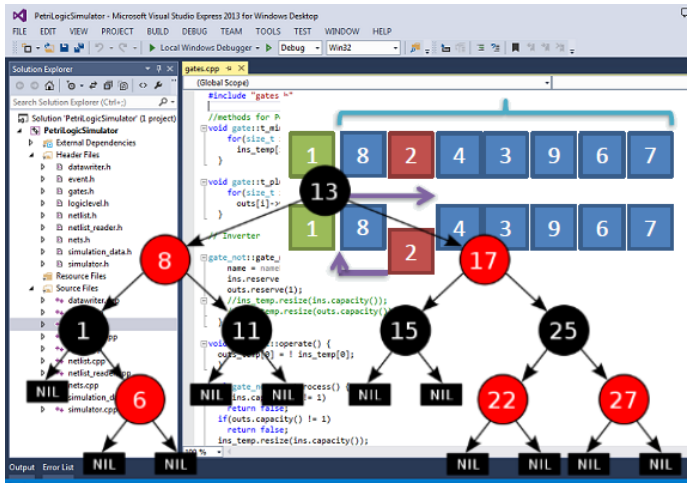
МИЭТ
Национальный исследовательский университет «МИЭТ»
Институт интегральной электроники (группы ЭН-24-25, каф. ПКИМС)

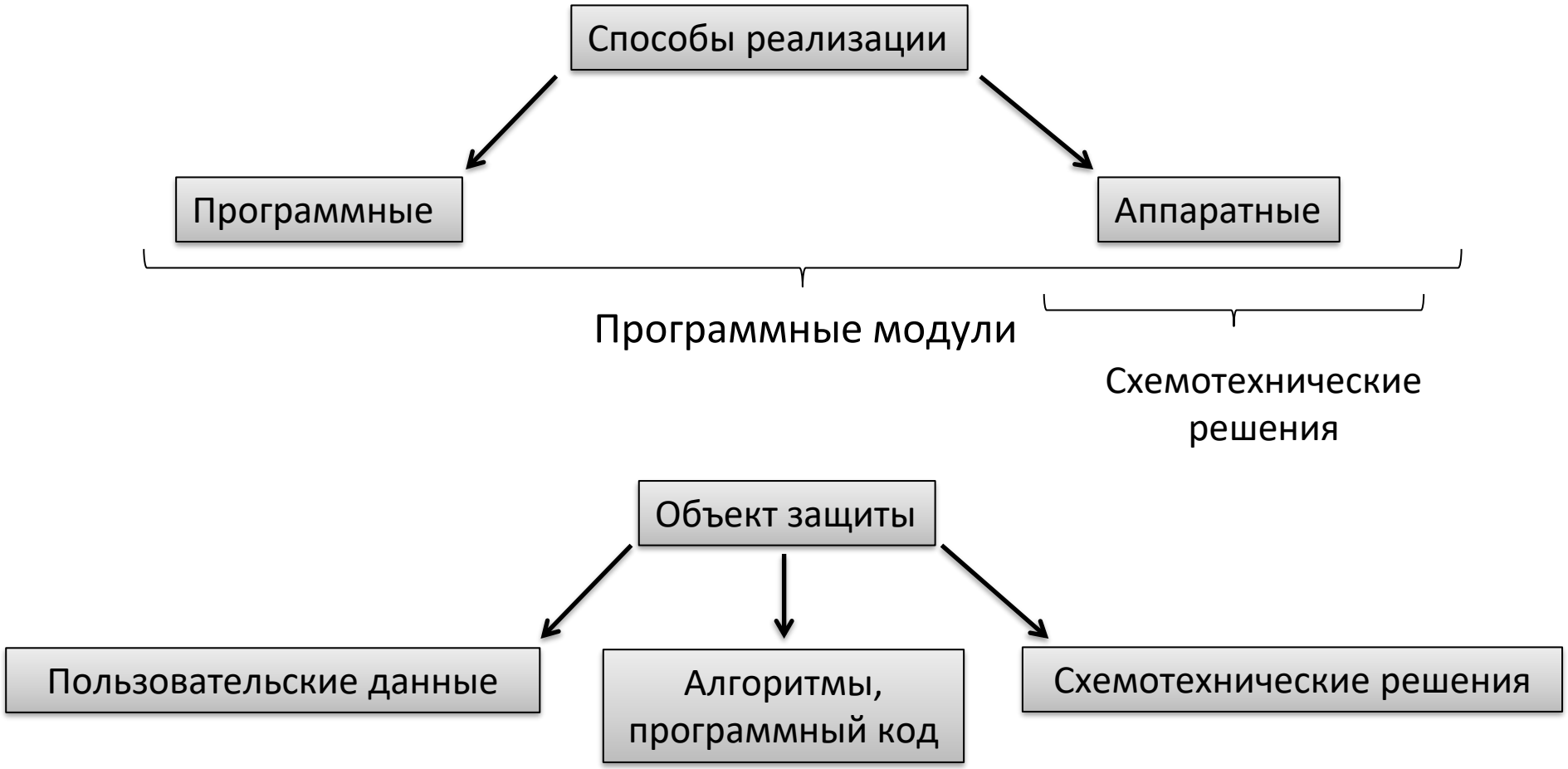
Теория алгоритмов



Лекция 6

Алгоритмические подходы к защите данных

Классификация методов защиты (1)



Квадрат Полибия

Первый шифр, не требующий специальной «аппаратной» составляющей

Полибий
III век до н.э.

	1	2	3	4	5	6
1	**А**	**Б**	**В**	**Г**	**Д**	**Е**
2	**Ё**	**Ж**	**З**	**И**	**К**	**Л**
3	**М**	**Н**	**О**	**П**	**Р**	**С**
4	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**
5	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**
6	**Ю**	**Я**		**!**		

КАФЕДРА ПКИМС РУЛИТ!

