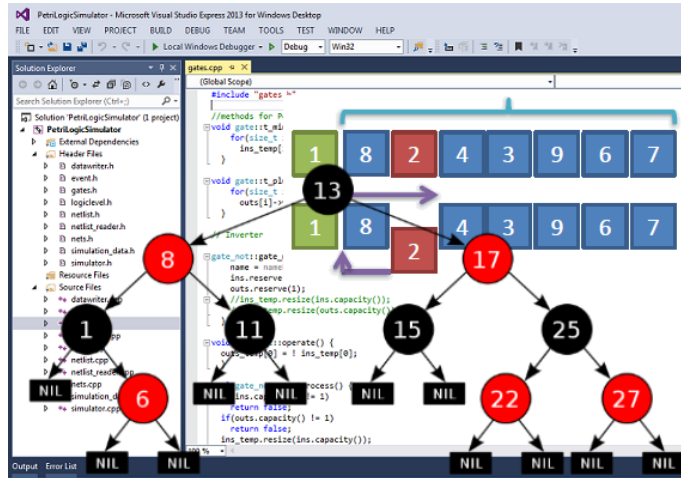




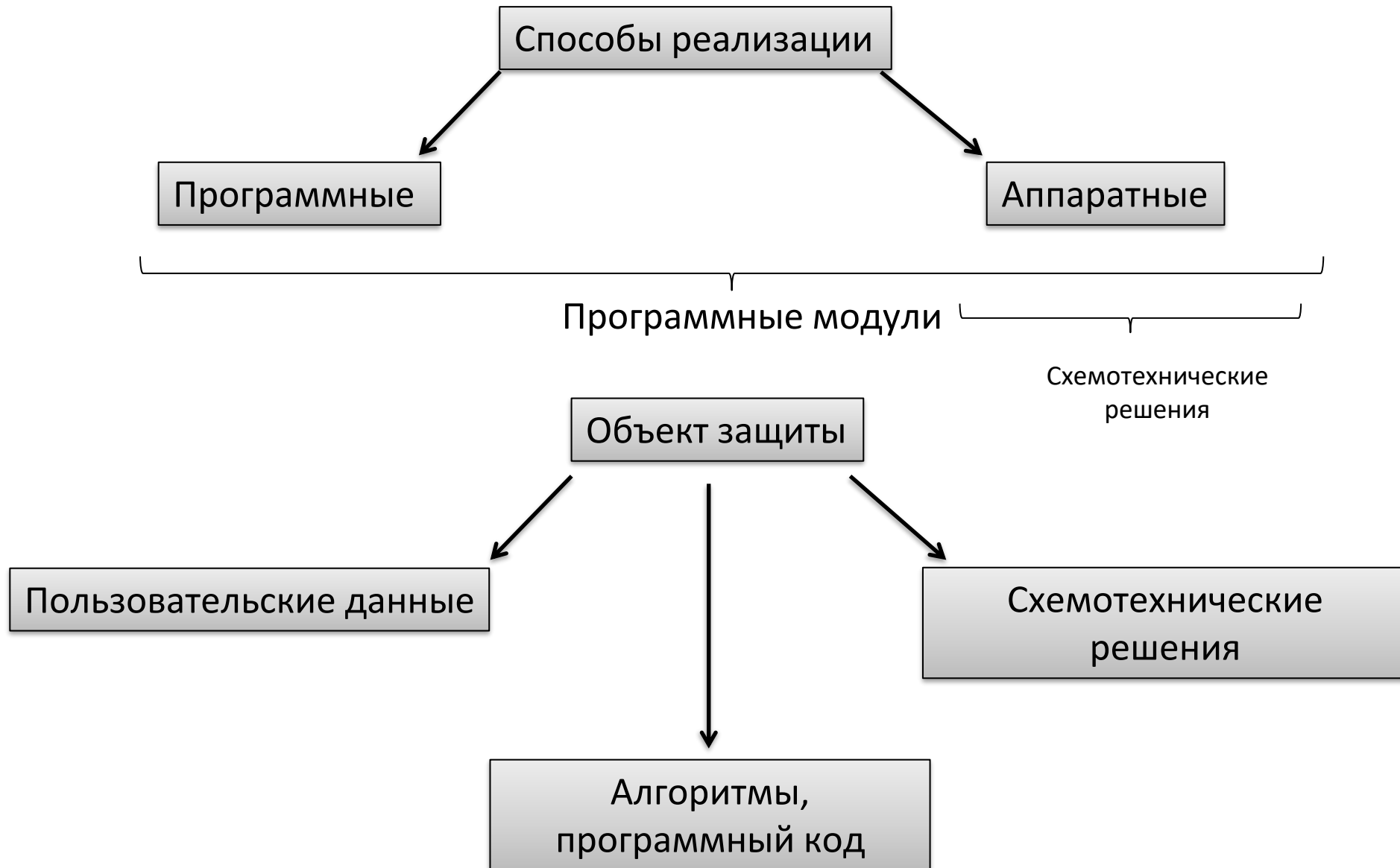
# Теория алгоритмов



Лекция 6

**Алгоритмические подходы к защите данных**

# Классификация методов защиты (1)



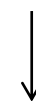
## Квадрат Полибия

Первый шифр, не требующий специальной «аппаратной» составляющей

**Полибий**  
III век до н.э.

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

КАФЕДРА ПКИМС РУЛИТ!



25114316153511633425  
24313663354226244164



## Шифр, с которого начинают все программисты

### Шифр Цезаря

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!



Гай Юлий Цезарь  
I век до н.э.

