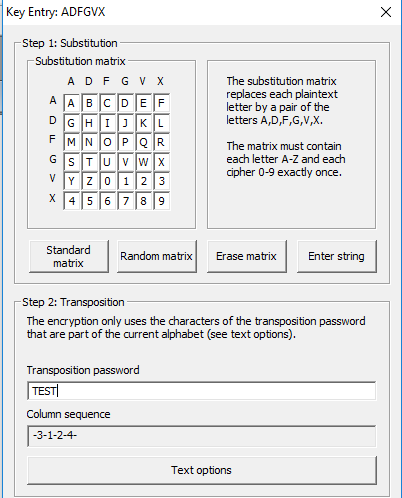
Получаем последовательность: *AFDFFGDDAVFXAVGXAAFAFGDXAV*

1. Производим перестановку:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **o** | **u** | **r** | **k** | **e** | **y** | => | **e** | **k** | **o** | **r** | **u** | **y** |
| **3** | **5** | **4** | **2** | **1** | **6** | **1** | **2** | **3** | **4** | **5** | **6** |
| a | f | d | f | f | g | f | f | a | d | f | g |
| d | d | a | v | f | x | f | v | d | a | d | x |
| a | v | g | x | a | a | a | x | a | g | v | a |
| f | a | f | g | d | x | d | g | f | f | a | x |
| a | v |  |  |  |  |  |  | a |  | v |  |

Выписываем текст по столбцам и формируем шифротекст: FFADFVXGADAFADAGFFDVAVGXAX

* 1. **Реализация в CrypTool 1.0**



В блоке Substitution можно задать матрицу перестановки.

В блоке Transposition задается перестановка столбцов кодовым словом.

**2.3 Пример работы шифра для выбранных параметров.**

Во всех примерах матрица замены стандартная.

|  |  |  |
| --- | --- | --- |
| **Открытый текст** | **Кодовое слово** | **Результат шифрования** |
| KOBILIANSKY | TEST | VDXAAAFDDFDDADAGVFFFDV |
| KOBILIANSKY | TESTY | VDFGAFFAADDDDVFDADAXFV |
| TEST | TEST | DAAGGGVD |

**2.4 Тип шифра**

Тип шифра – комбинированный.

**2.5 Ключ шифра**

Ключ шифра – матрица замены и перестановка столбцов.

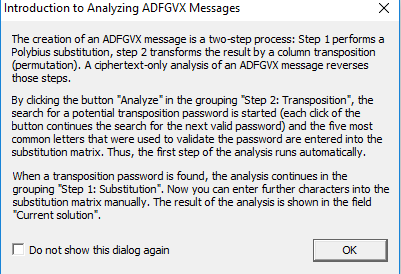
**2.6 Оценка сложности атаки “грубой силы”**

Пусть длина алфавита равна , а длина теста равна . Если известна длина перестановки , то необходимо перебрать вариантов.

Если длину перестановки надо найти, то в худшем случае потребуется не более

попыток.

**2.7 Описание атаки на шифр с использованием утилит CrypTool 1.0.**



Сначала автоматически ищется такая перестановка, чтобы распределение биграмм примерно соответствовало распределению букв в исходном алфавите.

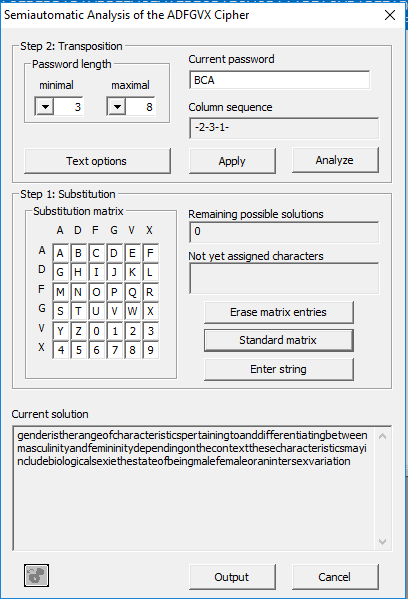
Затем пользователю предлагают попытаться вручную восстановить матрицу замены.

