Основы защиты информации

Л10.
Основные понятия криптографии.
Историческая криптография

УИР, ПОИТ, ПМ

Основные понятия

- **Криптография** – наука о сохранении секретности сообщений.
- **Криптоанализ** – наука о методах взлома зашифрованных сообщений.
- **Криптология** – отрасль математики, включающая в себя криптографию и криптоанализ.
- **Криптографический алгоритм** – математические функции, используемые для шифрации и дешифрации.

- Если надежность алгоритма основана на хранении алгоритма в секрете, то такая надежность называется ***ограниченной*** *(очень легко ломается).*
- Для секретности все современные алгоритмы используют *ключ (обозначим его k).*
- *Набор* возможных значений ключа – *пространство ключей (keyspace).*

Основная задача криптографии – сохранить исходный текст от противника

$E_k(p) = c$ $D_k(c) = p$	$E_{k_1}(p) = c$ $D_{k_2}(c) = p$
Алгоритмы с симметричным ключом	Алгоритмы с открытым ключом

Атака – это попытка криптоанализа.
Успешная атака – **метод**.
Атака предполагает знание криптографического алгоритма.

Классическая криптография

- Тайнопись (стеганография) – скрыть **наличие** сообщения:
  - Письма на бритой голове (Гистий, 480 г. д.н.э.
  - Письмена на скорлупе вареного яйца (16 век)
  - Симпатические чернила
  - Микроточка (1940 г.)
  - Марки на почтовых конвертах
- Криптография – скрыть **смысл** сообщения

Шифры замены:
одни буквы заменяются другими

и

Шифры перестановки:
меняется порядок букв

«Штакетник» - шифр перестановки

РАССМОТРИМ ЭТО СООБЩЕНИЕ

⇓

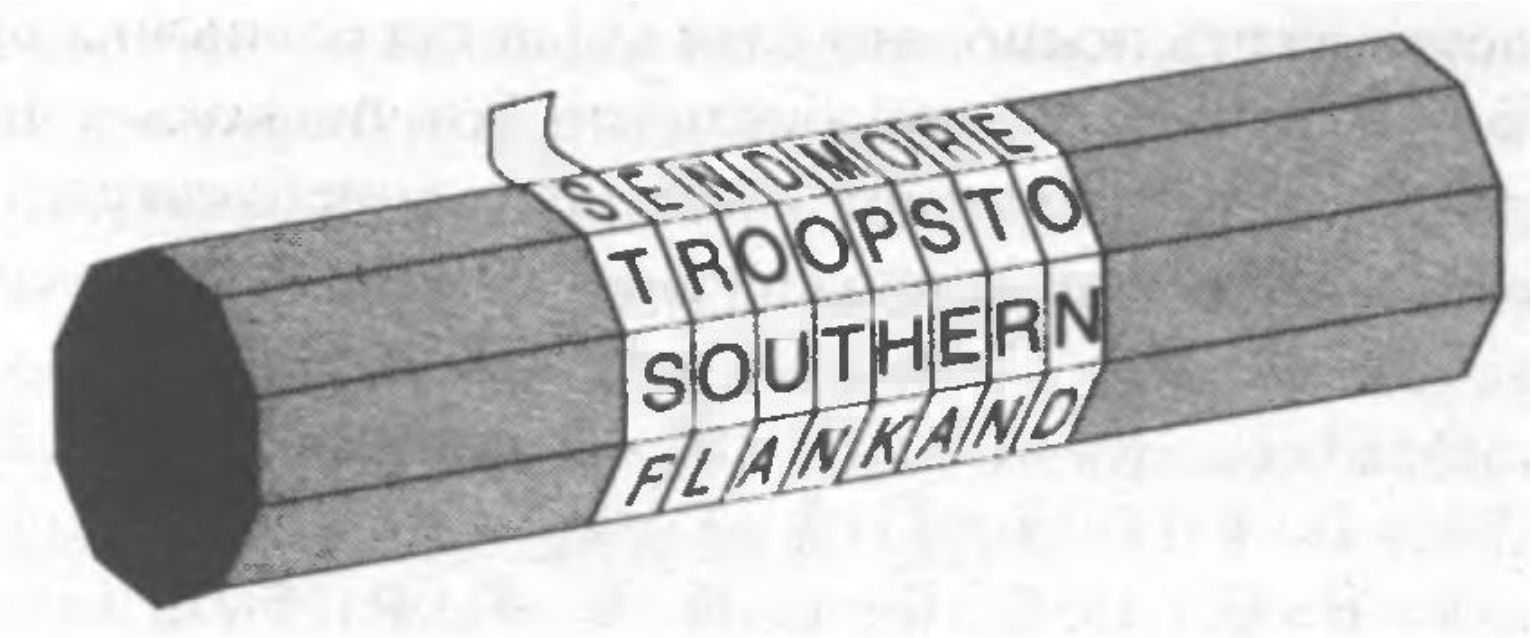
Р С М Т И Т О Б Е И

А С О Р М Э О С О Щ Н Е

⇓

РСМТИ Т ОБЕИАСОРМЭОСОЩНЕ

«Скитала» (5 век д.н.э.) пример стеганографии



STSF…EROL…NOUA…DOTN…MPHK…OSEA

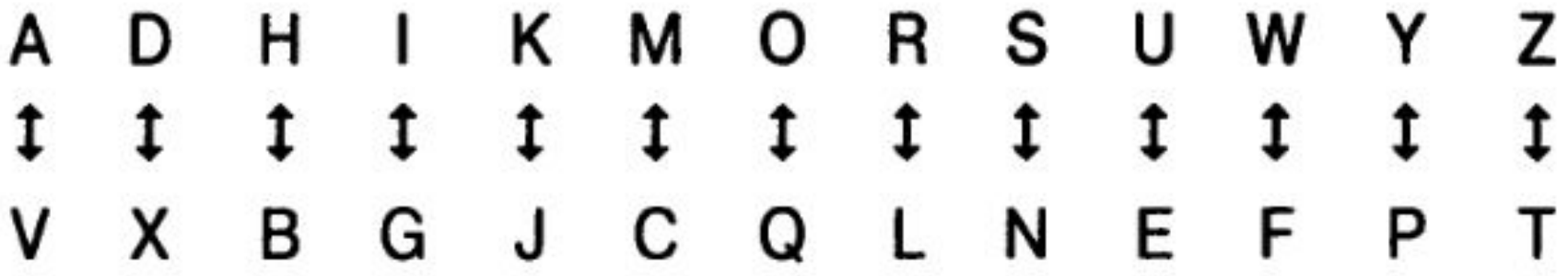
Подстановочные шифры – такие шифры, в которых одни буквы заменяются на другие

- **4 типа подстановочных шифров:**

1. **простая перестановка** (одноалфавитный шифр замены: каждая буква заменяется единственной буквой, разные буквы - разными);
2. **многоалфавитная подстановка** (несколько постановок шифров, например, в зависимости от номера буквы в тексте);
3. **гомофоническая подстановка** (одной букве могут соответствовать несколько различных значений: “A” → 5, 13, 25, 56; “B” → 7, 19, 31, 42 …);
4. **полиграммный шифр** (шифрование группами “ABA” → “RTQ”, “ABB” → “SLL”)