## 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

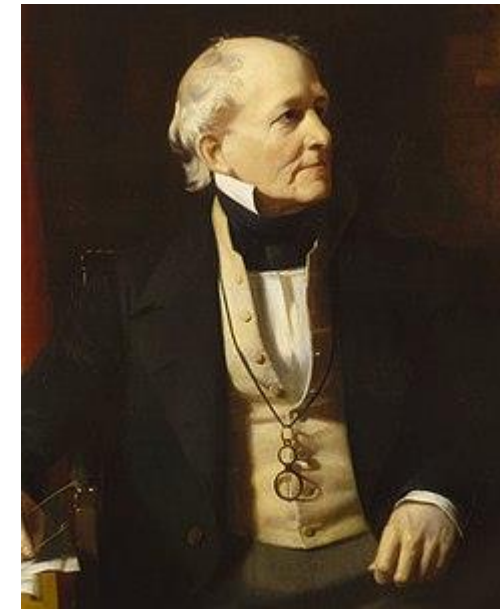


Блез де Виженер, 1523-1596  
Публикация шифра: 1586

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

## Простая литорея (тарабарский шифр)

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

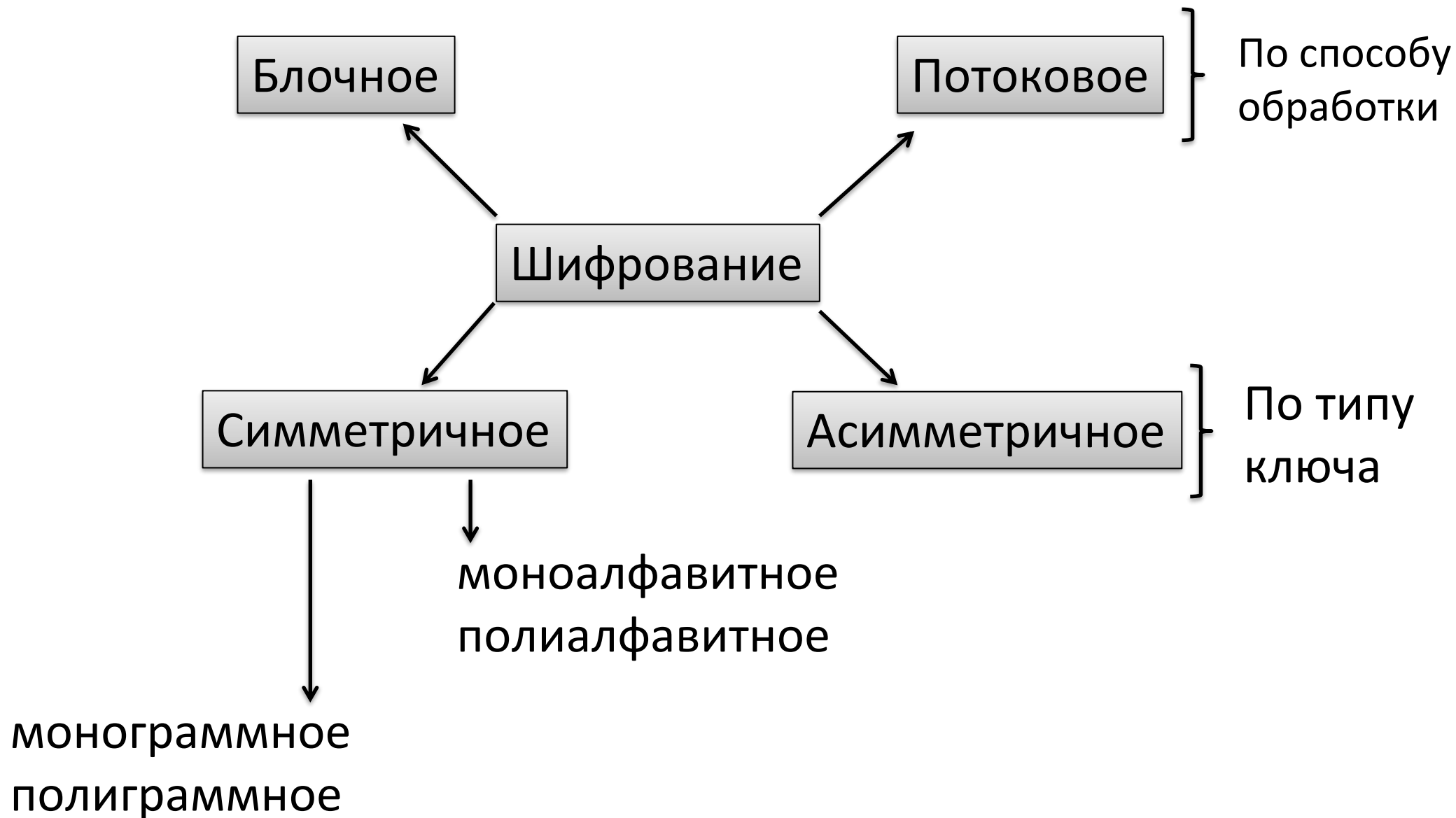
КАФЕДРА ПКИМС РУЛИТ



ТАЗЕЦМА НТИРЛ МУСИК



## Общая классификация методов программного шифрования



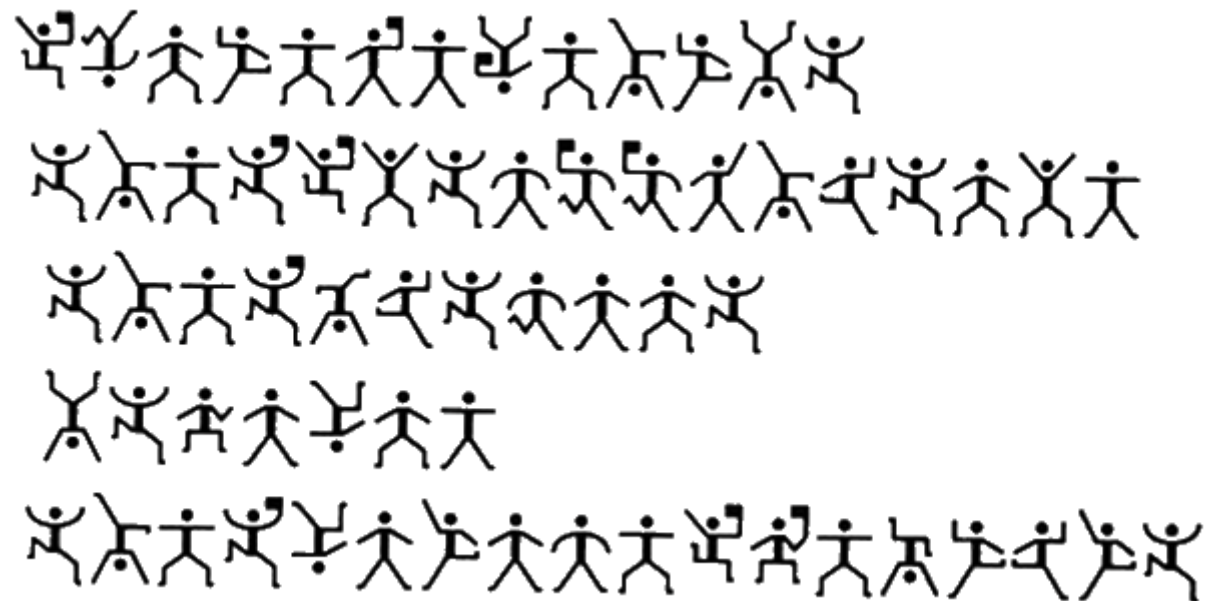
## Моноалфавитные монограммные шифры

1. Шифры типа алгоритма Цезаря - перестановочные

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

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

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



## Полиалфавитные монограммные шифры

Полиалфавитные шифры устраняют некоторые недостатки одноалфавитных шифров

Одноалфавитный

А  
Б  
В  
Г

А1  
А2  
А3  
А4

Полиалфавитный

А  
Б  
В  
Г

А1, А2  
А3  
А4  
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		!		

                  ↑           ↑   ↑

2511431615351163342524313666354226244164

## 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

...

...

## Полиграммный шифр – маленький шифр Наполеона

### *Малый шифр Наполеона (Petit Chiffre)*

(реконструирован Базери)

A – 15, ar – 25, al – 39

B – 37, bu – 3, bo – 35, bi – 29,

C – 6, ca – 32, ce – 20

D – 23, de – 52

E – 53, es – 82, et – 50, en – 68

F – 55, fa – 69, fe – 58, fo – 71

G – 81, ga – 51

H – 85, hi – 77

I – 119, jai – 122

J – 87, jai – 123

K – ?