**2.8 Результат расшифровки перехваченного от коллеги текста.**

Зашифрованный текст:

ADAXGDAXFAFXDAAFAXGDAAAXAFDDGFFGDXAXFDADFAADAVFAAFDDGAFGAAFFDDAVADDDFDDVFDAXGDGVDAAFAXGDAAAAFFGGAFDFDFDAGFGDGDGVADDDFAAXFAAFADFDFAGGFFGFFDVAVDADVADAFADFAGVDADFFVGAFFDDADAFAVADDADDAVGVFAGFDFDDADAVDDFFVGFVAFDFGDAFGVGDAAADFAGVDADFFADDDFADFXDFAXAXADAAADFXAFDADVAADVFADDAXAXAXADFDAFGFFGDFADVAFAXADFFGFGGFDDDFAFAAGAXFVGFGFDDGVADAAGXFFVAAXFFDDGAAGFGFAFDAFFDGDDVAFAXADFFGFGAVFAXAVDFFAAAGVDVDVGAAFAVFAAXAVAXFXFFGVGVGADADF

Расшифровка и ключ:



**2.9 Описание атаки на шифр реализованной в CrypTool 2.0.**

В CrypTool 2.0 сначала перебираются возможные ключевые слова, задающие перестановку столбцов. Ключевые слова берутся из словаря. Если индекс совпадений текста, расшифрованного данным ключом, больше порогового значения (0.05), то полученный текст сохраняется для дальнейшей расшифровки (для полной расшифровки необходимо еще найти матрицу замены).

**3. Шифр Плейфера (Playfair)**

**3.1. Исходное описание шифра (как в лекции).**

Для работы алгоритма используется матрица 5\*5 (если используется русский алфавит, то 4 \* 8). В первую строку записывается кодовое слово (без повторения символов) слева направо или по спирали из верхнего левого угла к центру матрицы. Оставшиеся клетки матрицы заполняются незадействованными буквами алфавита в своем изначальном порядке.

Чтобы зашифровать текст его необходимо разбить на пары символов. Процесс шифрования подчиняется следующим правилам:

1. Если два символа совпадают или остался один символ, то к первому символу добавляется *X* и шифруется уже эта пара.
2. Если символы находятся в одной строке, то они замещаются на расположенные в ближайших от них справа символы.
3. Если символы в одном столбце, то они замещаются на расположенные ниже в ближайших от них клетках
4. Если символы находятся в разных углах образуемого ими прямоугольника, то они заменяются на символы, стоящие в противоположных углах этого прямоугольника, в тех же строках.

Расшифровка сообщения происходит инверсией данных правил.

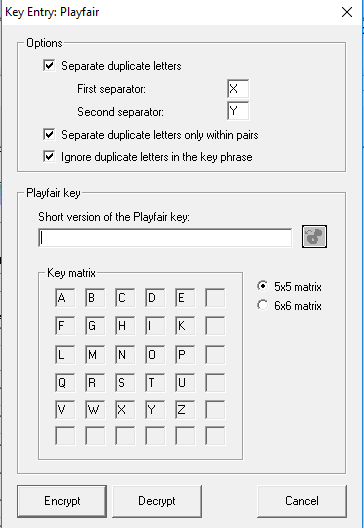
Пример шифрования:

Открытый текст: *HELLO* => *HE LL O* => *HE LX LO*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **l** | g | d | b | a |
| q | m | **h** | **e** | c |
| u | r | n | i | f |
| **x** | v | s | **o** | k |
| z | y | w | t | p |
| Шифрующая матрица | | | | |

Шифротекст: ECQZBX.