Простая подстановка

Одно из достоинств женщины, согласно восточным учениям, - владение тайнописью



MEET AT MIDNIGHT –> CUUZ VZ CGXSGIBZ

Шифр Цезаря. Сдвиг алфавита

Алфавит открытого текста

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

Шифралфавит

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

Исходный текст

veni, vidi, vici

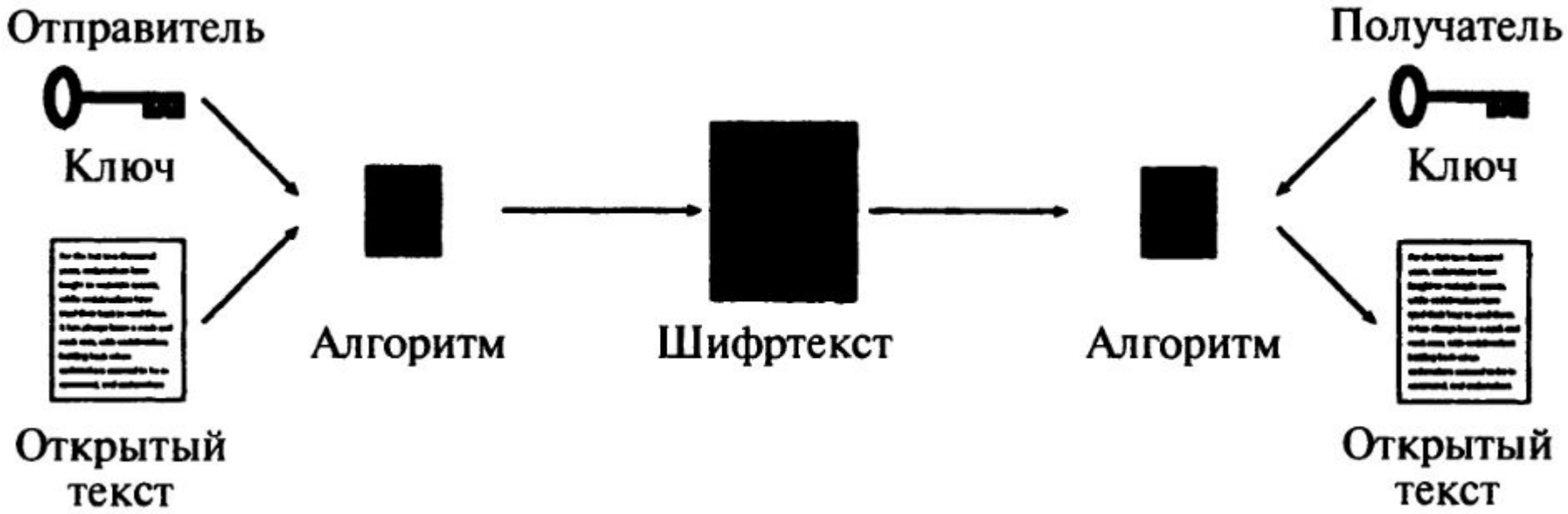
Зашифрованный текст

YHQL, YLGL, YLFL

Стойкость шифров замены = количеству возможных ключей

- Шифр Цезаря:
  - для 26 букв -> 26 сдвигов алфавита = 26 ключей = 26 различных шифров
- Шифр простой перестановки:
  - для 26 букв = 26! перестановок = 403 291 461 126 605 635 584 000 000 различных шрифтов

Проблема передачи ключа



- **ключ** определяет шифроалфавит
- Противник знает алгоритм, но не знает ключ
- Проблема –
  1. хранить ключ в секрете
  2. Передать ключ получателю шифротекста

Закон Керкхоффа

- **Секретность ключа** является основным принципом криптографии

- «**Стойкость криптосистемы** не должна зависеть от стойкости криптоалгоритма. Она зависит от **стойкости ключа**»

Огюст Керкхофф.
Военная криптография.1883 г.

1. Ключ должен держаться в секрете
2. Должен быть широкий выбор ключей

3. Как передавать ключ?

Пример усиления ключа Ключевая фраза

JULIUS CAESAR -> JULISCAER

Алфавит открытого текста

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

Шифроалфавит

JULISCAERTVWXYZBDFGHKMNOPQ

Взлом алгоритмов шифрования. Частотный анализ

На основе анализа отрывков из статей и романов (100 362 знака)

Буква	Частота появления (%)	Буква	Частота появления (%)
a	8,2	n	6,7
b	1,5	o	7,5
c	2,8	p	1,9
d	4,3	q	0,1
e	12,7	r	6,0
f	2,2	s	6,3
g	2,0	t	9,1
h	6,1	u	2,8
i	7,0	v	1,0
j	0,2	w	2,4
k	0,8	x	0,2
l	4,0	y	2,0
m	2,4	z	0,1

Частотный анализ пригоден для

- длинных текстов
- «стандартного» содержания

2. «From Zanzibar to Zambia and Zaire, ozone zones make zebra run zany zigzags»
3. 1969 г. Жорж Перек. «Исчезновение» («La Disparition»). Роман. 200 стр. Без буквы «е»
4. Гилберт Адэр. «A Void». Перевод с фр. на англ. Без буквы «е» !!!

Криптоанализ текста

- Английский текст, одноалфавитный шифр замены, ключ неизвестен

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXB-
JYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP
KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV
LBO DJCMPV ZOICJO BYS, KXUYPD: 'DJOXL EYPD, ICJ X LBCMKX-
PV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO
IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK.
SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOK-
LU?'

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Частотный анализ сообщения O,X,P – более 30 раз. Это - e,t,a?

Буква	Частота появления букв	
	Сколько раз встречается	Частота появления (%)
A	3	0,9
B	25	7,4
C	27	8,0
D	14	4,1
E	5	1,5
F	2	0,6
G	1	0,3
H	0	0,0
I	11	3,3
J	18	5,3
K	26	7,7
L	25	7,4
M	11	3,3

Буква	Частота появления букв	
	Сколько раз встречается	Частота появления (%)
N	3	0,9
O	38	11,2
P	31	9,2
Q	2	0,6
R	6	1,8
S	7	2,1
T	0	0,0
U	6	1,8
V	18	5,3
W	1	0,3
X	34	10,1
Y	19	5,6
Z	5	1,5

Проанализировать частоту появления O,X,P рядом с другими буквами

- Гласная – рядом практически с любой буквой
- Согласная – только рядом с некоторыми

	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
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

- => O,X – вероятно гласные «e», «a»
- P – согласная «t» (но это спорно)