↓

25114316153511633425
24313663354226244164

Шифр, с которого начинают все программисты

Самый популярный шифр, не требующий «аппаратной» составляющей?

Гай Юлий Цезарь
I век до н.э.

Характеризуется тем, что имеет
постоянное смещение для каждой буквы

А	**Б**	**В**	**Г**	**Д**
+2				
В	**Г**	**Д**	**Е**	**Ж**

КАФЕДРА ПКИМС РУЛИТ!

↓

МВЦЖЁТВ СМКОУ ТХНКФ!

Шифр Цезаря с ключом: шифр Виженера (1)

Характеризуется тем, что имеет смещение для каждой буквы, равное значению ключа

А	**Б**	**В**	**Г**	**Д**
+АБВ				
Б	**Г**	**Е**	**Д**	**Ж**

Блез де Виженер, 1523-1596
Публикация шифра: 1586

Шифр Цезаря с ключом: шифр Виженера (2)

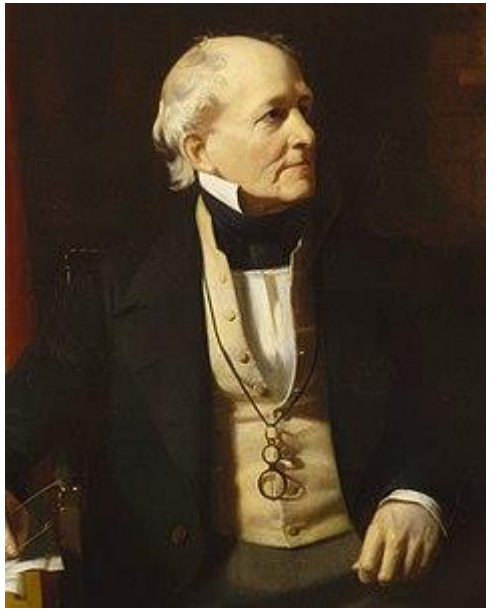
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Блез де Виженер, 1523-1596
Публикация шифра: 1586

PKIMS RULEZ
KEY ↓
ZOGWK PEPCJ

Модификация шифра Виженера: шифр Бофора/Бофорта

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



Сэр Френсис Бофорт
1774-1857

PKIMS RULEZ

KEY ↓

VUEYM HQTUL

Модификация шифра Виженера: шифр Гронсфельда

	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
0	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

Создан графом Гронсфельдом, руководителем дешифровальной службы Германии XVII века

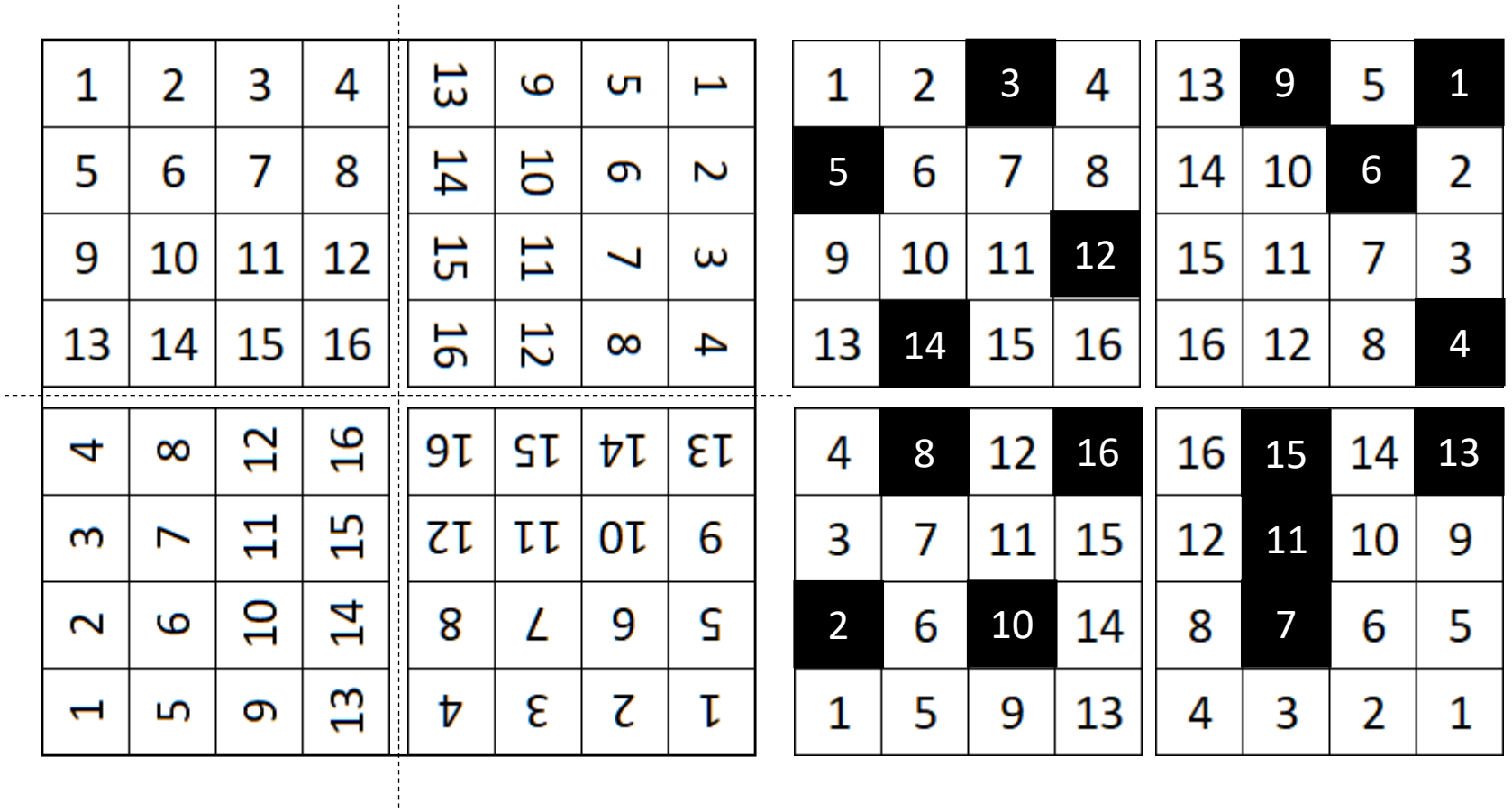
Простая литорея (тарабарский шифр)