L – 96, lu – 103, le – 117, la – 106

M – 114, ma – 107

N – 115, ne – 94, ni – 116

O – 90, ot – 153

P – 137, po – 152

Q – 173, que – 136

R – 169, ra – 146, re – 126, ri – 148,

S – 167, sa – 171, se – 177, si – 134, so – 168, su – 174

T – 176, ti – 145, to – 157

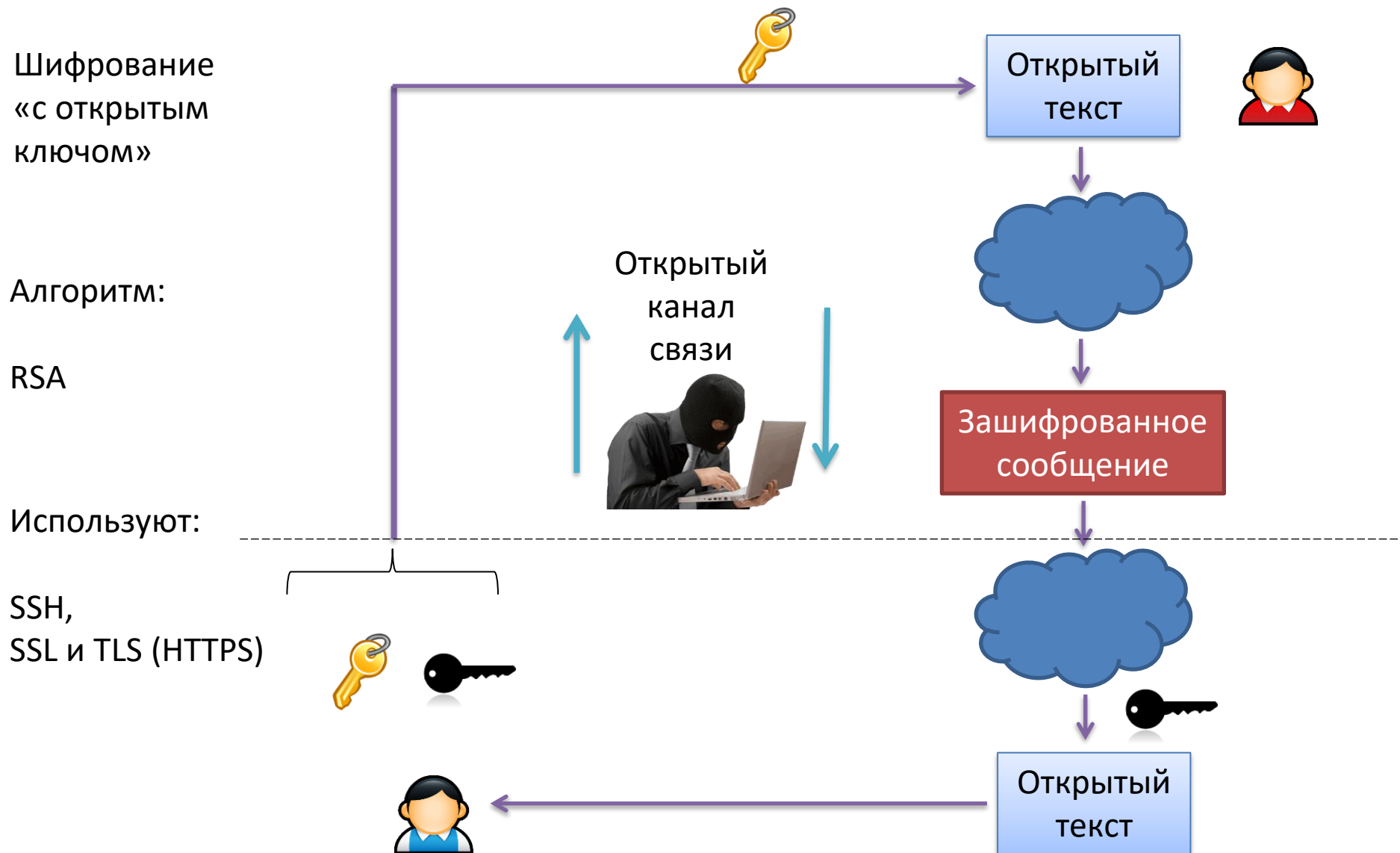
U – 138

V – 164, ve – 132, vi – 161, vo – 175

W, X, Y – ?

Z – 166

# Асимметричное шифрование - наше всё!



## 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  $\Phi(N)$ :

$$\Phi(N) = (P1-1) * (P2-1) = 52 * 58 = 3016$$

4. Выбираем небольшой показатель степени E:

$$E = 3$$

Вычисляем величину D:

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

В нашем случае:

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

$$P1 = 53$$

$$P2 = 59$$

$$N = 3127$$

$$\Phi(N) = 3016$$

$$E = 3$$

$$D = 2011$$

## Пример работы асимметричного шифрования (3)



$$P1 = 53$$

$$P2 = 59$$

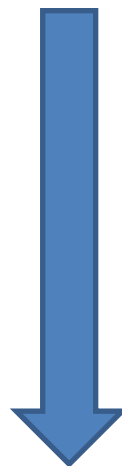