- Сочетание «OO» - 2 раза, «XX» - 0 раз
- Т.к. в англ. «ее» встречается чаще «аа», то предположим, что O – **e**, X – **a**
- Однобуквенные слова (их только 2): «a» и «i». В тексте: «X» и «Y». => Y – **i**
- **!!! Это из-за пробелов все так просто !!!**
- Буква «h» часто перед «e» (the, then, they …), и почти никогда после. => B - **h**

	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
после **O**	1	0	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
перед **O**	0	9	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

Самые частовстречающиеся 3-х буквенные слова – **the** и **and. Lhe** – 6 раз, **aPV** – 5 раз

=> L – **t**, P – **n**, V - **d**

PCQ VMJiPD LhiK LiSe KhahJaWaV haV ZCJPe EiPD KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV liJKL PiDhL, QheP Khe haV ePVeV Lhe LaRe CI Sa'aJMI, Khe JCKe aPV EiKKev Lhe DJCMPV ZeICJe hiS, KaUiPD: 'DJeaL EiPD, ICJ a LhCMKaPV aPV CPe PiDhLK i haNe ZeeP JeACMPLiPD LC UCM Lhe laZReK CI FaKL aDeK aPV Lhe ReDePVK CI aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a laNCMJ CI UCMJ SaGeKLU?'

eFiRCDMe, laReK UCS Lhe LhCMKaPV aPV CPe PiDhLK

Cn -> C – гласная. «o» или «u». **o.** Khe -> K – **s**
thuMsand and one niDhts **- 1001 ночь**
M – u, I – f, J – r, D – g, R – I, S - m

nCQ dMJinD thiK tiSe KhahJaWad had ZCJne EinD KhahJiUaJ thJee KCnK. Cn the thCMKand and liJKt niDht, Qhen Khe had ended the taRe CI Sa'aJMI, Khe JCKe and EiKKed the DJCMnd ZelCJe hiS, KaUinD: 'DJeat EinD, ICJ a thCMKand and Cne niDhtK i haNe Zeen JeACMntinD tC UCM the laZReK CI FaKt aDeK and the ReDendK CI anAient EinDK. SaU I SaEe KC ZCRd aK tC AjaNe a laNCMJ CI UCMJ SaGeKtU?'

eriRCDMe, laRek IJCS the thCMKand and Cne niDhtK

- Ключевая фраза:
  - A VOID BY GEORGES PEREC
  - AVOIDBYGERSPC

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

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

Now during this time Shahrazad had borne King Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: «Great King, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favor of your majesty?»

Epilogue, *Tales from the Thousand and One Nights**

«А Шахразада за это время родила царю Шахрияру трех сыновей. На тысячу и первую ночь, когда она закончила рассказ про Маруфа, она поднялась на ноги и, поцеловав землю перед ним, сказала: «О великий царь, вот уже тысяча ночей и одна ночь, как я передаю тебе рассказы о прошлом и легенды о древних царях. Есть ли у меня право перед твоим величеством, чтобы я могла пожелать от тебя желания?»

Эпилог, *«Тысяча и одна ночь»*.

Повышение стойкости одноалфавитных шрифтов

- Добавление «пустых» символов
- Преднамеренные ошибки в тексте
- Кодирование слов

убить	**= D**	**генерал**	**= Σ**	**немедленно**	**= 08**
шантаж	**= P**	**король**	**= Ω**	**сегодня**	**= 73**
захватить	**= J**	**министр**	**= Ψ**	**сегодня вечером**	**= 28**
защитить	**= Z**	**принц**	**= Θ**	**завтра**	**= 43**

Убить короля сегодня вечером

D-Ω-28

Направления «тайнописи»

- Коды – нужны «кодовые книги»

Двойной шифралфавит

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

!!! Одинаковые буквы открытого текста
не обязательно будут одинаковыми в шифротексте

- Четные буквы – 1-м шифром, нечетные – 2-м

hello -> AFPAD

Многоалфавитные шрифты. Квадрат Вижинера (1586 г.)

- Для шифрования используются 26 шифралфавитов
- Буква сообщения может быть зашифрована **любой** строкой квадрата
- Использует ключевое слово для выбора шифралфавита

Открытый алфавит	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Пример использования квадрата Вижинера

- Ключевое слово **WHITE**

Ключевое слово	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I	
Исходный текст сообщения	d	i	v	e	r	t	t	r	o	o	p	s	t	o	e	a	s	t	r	i	d	g	e	
Зашифрованный текст сообщения	Z	P	D	X	V	P	A	Z	H	S	L	Z	B	H	I	W	Z	B	K	M	Z	N	M	

- **d** кодируется строкой квадрата, которая начинается в буквы **W**
- Неуязвим для частотного анализа

Гомофонические шрифты

Букве – количество чисел, пропорциональное ее частоте

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	42						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Шифры гаммирования

- Наложение и снятие гаммы

	3425	7102	8139		9838	3515	4552
+	6413	6413	6413	−	6413	6413	6413
	9838	3515	4552		3425	7102	8139

- X = (Символ + Гамма) mod 26

A	**B**	**C**	**…**	**X**	**Y**	**Z**
0	**1**	**2**	**…**	**23**	**24**	**25**

И т.д.

Много разных и интересных исторических шифров

https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema5

Абсолютно стойкие системы шифрования

Абсолютно стойкие системы шифрования. Требования:

1. Ключ генерируется для каждого сообщения (каждый ключ используется один раз)
2. Ключ статистически надёжен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны)
3. Длина ключа равна или больше длины сообщения
4. Исходный (открытый) текст обладает некоторой избыточностью (является критерием оценки правильности расшифровки)

Абсолютно стойкие системы шифрования

1. Стойкость этих систем **не зависит** от того, какими вычислительными возможностями обладает криптоаналитик.
2. Практическое применение ограничено соображениями стоимости и удобства пользования (передача шифроблокнота).
3. Некоторыми аналитиками утверждается, что Шифр Вернама является одновременно абсолютно криптографически стойким и к тому же единственным шифром, который удовлетворяет этому условию.

Шифр Вернама

- Для создания шифротекста открытый текст объединяется операцией «исключающее ИЛИ» с ключом (называемым одноразовым блокнотом или шифроблокнотом).

- При этом ключ должен обладать тремя критически важными свойствами:
  - быть истинно случайным;
  - совпадать по размеру с заданным открытым текстом;
  - применяться только один раз.