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

КАФЕДРА ПКИМС РУЛИТ

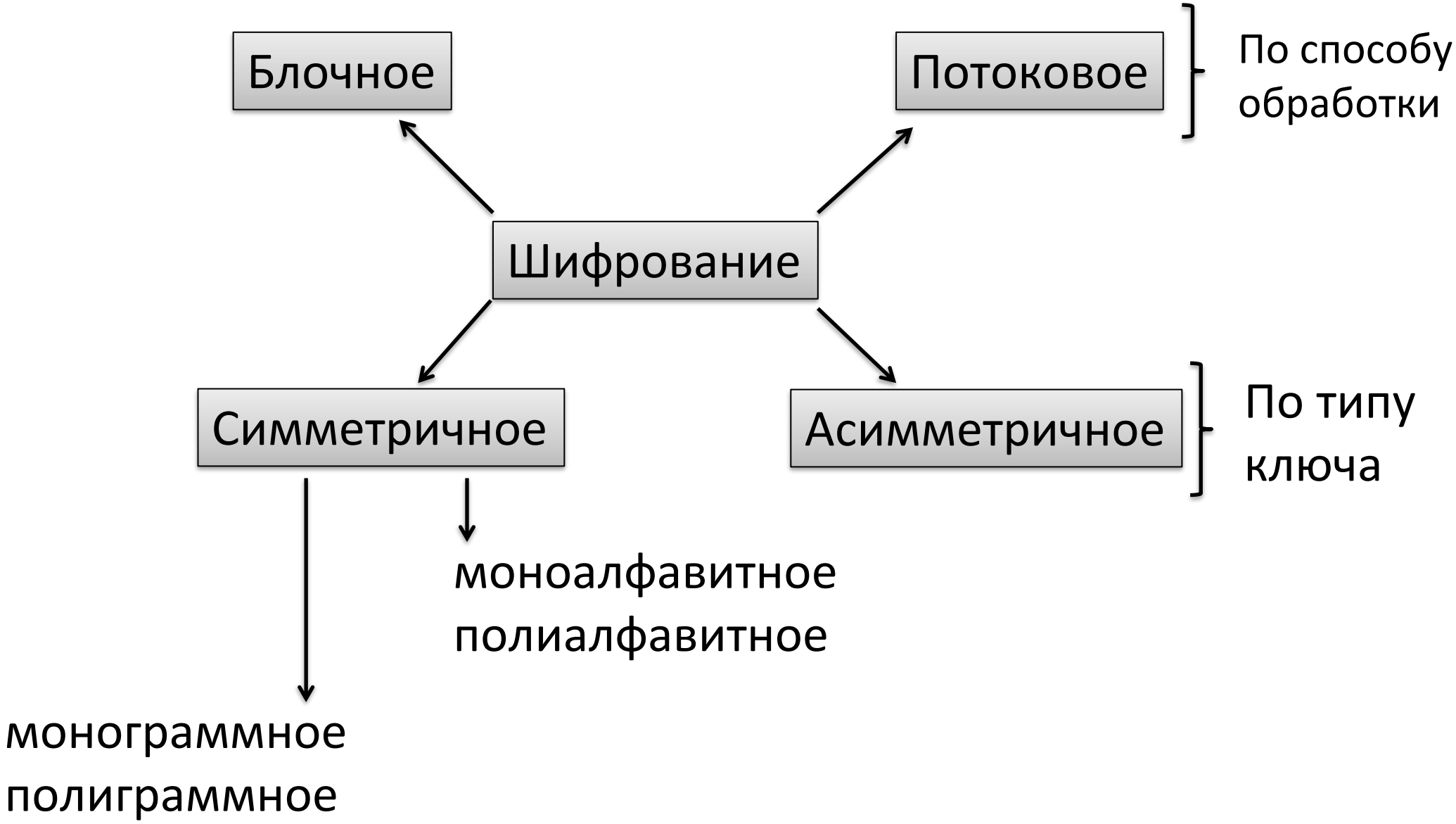
ТАЗЕЦМА НТИРЛ МУСИК

Принцип формирования решётки Кардано



Шаг1. Квадратная область делится на 4 части, каждая из которых делится на 16 клеток.
Шаг 2. Клетки каждого из квадратов последовательно нумеруются числами от 1 до 16.
Шаг 3. Первый квадрат остаётся в неизменном виде, а каждый следующий вращается по часовой стрелке на 90 градусов.
Шаг 4. Произвольным образом в каждом из квадратов выбираются числа от 1 до 16 так, чтобы во всей области была выбрана всего 1 клетка (из 4х квадратов) с этим номером.
Шаг 5. В выбранных клетках записывается текст, остальные клетки заполняются произвольно.