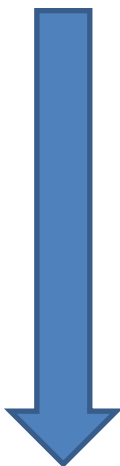
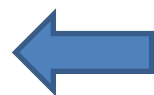
$$N = 3127$$

$$\Phi(N) = 3016$$

$$E = 3$$

$$D = 2011$$

Открытый ключ



$$N = 3127$$
$$E = 3$$



$$N = 3127$$
$$E = 3$$





## Пример работы асимметричного шифрования (4)



$N=3127$

$E=3$



89

Вычисляем зашифрованное сообщение:

$$C = 89^E \pmod N = 89^3 \pmod 3127 = 1394$$



Открытое сообщение



Зашифрованное сообщение

## Пример работы асимметричного шифрования (5)



$C = 1394$



$P1 = 53$

$P2 = 59$

$N = 3127$

$\Phi(N) = 3016$

$E = 3$

$D = 2011$

$C = 1394$

$N = 3127$

$E = 3$

$C = 1394$



## Пример работы асимметричного шифрования (6)



Расшифровка:

$$P1 = 53$$

$$P2 = 59$$

$$N=3127$$

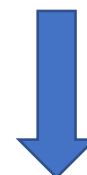
$$\Phi(N)=3016$$

$$E=3$$

$$D=2011$$

$$C=1394$$

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



## Пример работы асимметричного шифрования (7)



$N=3127$

$E=3$

$C=1394$

?