1917 год. Шифроблокноты к шифру Виженера. Джозеф Моборн и Гильберт Вернам

- «attack the valley at dawn» «нападите на долину на рассвете»: 26^{21} вариантов кодировки
  518 131 871 275 444 633 654 274 293 760

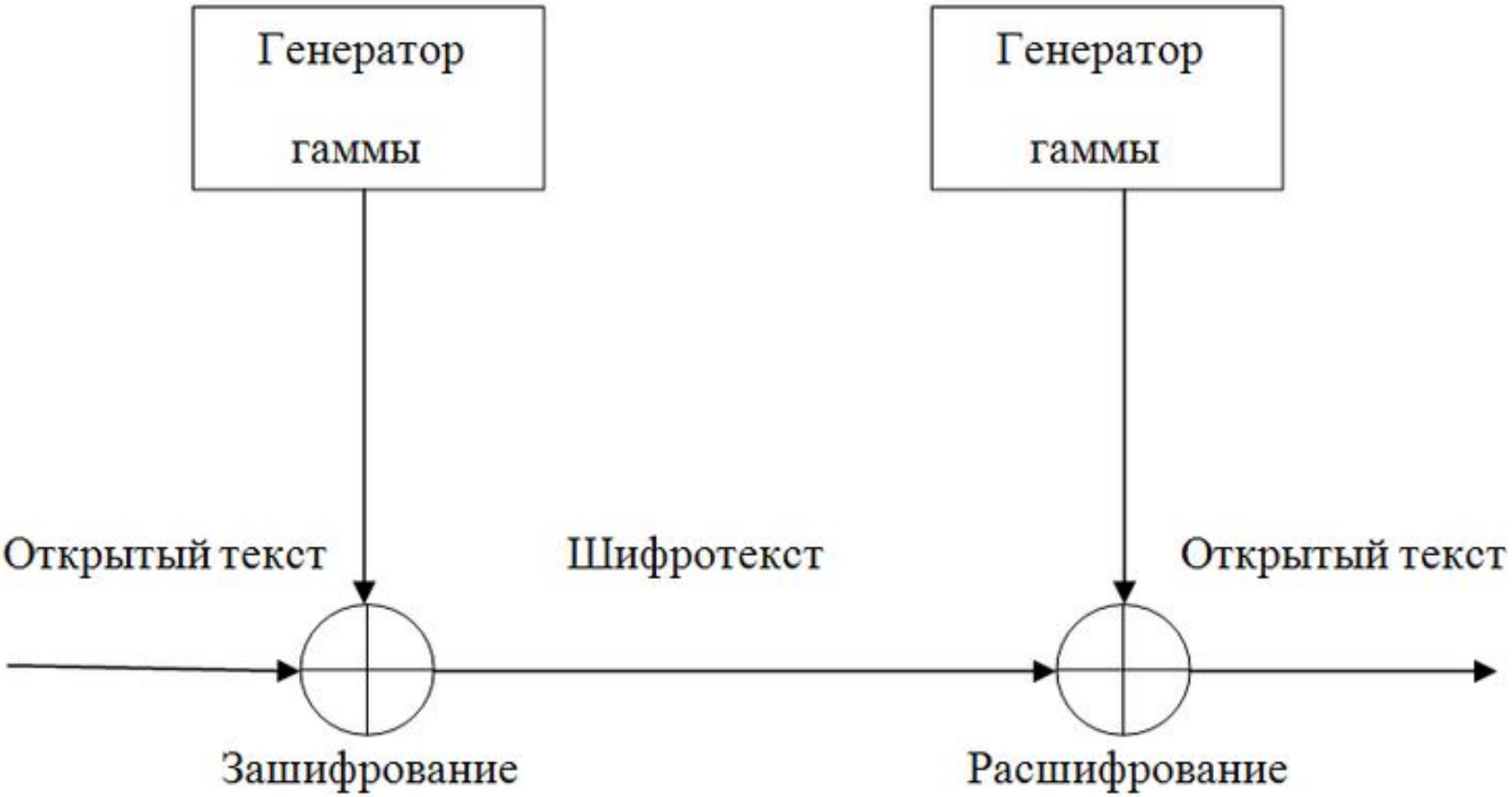
Лист 1				
P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Лист 2				
O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

Лист 3				
J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

Ключ	P	L	M	O	E	Z	Q	K	J	Z	L	R	T	E	A	V	C	R	C	B	Y
Открытый текст	a	t	t	a	c	k	t	h	e	v	a	l	l	e	y	a	t	d	a	w	n
Шифртекст	P	E	F	O	G	J	J	R	N	U	L	C	E	I	Y	V	V	U	C	X	L

Реализация шифра Вернама. Поточные системы шифрования



Выводы

- Стойкость системы зависит не от алгоритма, а от стойкости ключа
- Ключ определяет выбор шифралфавита
- Ключ должен быть «случайным»
- Пространство ключей - большим

О частотных характеристиках шифров замены

Шифр простой замены

A – алфавит открытого текста, B – алфавит шифротекста.

#A = #B , алфавиты одного размера

K : A -> B, ключ – перестановка. **К - биекция** – взаимнооднозначное соответствие. E(M,K)=C, D(C,K)=M

Пример.

A = {A,B,C,D,E, …, U,V,W,X,Y,Z}, B = {D,E,F,G,H, …, X,Y,Z,A,B,C }
Шифр Цезаря, ключ – сдвиг на 3 позиции
K = {0,1,2, … , 22,23,24,25} -> {3,4,5, … , 25,0,1,2}

По русски

Каждый символ исходного алфавита может заменяться только одним символом шифроалфавита.

Причем разные символы заменяются разными

Шифр замены (не «простой» !)

A – алфавит открытого текста, B – алфавит шифротекста.

#A ≠ #B, алфавиты могут быть **разного** размера

K : ключ – не перестановка. Задается другим способом

Биекции нет !!!

E(M,K)=C, D(C,K)=M

Пример.

A = B = {A,B,C,D,E, …, U,V,W,X,Y,Z}

Шифр Вижинера, ключ – строка, не перестановка алфавита !!

K = A -> 2^B (Отображение A в множество подмножеств B)

По русски

Каждый символ исходного алфавита может заменяться **различными** символами шифроалфавита.