Общая классификация методов программного шифрования



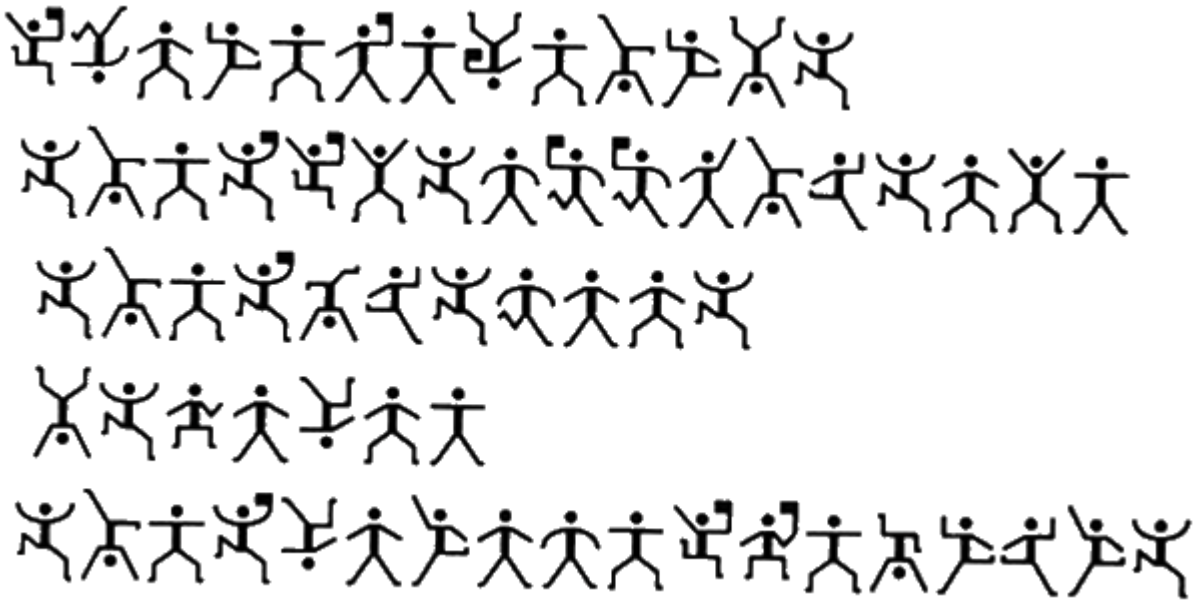
Моноалфавитные моногрaммные шифры

1. Шифры типа алгоритма Цезаря - перестановочные

$$y=f(x, N),\ f(x, N) \rightarrow x(i)+N,$$

$$x(i)*N,\ x(i)\%N$$

2. «Школьные», «книжные» шифры – не реализуемые на ЭВМ



Что такое частотный анализ?

Диаграмма частот использования букв алфавита для Русского языка

Диаграмма частоты использования букв алфавита в Английском языке

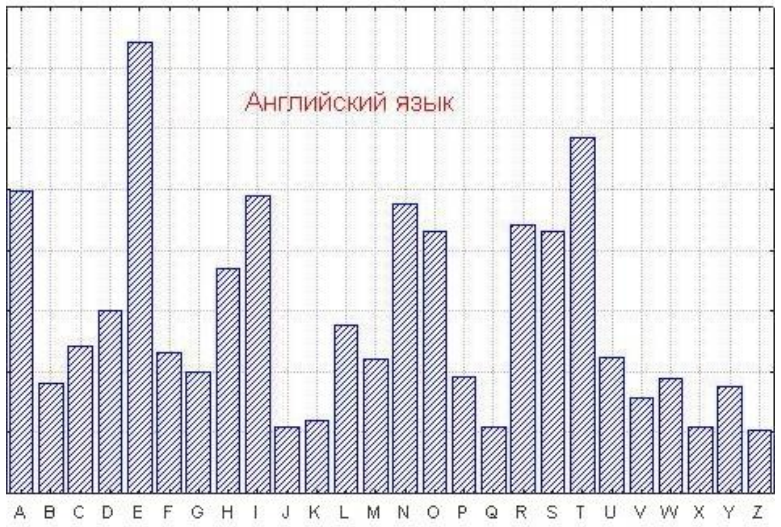
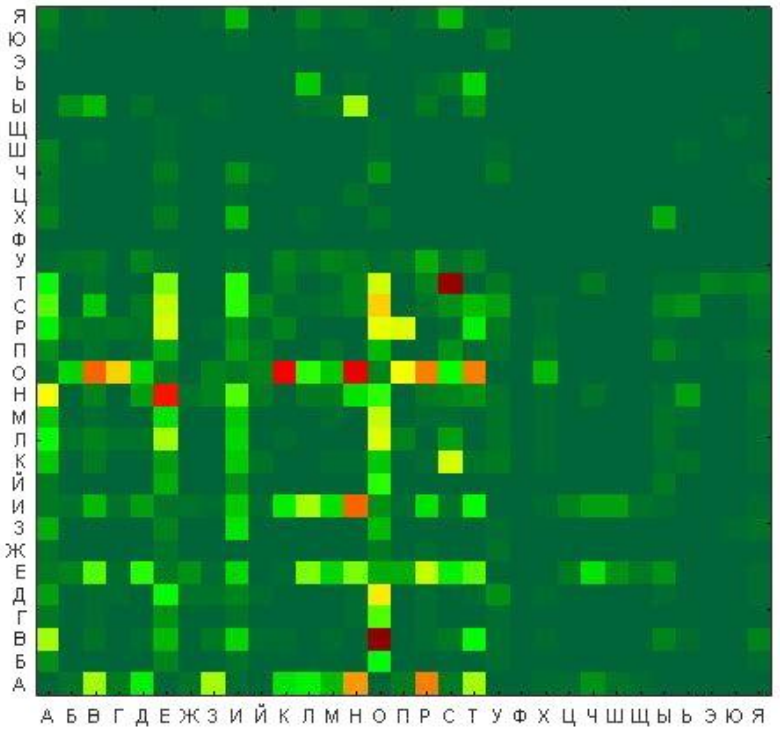
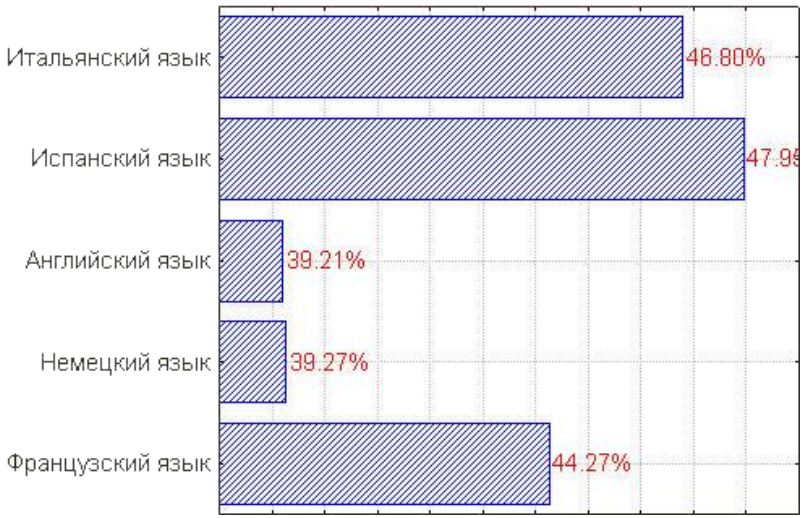


