Ведение в криптографию.

Шифры подстановки

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

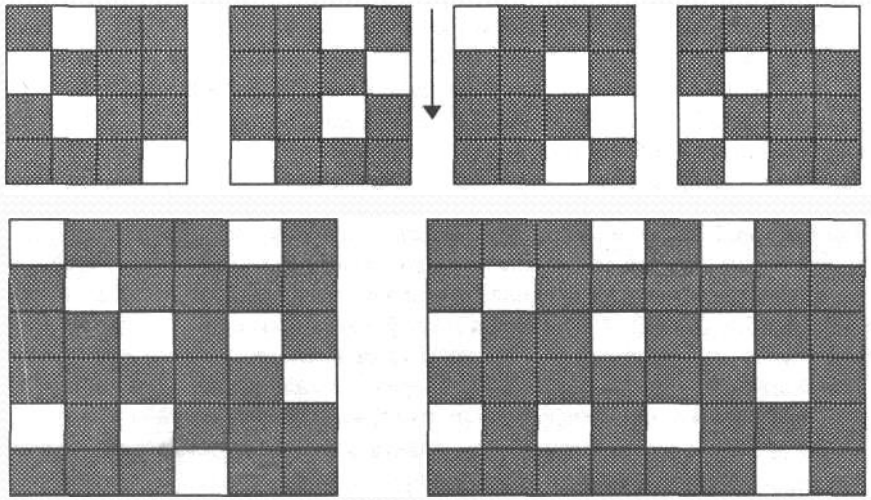
⇑ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
⇓ D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

YHQL YLGL YLFL

Шифры перестановки

1	2	3	4	5	6	7	8	9
п	р	и	л	е	п	л	я	я
р	д	у	м	е	р	п	я	с
у	м	п	р	е	м	у	д	р
в	б	а	ь	ш	е	д	у	б

5	3	8	4	6	1	9	7	2
п	р	и	л	е	п	л	я	я
с	я	п	р	е	м	у	д	р
у	м	п	р	е	м	у	д	р
б	у	д	е	ш	ь	а	б	в



Раскрытие шифра подстановки.

Арабы.

В начале XV в. арабы опубликовали энциклопедию *"Шауба Алъ-Аща",* в которой есть специальный раздел о шифрах. В этой энциклопедии указан способ раскрытия шифра простой замены. Он основан на различной частоте повторяемости букв в тексте. Произведен расчет перечня букв в порядке их повторяемости на основе изучения текста Корана.

В русском тексте чаще всего встречается буква "О", затем буква "Е" и на третьем месте стоят буквы "И" и "А". Более точно: на 1000 букв русского текста в среднем приходится 90 букв "О", 72 буквы "Е" или "Ё" и по 60 букв "И" и "А" и т.д.

Пример.

Д ЖТЦ БЦТ ЧКЙ ХТЖЙФЬЙССТ ХЙОФЙЦСТЙ ХТТЕЭЙСМЙ СДР УФМЬПТХа ХИЙПДЦа ЙЗТ ИТХЦДЦТЫСТ ИПМССЯРОЫЦТЕЯ РТКСТ ЕЯПТ УФТИЙРТСХЦФМФТЖДЦа ФДЕТЦЧ РЙЦТИДЫДХЦТЦСТЗТ ДСДПМЛД

Частота в станд. тексте:	**Частота в закодированном:**
О == 0.0886741	**Т == 0.152866**
И == 0.0653615	**Ц == 0.082805**
Е == 0.0650947	**С == 0.076433**
Т == 0.0601900	**Й == 0.076433**
А == 0.0570297	**Д == 0.070063**
С == 0.0461327	**Х == 0.050956**
Н == 0.0453323	**Ф == 0.044589**
В == 0.0381292	**М == 0.031815**
Р == 0.0321779	**Р == 0.031815**
Л == 0.0320343	**П == 0.031815**
М == 0.0311929	**И == 0.031815**
К == 0.0240719	**Е == 0.025477**
Д == 0.0231484	**Ж == 0.019108**
…	**…**

«Т» –> «О»:

Д ЖОЦ БЦО ЧКЙ ХОЖЙФЬЙССО ХЙОФЙЦСТЙ ХООЕЭЙСМЙ СДР УФМЬПОХа ХИЙПДЦа ЙЗО ИОХЦДЦОЫСО ИПМССЯРОЫЦОЕЯ РОКСО ЕЯПО УФОИЙРОСХЦФМФОЖДЦа ФДЕОЦЧ РЙЦОИДЫДХЦОЦСОЗО ДСДПМЛД

«Д» –> «А»? или «Д» –> «Т»/«С»

А ЖОЦ БЦО ЧКЙ ХОЖЙФЬЙССО ХЙОФЙЦСТЙ ХООЕЭЙСМЙ САР УФМЬПОХа ХИЙПАЦа ЙЗО ИОХЦАЦОЫСО ИПМССЯРОЫЦОЕЯ РОКСО ЕЯПО УФОИЙРОСХЦФМФОЖАЦа ФАЕОЦЧ РЙЦОИАЫАХЦОЦСОЗО АСАПМЛА