**3.2 Реализация в Cryp Tool 1.0 (скриншот, спецификация параметров).**



Separate duplicate letters – когда буква без пары или пара состоит из повторяющихся букв, надо добавить сепаратор. Если первая буква пары не равна First separator, то добавляется он, иначе добавляется Second separator.

Separate duplicated letters only within pairs – вставлять ли сепаратор между подряд идущими одинаковыми буквами, когда они в разных парах. Пример: ABBAT разбивается на AB BA TX, B – повторяются, но не входят в одну пару. Если убрать галочку, то будет AB XB AT.

Ignore duplicate letters in the key phrase – если галочка стоит, то key phrase “BOOK” станет “BOK”, если не стоит, то “BOPK”. Т.е повторяющиеся буквы либо игнорируются, либо заменяются на следующие за ними в алфавите.

В группе Playfair key можно задать шифрующую матрицу с помощью ключевой фразы и выбрать размер матрицы5x5 или 6x6 (с цифрами).

**3.3 Пример работы шифра для выбранных параметров.**

|  |  |  |
| --- | --- | --- |
| **Открытый текст** | **Key** | **Результат шифрования** |
| KOBILIANSKY | KEY | BIKOMLGSPAAW |
| KOBILIANSKY | TEST | IPTNMKBMELZY |
| KOBILIANSKY | TESTY | IPCHMKTRDPFY |

**3.4 Тип шифра**

Тип шифра – блочный.

**3.5 Ключ шифра**

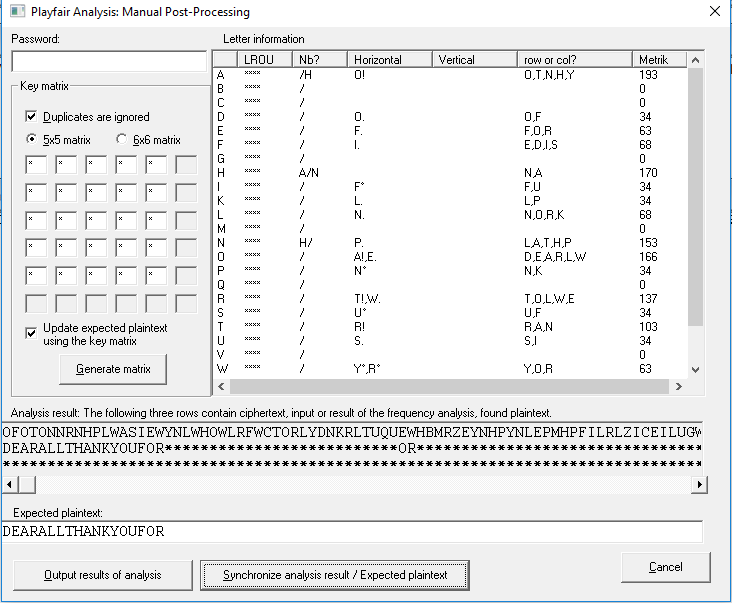
Ключ шифра –шифрующая матрица или кодовое слово и размер шифрующей матрицы.

**3.6 Оценка сложности атаки “грубой силы”**

При матрице имеем сложность Тогда, в худшем случае, при размере матрицы (с цифрами), имеем сложность:

**3.7 Описание методики атаки на шифр с использованием утилиты CrypTool 1.0.**

В Cryptool 1.0 доступно только ручное расшифровывание. Если известна часть открытого текста, то можно восстановить часть структуры шифрующей матрицы. Данная информацию будет собрана в таблицу.