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

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

$$C^D \text{ mod } N =$$

## 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  
 $p_0=(1;2)$  и  
 $p_1=(2;3)$

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

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

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

## 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

$(x_0; y_0), (x_1; y_1)$

$$(x_0; y_0) = (24; 11235)$$

$$(x_1; y_1) = (25; 12178)$$

$$(x_2; y_2) = (32; 19843)$$

$$(x_3; y_3) = (41; 32434)$$

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

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

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

## 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.



## Аутентификация пользователей

Аутентификация пользователей строится на хэшах. (hash)

Основной алгоритм - алгоритм md5.

Примеры:

'a' - **0cc175b9c0f1b6a831c399e269772661**

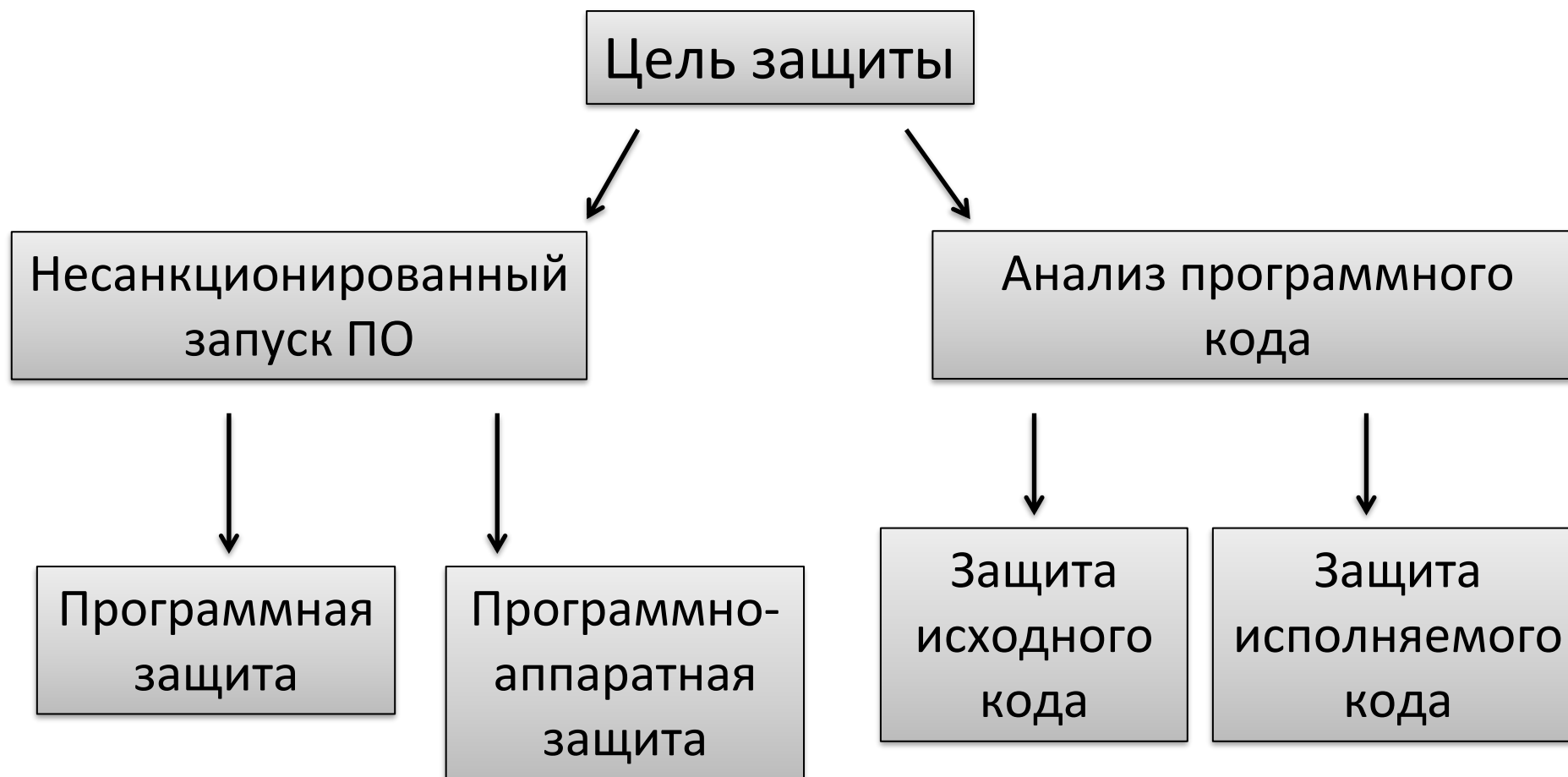
'b' - **92eb5ffee6ae2fec3ad71c777531578f**