Известные союзы и предлоги? «ЖОЦ» –> «ВОТ», «БЦО» –> «ЭТО» и так далее:

А ВОТ ЭТО УЖЕ ХОВЕФЬЕННО ХЕОФЕТНОЕ ХООЕЭЕНМЕ НАМ УФМЬПОХа ХИЕПАТа ЕЗО ИОХТАТОЫНО ИПМННЯМОЫТОЕЯ МОЖНО ЕЯПО УФОИЕМОНХТФМФОВАТа ФАЕОТУ МЕТОИАЫАХТОТНОЗО АНАПМЛА

«ХОВЕФЬЕННО ХЕОФЕТНОЕ» видимо «СОВЕРШЕННО СЕКРЕТНОЕ». Итог:

А ВОТ ЭТО УЖЕ СОВЕРШЕННО СЕКРЕТНОЕ СООБЩЕНИЕ НАМ ПРИШЛОСЬ СДЕЛАТЬ ЕГО ДОСТАТАЧНО ДЛИННЫМ ЧТОБЫ МОЖНО БЫЛО ПРОДЕМОНСТРИРОВАТЬ РАБОТУ МЕТОДА ЧАСТОТНОГО АНАЛИЗА

Усложнение шифра подстановки.

1. Многобуквенная система шифрования (с лозунгом)

РАСКИНУЛОСЬМОРЕШИРОКО

МОНАСТЫРЬМОНАСТЫРЬМОН

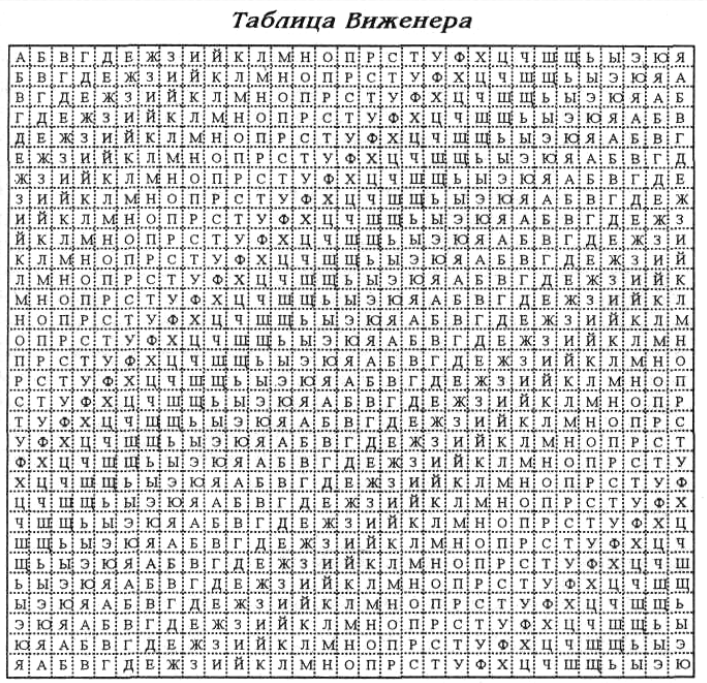
ЭОЯКЩАПЫЙЮЙЩОВЧФШЛЬШЫ

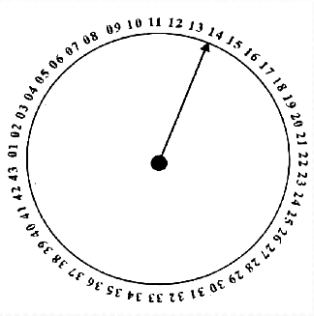
2. Шифр по книге (Шэрлок Холмс).

Страница + Строка

3. Пример нераскрываемого шифра

Блокнот и случайные величины





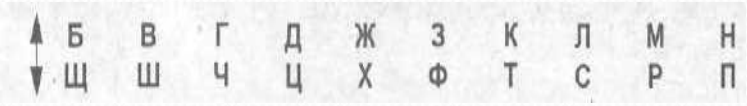
Тайнопись в России.

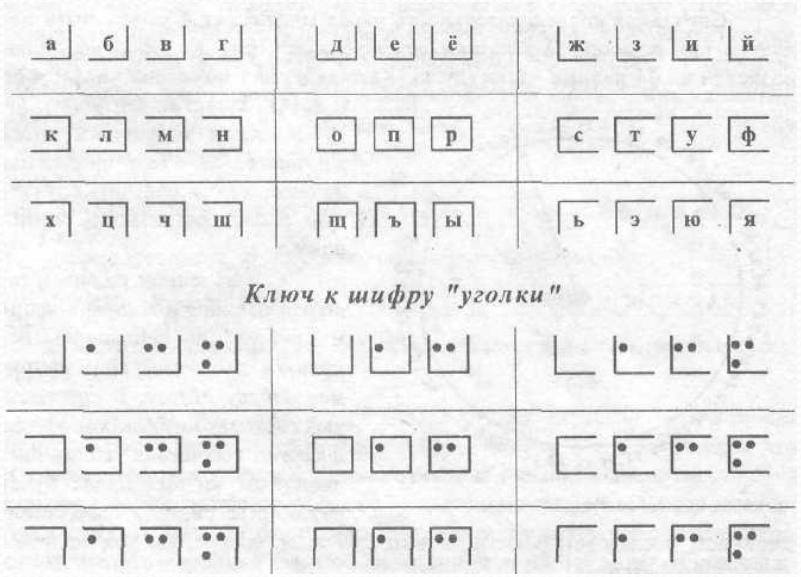
XIII в. –*"тарабарская грамота".*

XVII в. – *Уголки*

Петр I – **"цифирь"** или **"цифирная** азбука".
Особенности.