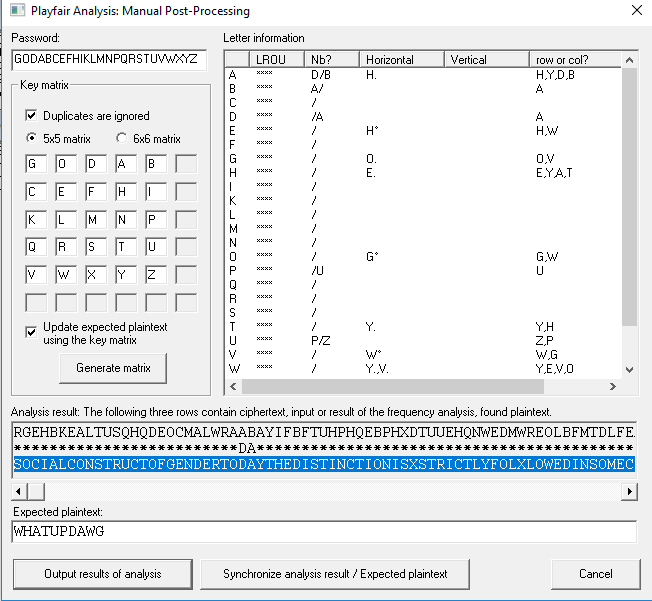
Далее, делая догадки о составе шифрующей матрице и проверяя их вручную, можно расшифровать исходный текст.

**3.8 Результат атаки и расшифровка перехваченного от коллеги текста.**

Известное обращение: «What up dawg”

Зашифрованный текст: YEHYZUABVORFWDREBCTUEBNTLDLHZHTYWEBSEFASIFRHSLHPERDOCEONBFTUHPHQEBPAHROLHLIPERDOCEONRFYDMAOCMALWDTOTERFCPAFHEWFIFUOEQLHUYOTQKHDLLDTYBRRFYNLOEWAOHLOFSUEWFHLWRAHTAYICKAIZQATOSDNDUHHGKEHYCOEWCFTFEOCWLWLDLHXTLFHTHPODHSIFOESOBFAMAROIEGLFZEOFUMWLBATPUHNRIFRXIFMHFLHPFUSYYNLETWFLOUGHFOYNFEALEFNUDEBAFUUHKHUHALOIRYFWHLIPERDOCEONRFYDMAYNFRGEHBKEALTUSQHQDEOCMALWRAABAYIFBFTUHPHQEBPHXDTUUEHQNWEDMWREOLBFMTDLFEALRHYSRFUMFEHBMWNWYNFRGEHBMRECHLEFTDMAADIQLFTYRXUESYRHPAAYIFOEWRAFHONREAQOHTPBHYEBLYEA

Ключ шифрования: GOD



Расшифрованный текст:

WHATUPDAWGSEXOLOGISTIOHNMONEYINTRODUCEDTHETERMINOLOGICALDISTINCTIONBETWEENBIOLOGICALSEXANDGENDERASAROLEINBEFOREHISWORKITWASUNCOMMONTOUSETHEWORDGENDERTOREFERTOANYTHINGBUTGRAMXMATICALCATEGORIESHOWEVERMONEYSMEANINGOFTHEWORDDIDNOTBECOMEWIDESPREADUNTILTHESWHENFEMINISTXTHEORYEMBRACEDTHECONCEPTOFADISTINCTIONBETWEXENBIOLOGICALSEXANDTHESOCIALCONSTRUCTOFGENDERTODAYTHEDISTINCTIONISXSTRICTLYFOLXLOWEDINSOMECONTEXTSESPECIALXLYTHESOCIALSCIENCESANDDOCUMENTSWRITXTENBYTHEWORLDHEALTHORGANIZATIONWHO

**Вывод**

* Шифр “Hill”

Тип шифра – блочный.

Ключ шифра – матрица шифрования

При длине сообщения и длине алфавита сложность равна

При известном размере матрицы шифрования сложность

* Шифр “ADFGVX ”

Тип шифра – комбинированный.

Ключ шифра – матрица замены и перестановка столбцов.

При длине сообщения и длине алфавита сложность равна

* Шифр “Playfair”

Тип шифра – блочный.

Ключ шифра – шифрующая матрица или кодовое слово и размер шифрующей матрицы.

При матрице имеем сложность