Причем **разные** символы могут заменяться **одинаковыми**

Шифры исторической криптографии

M = m1 m2 m3 ... m_n

K = k1 k2 k3 ... k_n или **K ∈ 2^ZN**

C = c1 c2 c3 ... c_n

N – размер алфавита

Шифр Цезаря

ci = E(ci, K) = (mi + K) mod N, mi = D(ci,K) = (ci - K) mod N

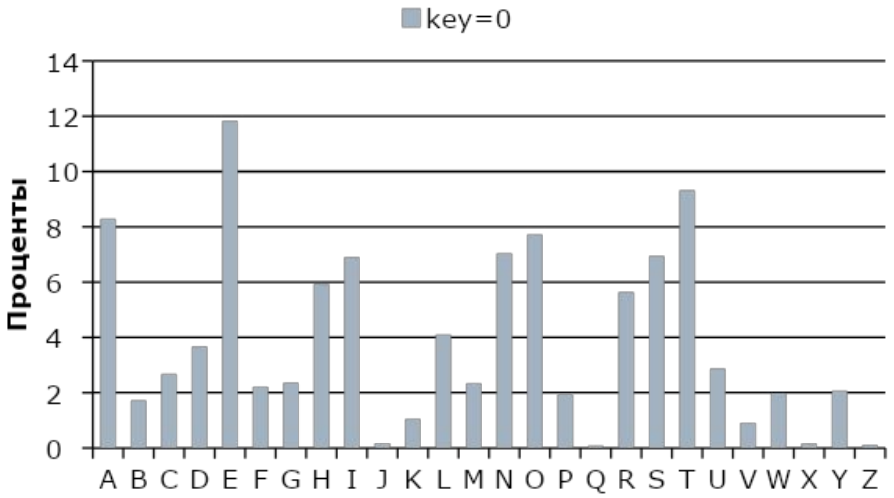
Аффинный шифр Цезаря

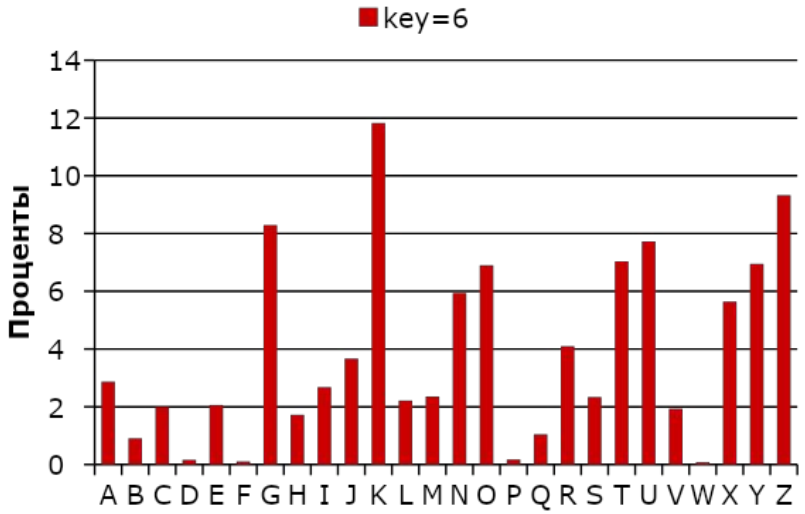
ci = E(ci, (k1,k2)) = (mi + k1)*k2 mod N,
mi = D(ci,(k1,k2)) = (ci*$k2^{-1}$ – k1) mod N

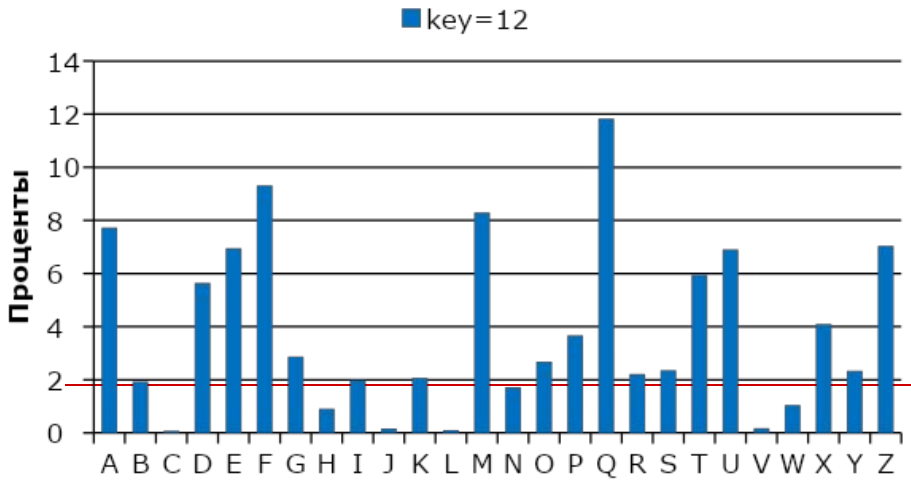
Шифр Вижинера

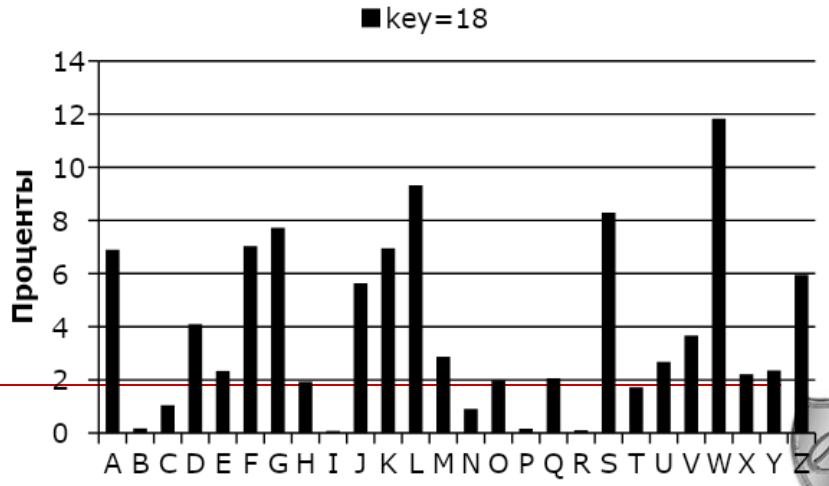
ci = E(ci, ki) = (mi ⊕ ki) mod N, mi = D(ci,ki) = (ci ⊕ ki) mod N

Частотная диаграмма. Нил Стивенсон, «Криптономикон»
2319052 символа, 415784 слова, 22803 различных слова
Шифр Цезаря (key = 0,6,12,18)