Елизавета Петровна и Христиан Гольдбах





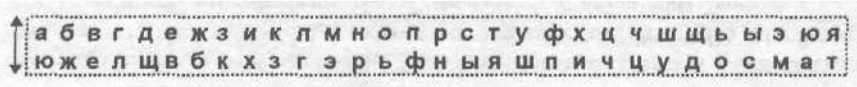
Ключ к шифру "уголки"

Шифры подполья.

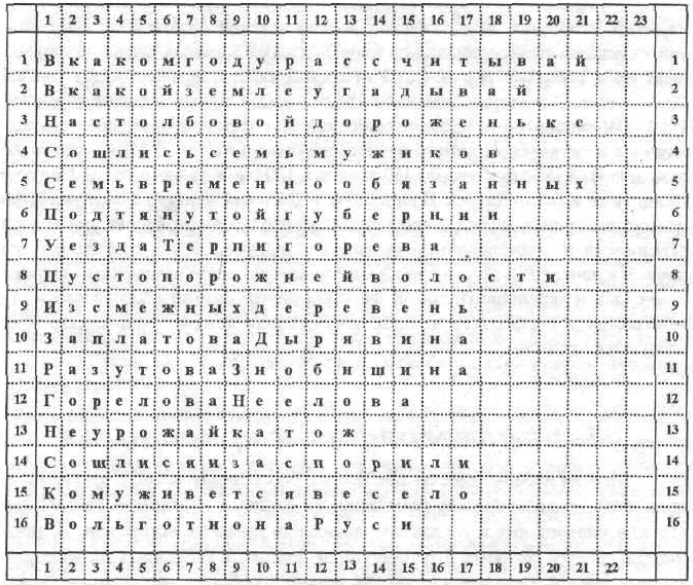
а) *Тюремная азбука* - **аналог** квадрата **Полибия.**

	1	2	3	4	5
1	а	б	в	г	д
2	е	ж	з	и	к
3	л	м	н	о	п
4	р	с	т	у	ф
5	х	ц	ч	ш	щ
6	ь	ы	э	ю	я

б) *Парный шифр,* ключом которого является фраза, содержащая 15 разных букв.



в) Шифр по *стихотворению* – вариант шифра *"по книге"*.



Что-то еще из истории?

Из истории 2 мировой войны.

Опять пример невскрываемого шифра

Иероглифы?

Математика, статистика и логика.

Теория вероятности и математическая статистика – при чем здесь они?

Случайные числа и последовательности:

- Генерация?
- Использование
- Насколько они случайны?

Алгоритмы симметричного шифрования.

Общая схема симметричного шифрования

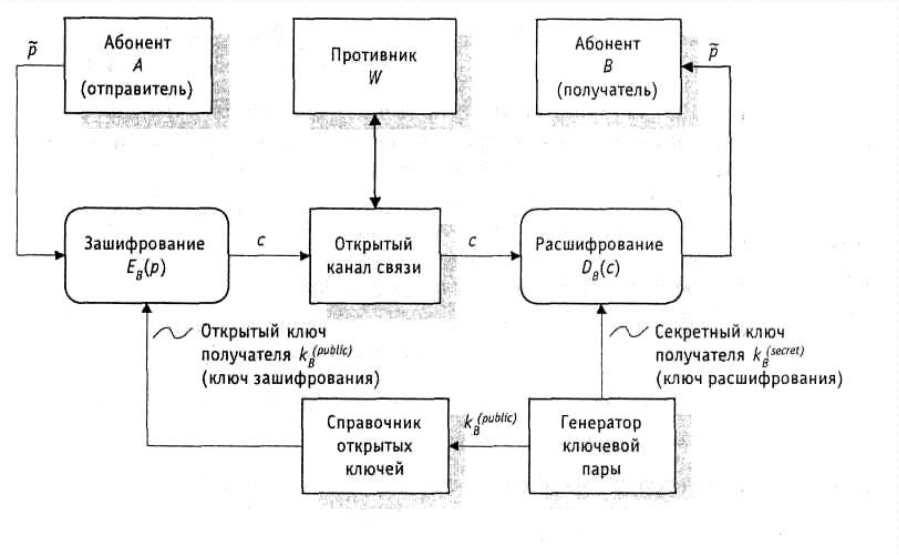
Особенности:

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа

Криптосистемы с открытым ключом.



Открытое распределение ключей.

Криптостойкость, Гибриды.

Хэш функции.

Электронная цифровая подпись.