График частот использования пар букв русского алфавита



Доля гласных букв в алфавитах



Полиалфавитные монограммные шифры

Полиалфавитные шифры устраняют некоторые недостатки одноалфавитных шифров

Одноалфавитный	
А	А1
Б	А2
В	А3
Г	А4

Полиалфавитный	
А	А1, А2
Б	А3
В	А4
Г	А5, А6

	1	2	3	4	5	6
1	**А**	**Б**	**В**	**Г**	**Д**	**Е**
2	**Ё**	**Ж**	**З**	**И**	**К**	**Л**
3	**М**	**Н**	**О**	**П**	**Р**	**С**
4	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**
5	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**
6	**Ю**	**Я**		**!**		

25114316153511633425243136663542262441 64

Следующий шаг - полиграммные шифры

Вместо замены символов – замена групп символов.
В некоторых способах реализации приводит к сокращению объёма данных.

Английский язык:	Русский язык:
you, he, she, it	ты, вы, он, она, оно, они, …
the	
..tion	..ция
..ing	..ение
..ness	..ость
…	…

Асимметричное шифрование - наше всё!

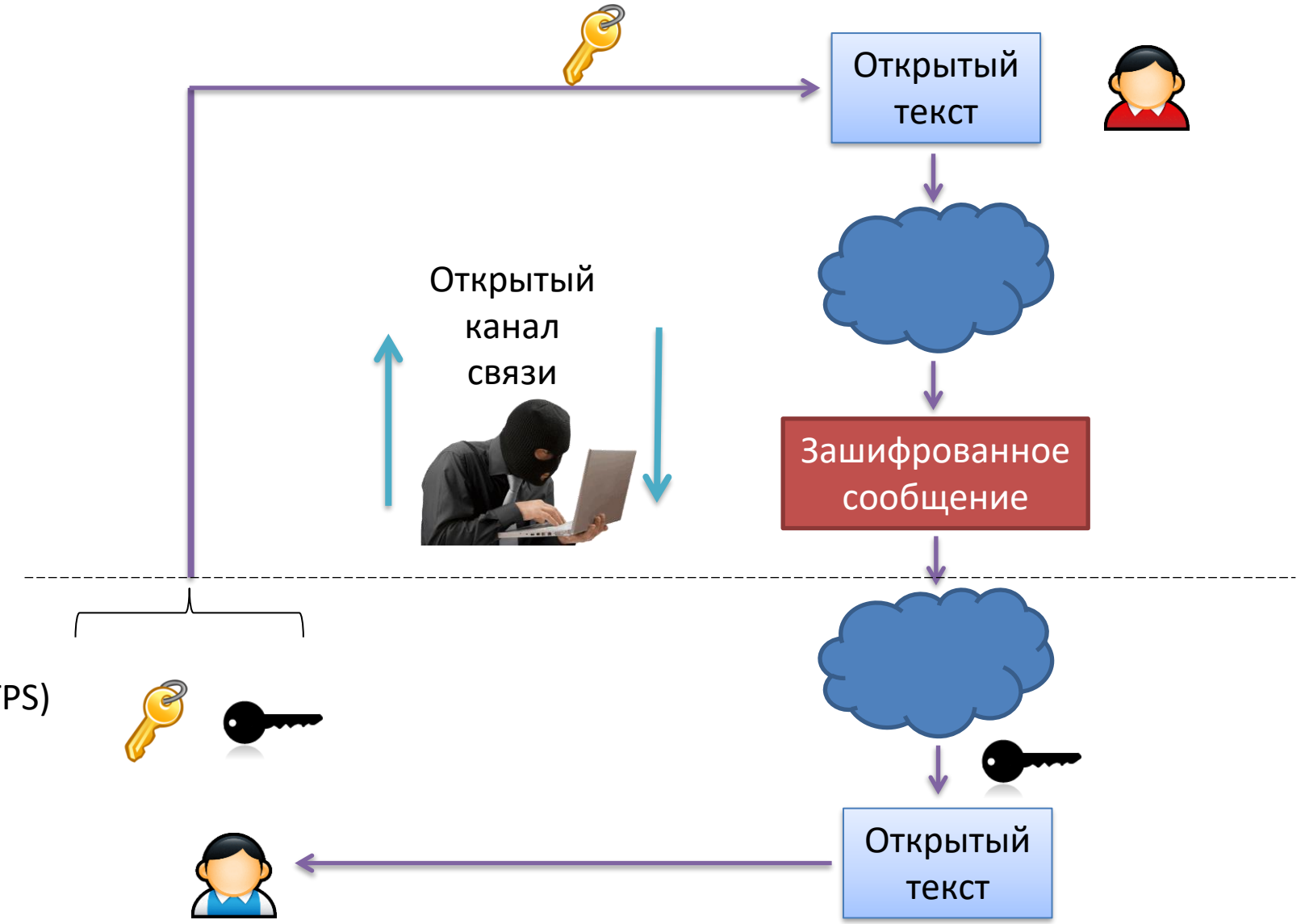
Шифрование «с открытым ключом»

