

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

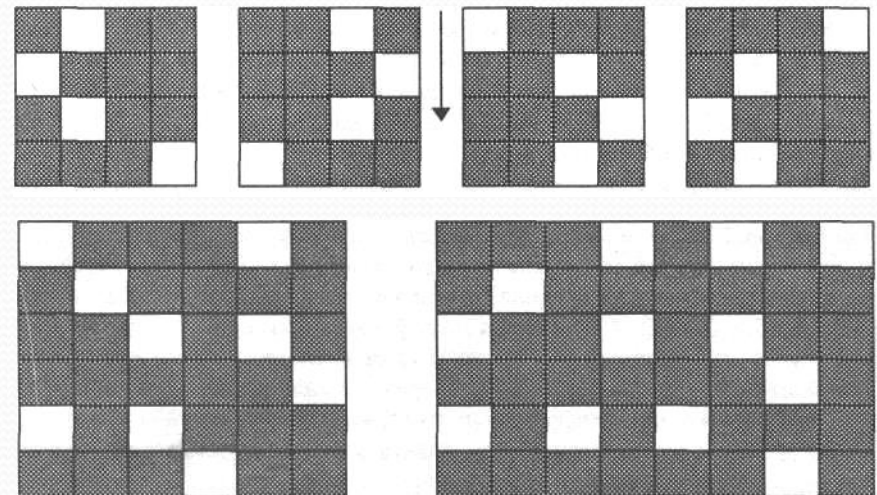
YHQL YLGL YLFL

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 Аль-Ацца*", 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	П == 0.031815
Л == 0.0320343	И == 0.031815
М == 0.0311929	Е == 0.025477
К == 0.0240719	Ж == 0.019108
Д == 0.0231484	...
...	...

«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 УФОИЕМОХТФМФОВАТа ФАЕОТУ
МЕТОИАЫАХТОТНОЗО АНАПМЛА

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

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

Усложнение шифра подстановки.

1. Многобуквенная система шифрования (с лозунгом)

**РАСКИНУЛОСЬ МОРЕ ШИРОКО
МОНАСТЫРЬ МОНАСТЫРЬ МОН**

ЭОЯКЩАПЫЙЮЩОВЧФШЛЬШЫ

2. Шифр по книге (Шэрлок Холмс).

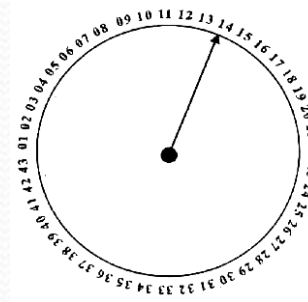
Страница + Строка

3. Пример нераскрываемого шифра

Блокнот и случайные величины

Таблица Виженера

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	Э	Ю	Я
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	Э	Ю	Я	А
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	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	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
Ч	Ш	Щ	Ъ	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
Ш	Щ	Ъ	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
Щ	Ъ	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
Ъ	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
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
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	Э
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	Э	Ю



Тайнопись в России.

XIII в. – *"тарабарская грамота"*.

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

XVII в. – *Уголки*

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

Ключ к шифру "уголки"

┌	•	••	•••	┌	•	••	┌	•	••	•••
┐	•	••	•••	┐	•	••	┐	•	••	•••
└	•	••	•••	└	•	••	└	•	••	•••

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

Елизавета Петровна и Христиан Гольдбах

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.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15				
Ж	Е	Л	З	Н	Ы	Ш	П	И	Ц	Д	О	М	А	Л	Е	Ж	И	Т
Б	В	Г	К	Р	С	У	Ф	Х	Ч	Щ	Ь	Э	Ю	Я				

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	э	ю	я
ю	ж	ел	щ	в	б	к	х	з	г	э	р	ь	ф	н	я	ш	п	и	ч	ц	уд	ос	ма	т				

Пример 1:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ИМОСКВАНЕСР АЗ У СТ РО ИЛ А С Ъ														
↓	А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Э Ю Я													
	Х И Ф Б В Ч С Щ Б Ю Г Ц Д К Ш Ж Э Ъ В А Н Е Р З Я Т Л Ъ													

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

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23		
1	В	к	а	к	о	м	г	о	д	у	р	а	с	с	ч	и	т	ы	в	а	й				1
2	В	к	а	к	о	й	з	е	м	л	е	у	г	и	д	ы	в	а	й						2
3	Н	а	с	т	о	л	б	о	в	о	й	д	о	р	о	ж	е	н	ь	к	е				3
4	С	о	ш	л	и	с	ь	с	е	м	ь	м	у	ж	и	к	о	и							4
5	С	е	м	ь	в	р	е	м	е	н	и	о	о	б	и	з	а	н	и	н	ы	х			5
6	П	о	д	т	я	и	у	т	о	й	г	у	б	е	р	ц	и	и							6
7	У	е	з	д	я	Т	е	р	п	и	г	о	р	е	в	а									7
8	П	у	с	т	о	п	о	р	о	ж	и	е	й	в	о	л	о	с	т	и					8
9	И	з	с	м	е	ж	и	х	д	е	р	е	в	е	н	ь									9
10	З	а	п	л	а	т	о	в	а	Д	ы	р	я	в	и	н	а								10
11	Р	а	з	у	т	о	в	а	З	и	о	б	и	ш	и	н	а								11
12	Г	о	р	е	л	о	в	а	Н	е	л	о	в	а											12
13	Н	е	у	р	о	ж	а	й	к	а	т	о	ж												13
14	С	о	ш	л	и	с	я	и	з	а	с	п	о	р	и	л	и								14
15	К	о	м	у	ж	и	в	е	т	я	в	е	с	е	л	о									15
16	В	о	л	ь	г	о	т	и	о	и	а	Р	у	с	и										16
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22			

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

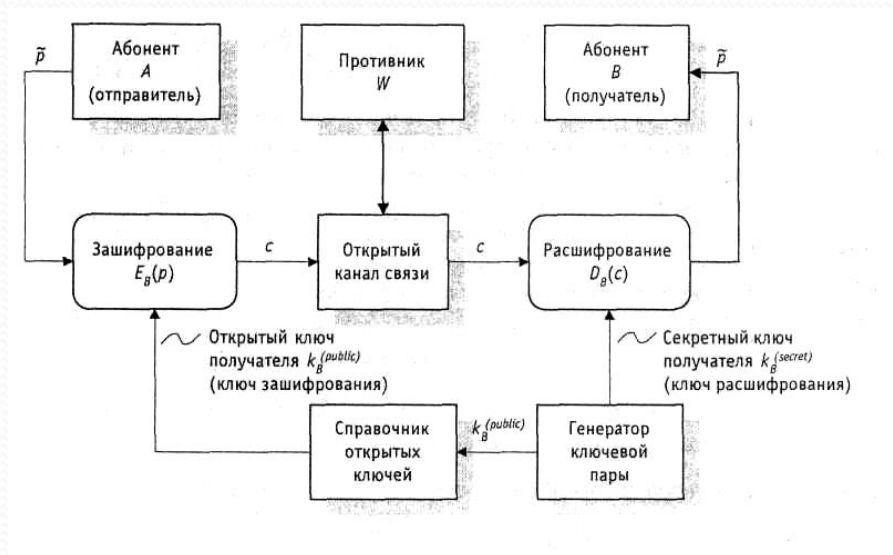
Особенности:

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.