' ' - **d41d8cd98f00b204e9800998ecf8427e**

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

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

## 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

Метод взлома:  
опрос и эмуляция

Сложность: нужно купить хотя  
бы один ключ

Ключи:

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

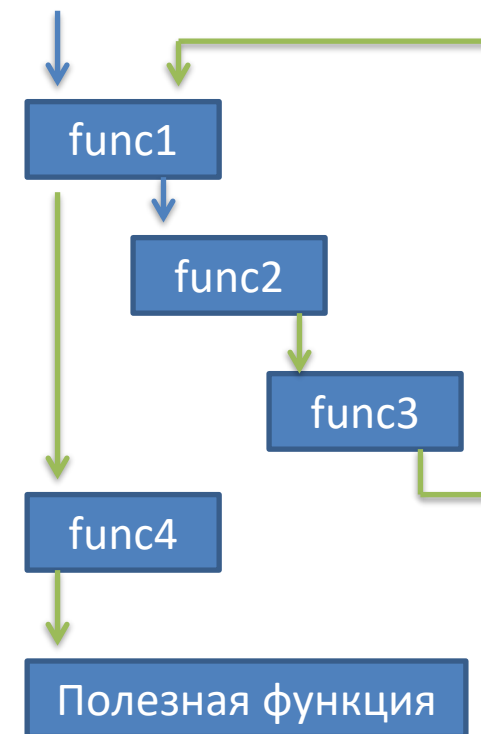


Цена вопроса: от 2500 рублей за ключ

## Защита исходного кода

1. Защита от дизассемблирования
2. Запутывание программного кода
3. Распараллеливание

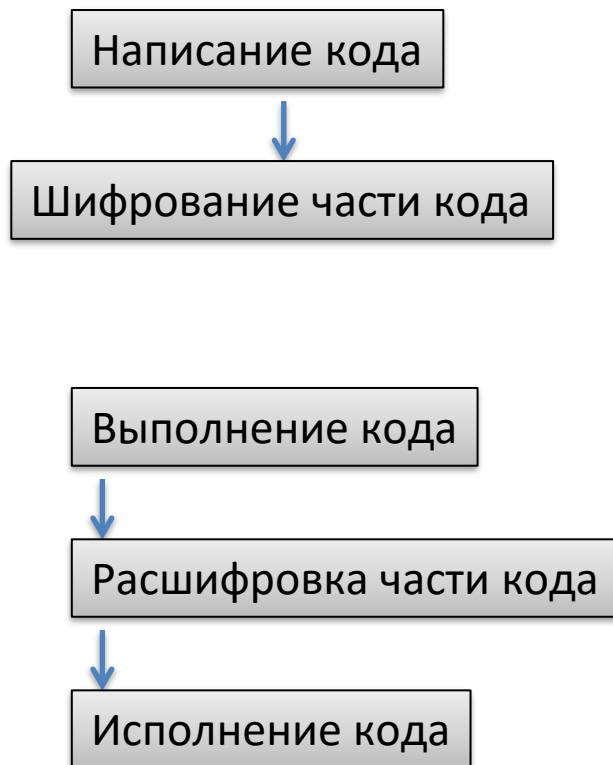
```
BOOL WINAPI IsDebuggerPresent();
```



## 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  
}
```