Алгоритм:

RSA

Используют:

SSH,
SSL и TLS (HTTPS)



Пример работы асимметричного шифрования (1)

1. Выбираем два случайных простых числа:

P1 = 53

P2 = 59

2. Вычисляем N - произведение P1*P2:

N = P1 *P2 = 53*59 = 3127

3. Вычисляем Ф(N):

Ф(N) = (P1-1) *(P2-1) = 52*58 = 3016

4. Выбираем небольшой показатель степени E:

E = 3

Пример работы асимметричного шифрования (2)

Вычисляем величину D:

$$D = \frac{2*\Phi(N) + 1}{E}$$

P1 = 53
P2 = 59
N=3127
Φ(N)=3016
E=3
D=2011

В нашем случае:

$$D = \frac{2*\Phi(N) + 1}{E} = 2011$$

Пример работы асимметричного шифрования (3)

P1 = 53
P2 = 59
N=3127
Ф(N)=3016
E=3
D=2011

Открытый ключ

N=3127
E=3

N=3127
E=3

Пример работы асимметричного шифрования (4)

N=3127

E=3

89

Вычисляем зашифрованное сообщение:

$$C = 89^{E} \mod N = 89^{3} \mod 3127 = 1394$$

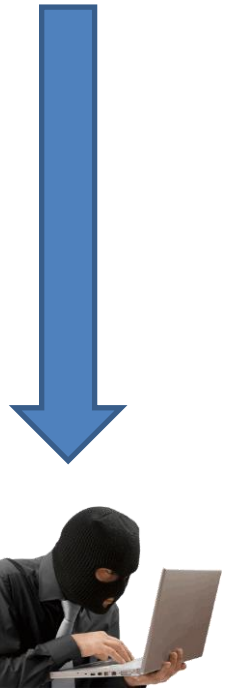
Открытое сообщение

Зашифрованное сообщение

Пример работы асимметричного шифрования (5)

C = 1394

P1 = 53
P2 = 59
N=3127
Φ(N)=3016
E=3
D=2011
C=1394



N=3127
E=3
C=1394

Пример работы асимметричного шифрования (6)

P1 = 53

P2 = 59

N=3127

Φ(N)=3016

E=3

D=2011

C=1394

Расшифровка:

$$C^{D} \bmod N = 1394^{2011} \bmod 3127 = 89$$

Пример работы асимметричного шифрования (7)

N=3127

E=3

C=1394

?

$$\Phi(N) = (P1-1) * (P2-1)$$

$$D = \frac{2*\Phi(N) + 1}{E}$$

$$C^{D} \bmod N =$$

Интерполяционный полином Лагранжа

$$L(x) = \sum_{i=0}^{N} \left[y_i \cdot \prod_{j=0, j \neq i}^{N} \frac{x - x_j}{x_i - x_j} \right]$$

Пример:
мы имеем точки
p0=(1;2) и
p1=(2;3)

$$L(x) = y_0 \cdot \frac{x - x_1}{x_0 - x_1} + y_1 \cdot \frac{x - x_0}{x_1 - x_0}$$

$$L(x) = 2 \cdot \frac{x - 2}{1 - 2} + 3 \cdot \frac{x - 1}{2 - 1}$$

$$L(x) = x + 1$$

Схема разделения секрета Шамира: пример (1)

Наш секрет: 3

$$S = (0;\ 3)$$

Формируем уравнение:

$$f(x) = 3 + 12 \cdot x + 19x^2$$

Генерируем 4 ключа:

$$x_0 = 24; y_0 = f(x_0) = 3 + 288 + 10944 = 11235$$
$$x_1 = 25; y_1 = f(x_1) = 3 + 300 + 11875 = 12178$$
$$x_2 = 32; y_2 = f(x_2) = 3 + 384 + 19456 = 19843$$
$$x_3 = 41; y_3 = f(x_3) = 3 + 492 + 31939 = 32434$$

Схема разделения секрета Шамира: пример (2)

$f(x) = 3 + 12 \cdot x + 19x^2$

Собрались люди, знающие ключи
$(x_0; y_0), (x_1; y_1), (x_3; y_3)$

$(x_0; y_0) = (24; 11235)$
$(x_1; y_1) = (25; 12178)$
$(x_2; y_2) = (32; 19843)$
$(x_3; y_3) = (41; 32434)$

$$L(x) = \sum_{i=0}^{N} \left[y_i \cdot \prod_{j=0, j \neq i}^{N} \frac{x - x_j}{x_i - x_j} \right]$$

$$L(x) = y_0 \left(\frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_3}{x_0 - x_3} \right) + y_1 \left(\frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_3}{x_1 - x_3} \right) + y_3 \left(\frac{x - x_0}{x_3 - x_0} \cdot \frac{x - x_1}{x_3 - x_1} \right)$$

$$L(x) = 11235 \left(\frac{x - 25}{24 - 25} \cdot \frac{x - 41}{24 - 41} \right) + 12178 \left(\frac{x - 24}{25 - 24} \cdot \frac{x - 41}{25 - 41} \right) + 32434 \left(\frac{x - 24}{41 - 24} \cdot \frac{x - 25}{41 - 25} \right) =$$

$$= \frac{5158 \cdot x^2 + 3264 \cdot x + 816}{272} = 19 \cdot x^2 + 12 \cdot x + 3$$