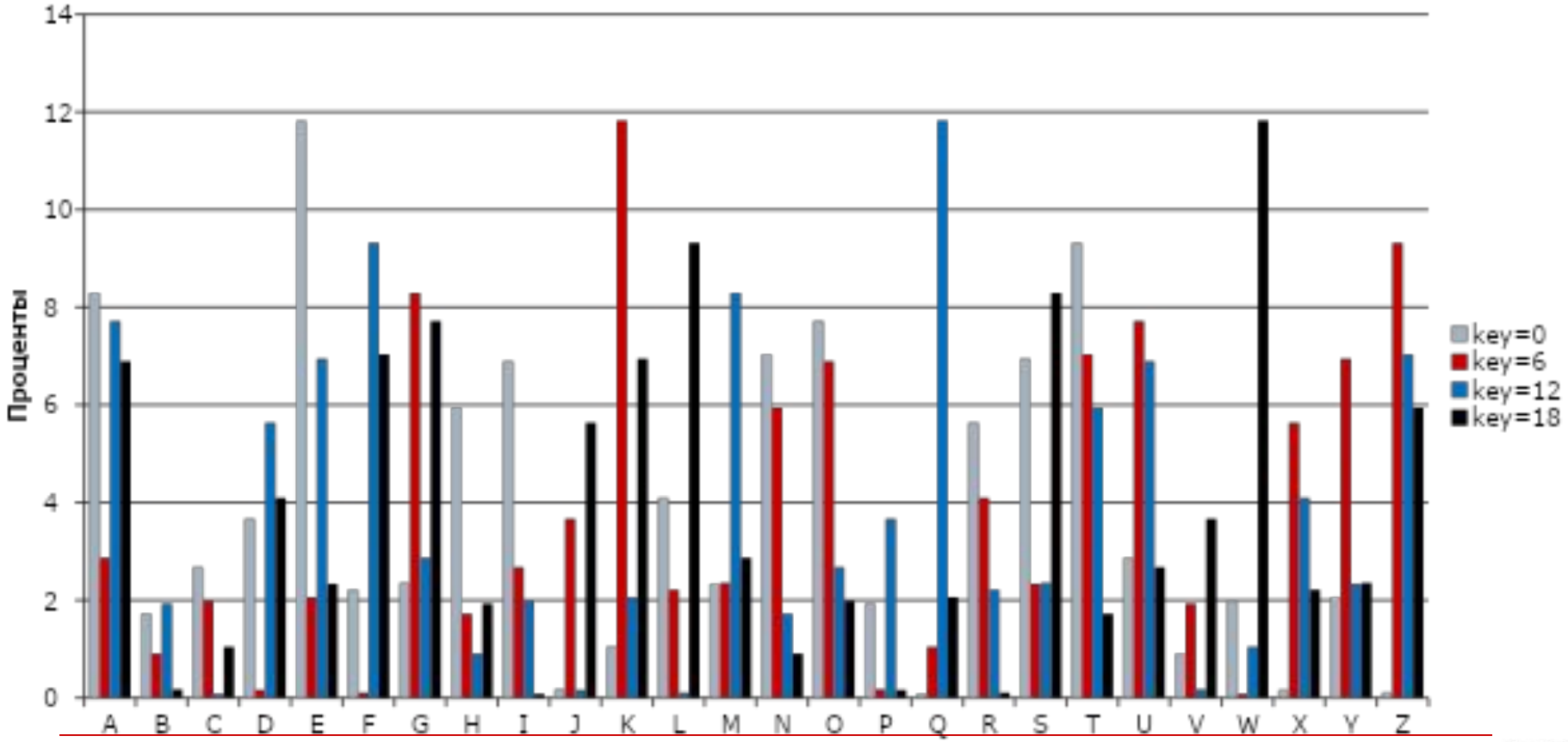




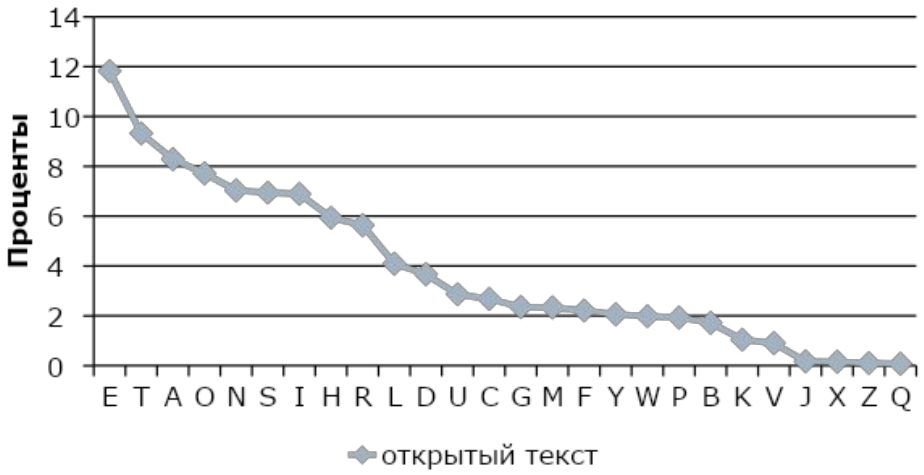


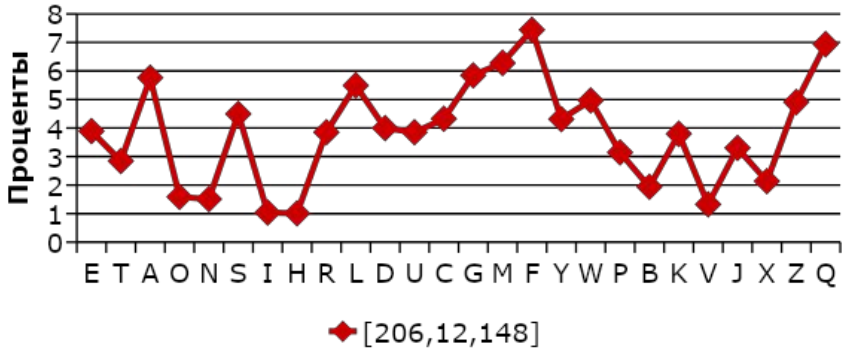


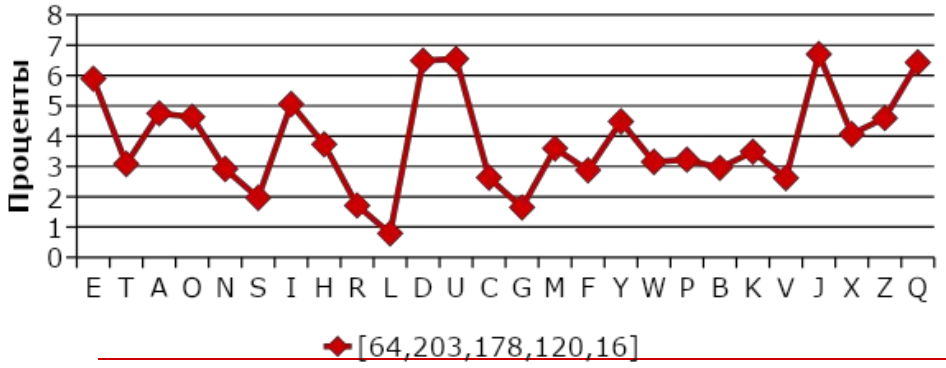
Частотная диаграмма. Нил Стивенсон, «Криптономикон»
2319052 символа, 415784 слова, 22803 различных слова
Шифр Цезаря (key = 0,6,12,18)

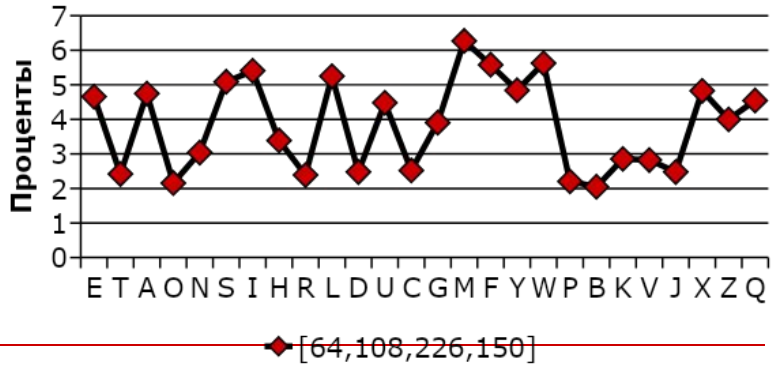


Частотная диаграмма. Нил Стивенсон, «Криптономикон»
2319052 символа, 415784 слова, 22803 различных слова
Шифр Вижинера (key = указан на гафике)

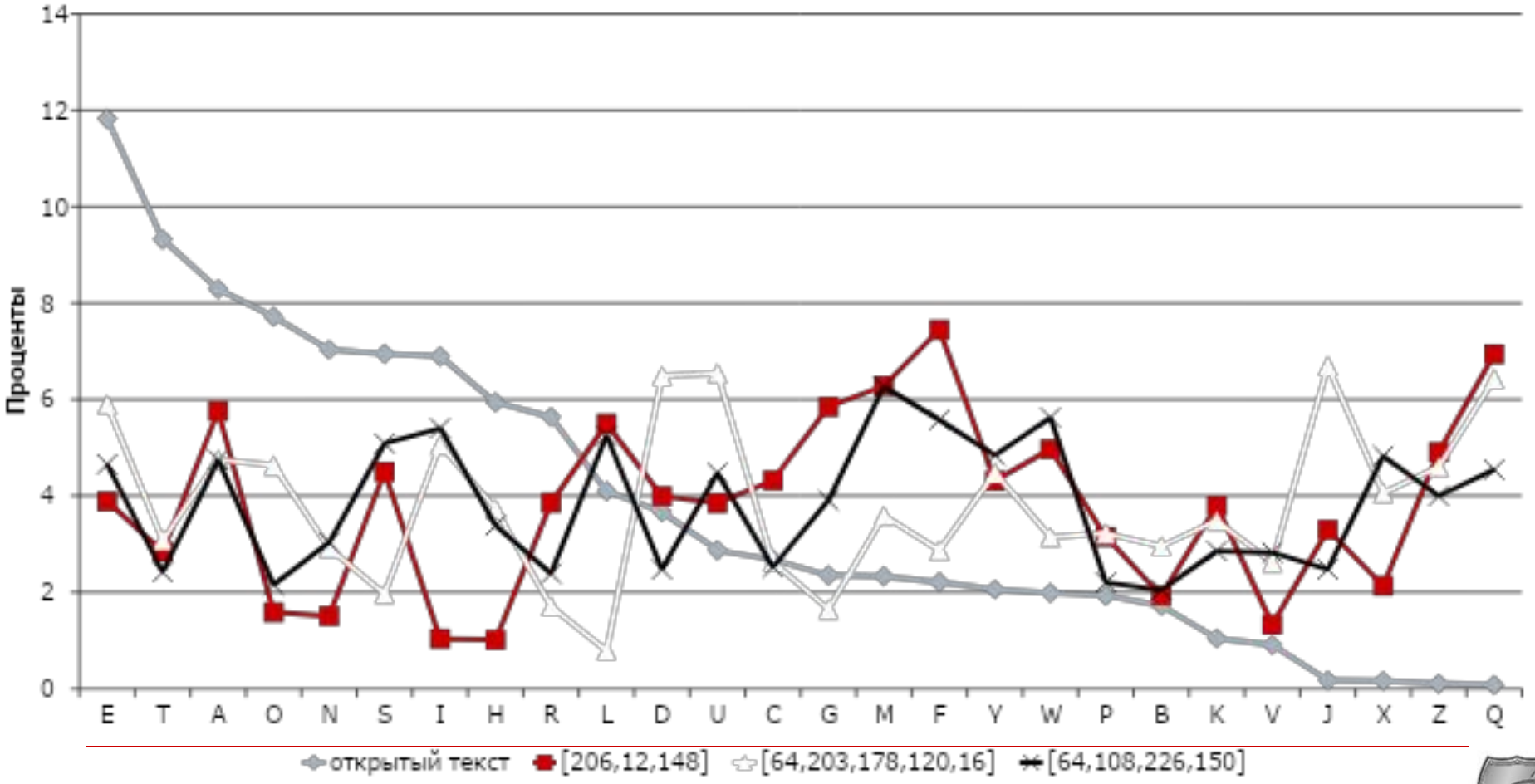






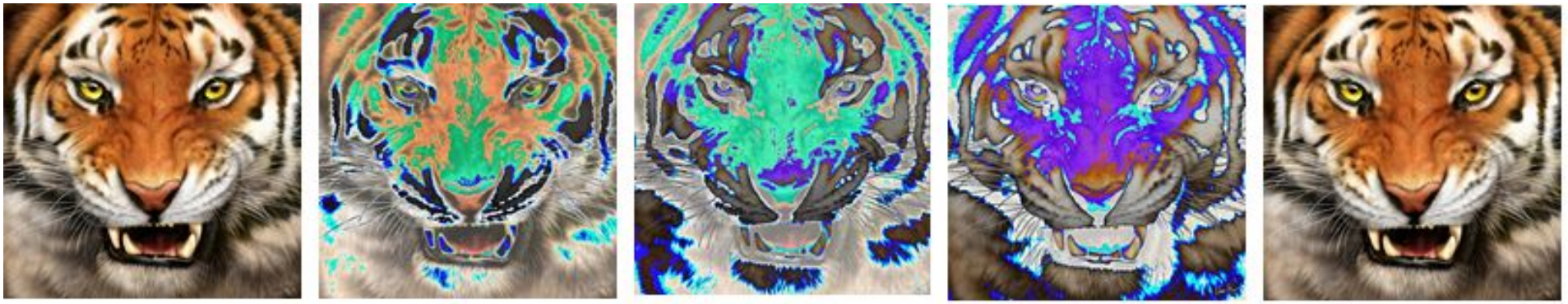


Частотная диаграмма. Нил Стивенсон, «Криптономикон»
2319052 символа, 415784 слова, 22803 различных слова
Шифр Вижинера (key =)