$S = (0;\ 3)$

$L(0) = 19 \cdot 0^2 + 12 \cdot 0 + 3 = 3$

Схема разделения секрета Шамира: пример (3)

$f(x) = 3 + 12 \cdot x + 19x^2$

Собрались люди, знающие ключи
$(x_1; y_1), (x_2; y_2), (x_3; y_3)$

$(x_0; y_0) = (24; 11235)$
$(x_1; y_1) = (25; 12178)$
$(x_2; y_2) = (32; 19843)$
$(x_3; y_3) = (41; 32434)$

$$L(x) = \sum_{i=0}^{N} \left[y_i \cdot \prod_{j=0, j \neq i}^{N} \frac{x - x_j}{x_i - x_j} \right]$$

$$L(x) = y_1 \left(\frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} \right) + y_2 \left(\frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} \right) + y_3 \left(\frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} \right)$$

$$L(x) = 12178 \left(\frac{x - 32}{25 - 32} \cdot \frac{x - 41}{25 - 41} \right) + 19843 \left(\frac{x - 25}{32 - 25} \cdot \frac{x - 41}{32 - 41} \right) + 32434 \left(\frac{x - 25}{41 - 25} \cdot \frac{x - 32}{41 - 32} \right) =$$

$$= \frac{134064 \cdot x^2 + 84672 \cdot x + 21168}{7056} = 19 \cdot x^2 + 12 \cdot x + 3$$

$S = (0;\ 3)$

$L(0) = 19 \cdot 0^2 + 12 \cdot 0 + 3 = 3$

Схема разделения секрета Шамира: пример (4)

$f(x) = 3 + 12 \cdot x + 19x^2$

Собрались люди, знающие ключи
$(x_0; y_0), (x_1; y_1)$

$(x_0; y_0) = (24; 11235)$
$(x_1; y_1) = (25; 12178)$
$(x_2; y_2) = (32; 19843)$
$(x_3; y_3) = (41; 32434)$

$$L(x) = y_0 \cdot \frac{x - x_1}{x_0 - x_1} + y_1 \cdot \frac{x - x_0}{x_1 - x_0}$$

$$L(x) = 11235 \cdot \frac{x - 25}{24 - 25} + 12178 \cdot \frac{x - 24}{25 - 24} = 11235 \cdot x - 11397$$

$$L(0) = 11235 \cdot 0 - 11397 = -11397$$

Аутентификация пользователей

Аутентификация пользователей строится на хэшах. (hash)

Основной алгоритм - алгоритм md5.

Примеры:
'a' - **0cc175b9c0f1b6a831c399e269772661**
'b' - **92eb5ffee6ae2fec3ad71c777531578f**

' ' - **d41d8cd98f00b204e9800998ecf8427e**

«Развернуть» хэш обратно однозначно **«нельзя»**!

Методы взлома – атака «грубой силой» (brute-force),
перебор по словарю.

Засаливание паролей (2)

Wordpress

Перед паролем приписывается соль и полученная строка хэшируется MD5 2^8 раз.

Joomla

Используется библиотека phpass, по умолчанию bcrypt с солью и 2^10 повторениями.

Drupal

По умолчанию соленый sha512 с 2^16 повторениями.

Как и где применяется шифрование

1. хранение информации – отдельные файлы;