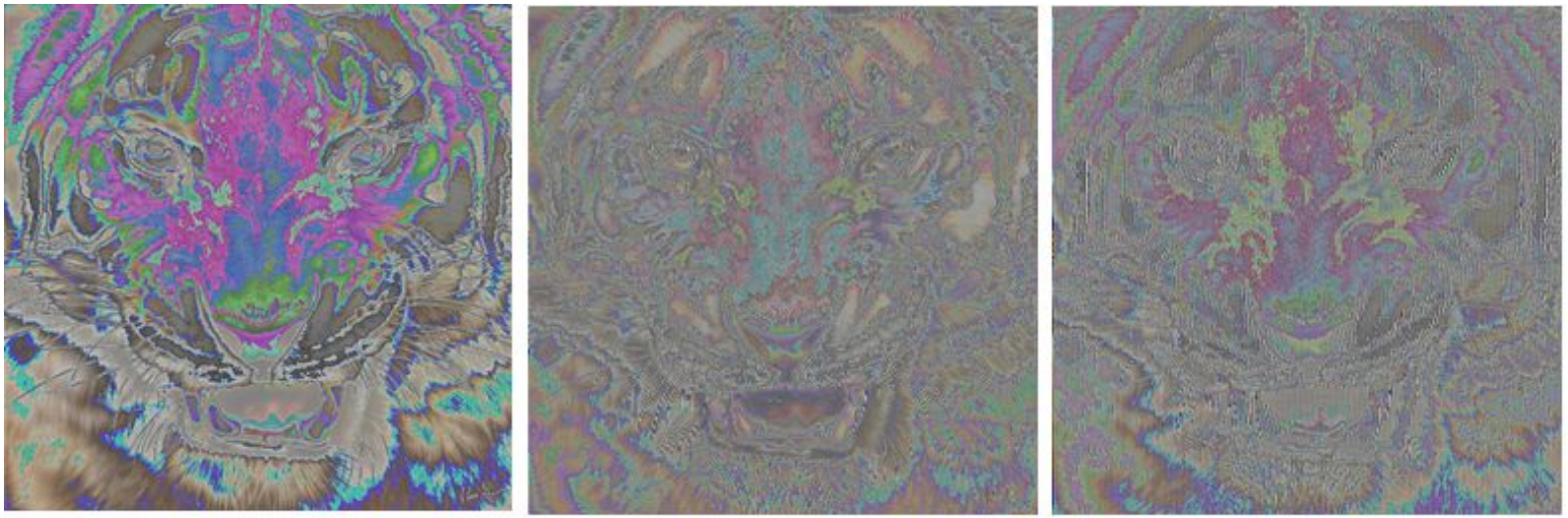
Было понятно, но не выразительно

Попробуем иначе



k : 0 64 128 192 256

Результат шифрования 256-цветного графического файла Tiger.bmp шифром Цезаря с различными ключами k



key: [64,192] [64,128,192,255] [175,234,32,168,61,99]

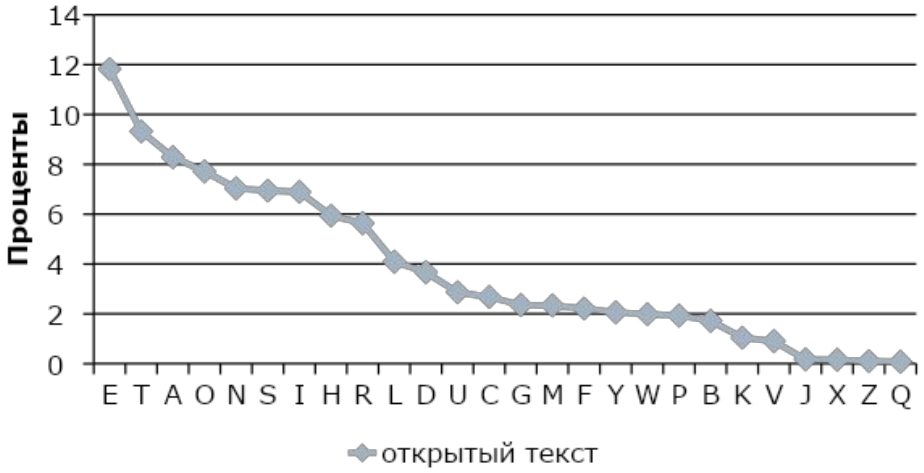
Результат шифрования 256-цветного графического файла Tiger.bmp шифром Виженера с различными ключами key

2 вопроса

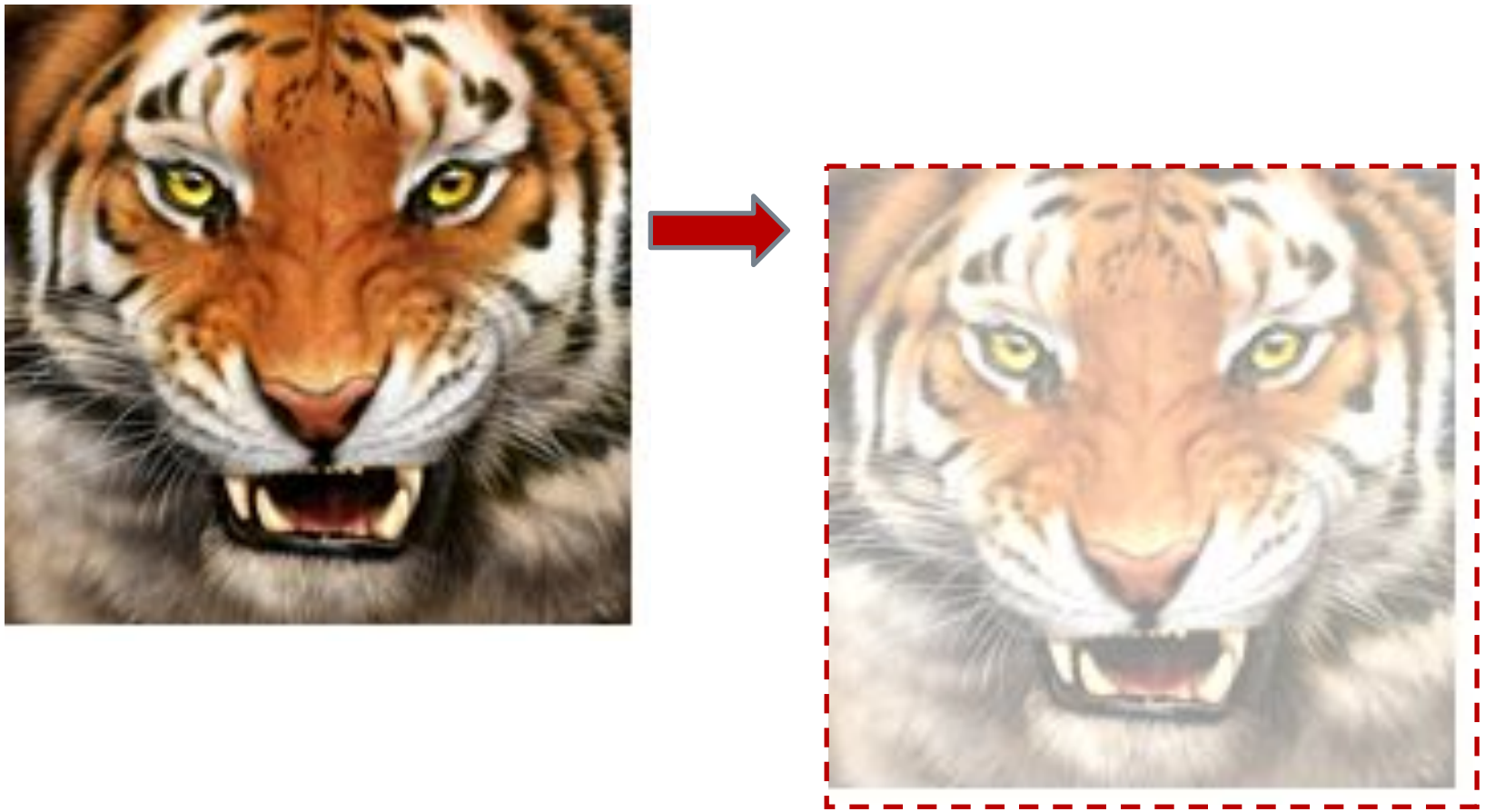
Какой из шифров,
Цезаря или Вижинера,
лучше скрывает исходные данные ?

Почему?

Как вы представляете себе частотные характеристики идеального шифра ????



А при шифровании изображения?



Благодарю за внимание