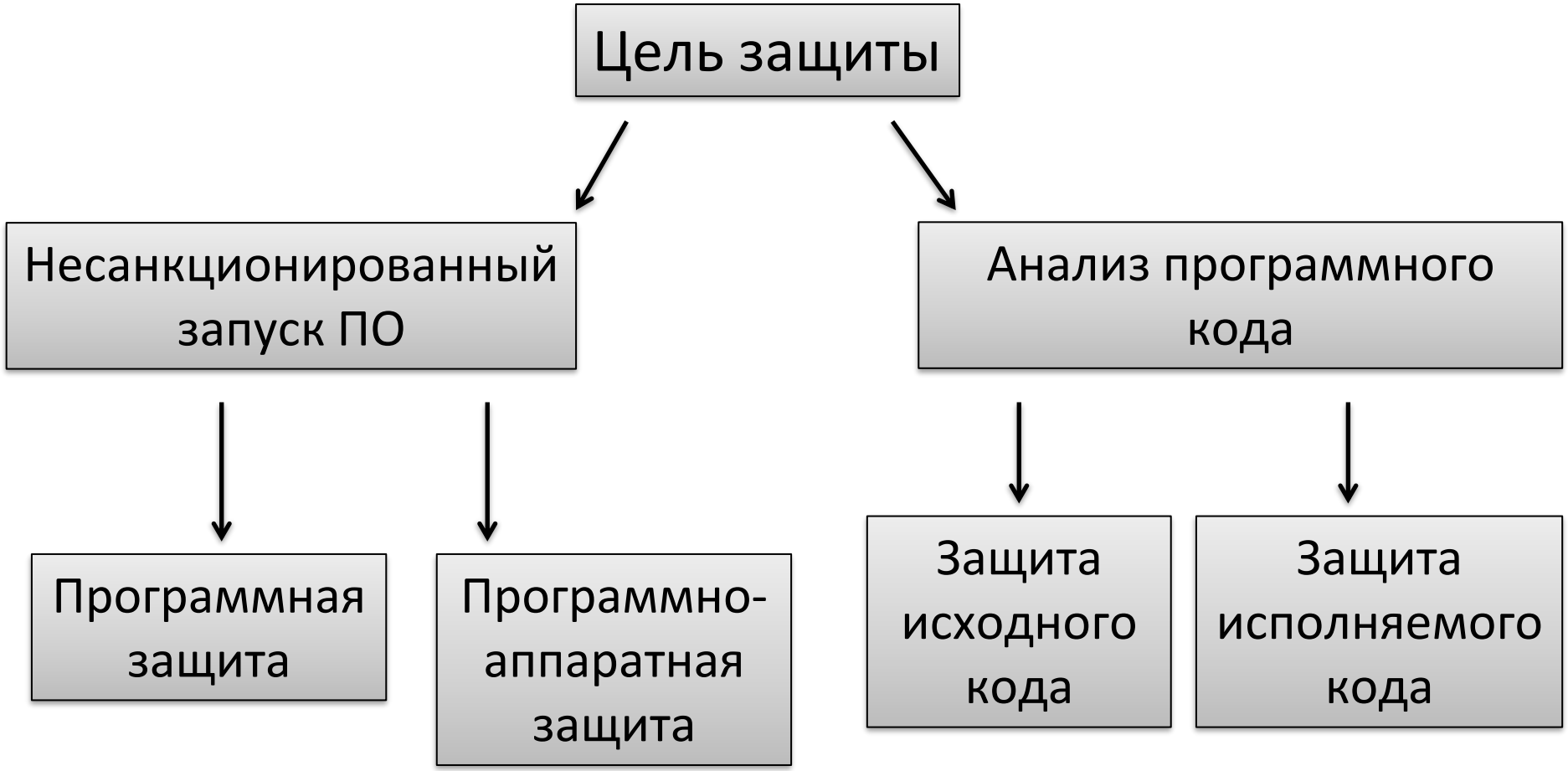
2. аутентификация пользователей

3. хранение информации – файловые системы;

4. протоколы передачи данных в сети интернет;

5. аппаратное шифрование на уровне устройств.

Защита программного кода



Программная защита - использование серийного номера

```
int main() {
  int key = 0;
  scanf("%d", &key);
  if(key == 32)
    printf("Secret info!");
  return 0;
}
```

Метод взлома:
замена опкода jne (0x75)
на опкод je (0x74)

```
    if(key == 32)
00F8101B  cmp     dword ptr [esp],20h
00F8101F  jne     main+2Fh (0F8102Fh)
    printf("Secret info!");
00F81021  push    offset string "Secret info!" (0F82108h)
00F81026  call    dword ptr [__imp__printf (0F8209Ch)]
00F8102C  add     esp,4
    return 0;
00F8102F  xor     eax,eax
```

Программно-аппаратная защита - электронные ключи

Что может делать ключ?

- Хранить серийник
- Хранить таблицу ответов на опросы
- Хранить программный код

Ключи:

Guardant от ООО Актив
LOCK от ООО Астрома
SenseLock от ЗАО «Секьюлэб»
и другие

Метод взлома:
опрос и эмуляция

Сложность: нужно купить хотя бы один ключ

Цена вопроса: от 4000 рублей за ключ

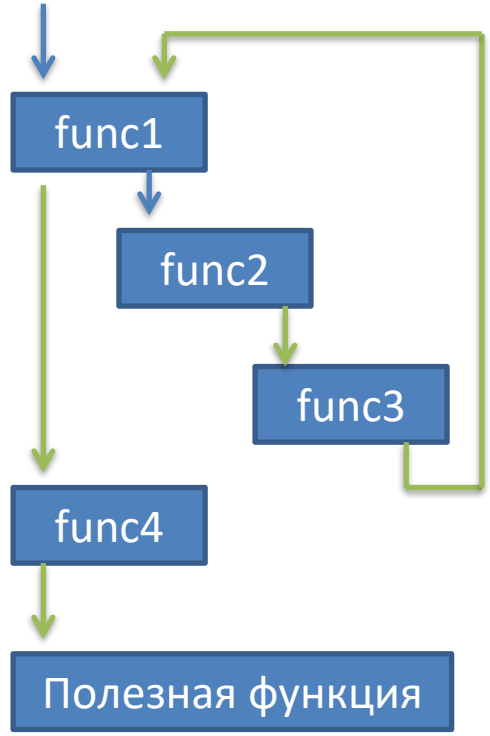
Защита исходного кода

1. Защита от дизассемблирования

2. Запутывание программного кода

3. Распараллеливание

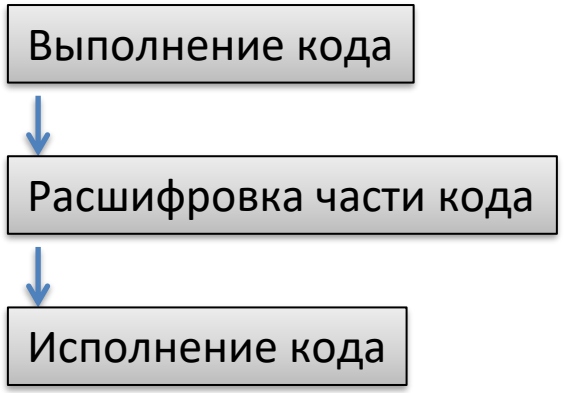
BOOL WINAPI IsDebuggerPresent();



Шифрование исполняемого кода

Память с данными = Последовательность байт
Машинный код = Последовательность байт

Можно запустить на исполнение произвольный участок памяти




```
void XOR_EAX_EAX_memory() {
  char *mach_code = new char [10];

  mach_code[0] = (char)0x55;
  mach_code[1] = (char)0x8B;
  mach_code[2] = (char)0xEC;
  mach_code[3] = (char)0x33;
  mach_code[4] = (char)0xC0;
  mach_code[5] = (char)0x8B;
  mach_code[6] = (char)0xE5;
  mach_code[7] = (char)0x5D;
  mach_code[8] = (char)0xC3;
  mach_code[9] = (char)0x90;

  __asm call mach_code
}
```