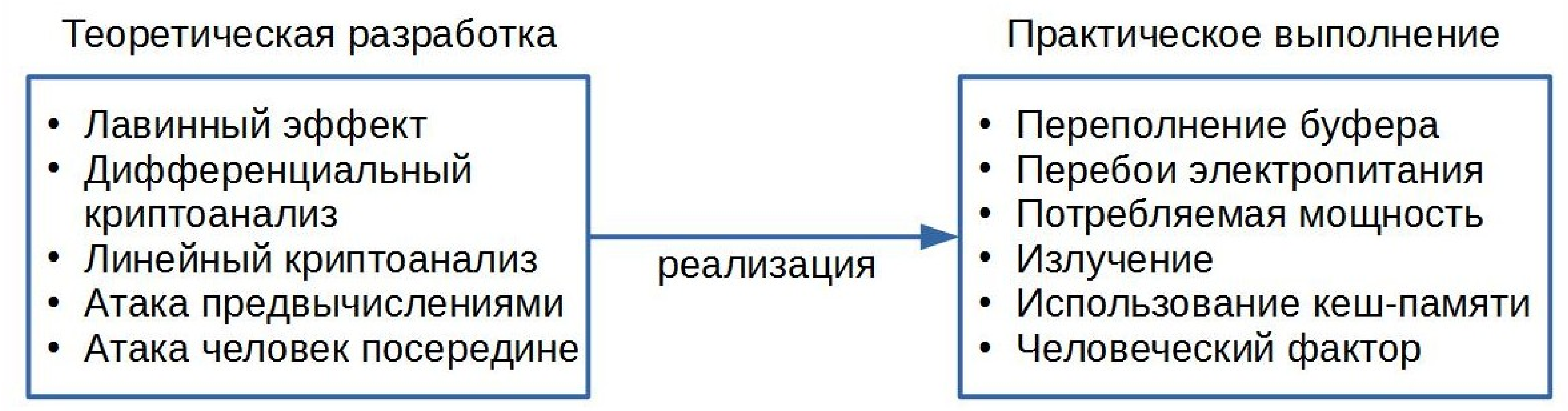
Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Атаки по сторонним каналам

Атака на реализацию



Виды атак по сторонним каналам

- Атака по времени
- Атака по энергопотреблению
- Атака по электромагнитному излучению
- Акустическая атака
- Атака по видимому излучению

Атака по времени

RSA

$N = p*q$

p, q – простые

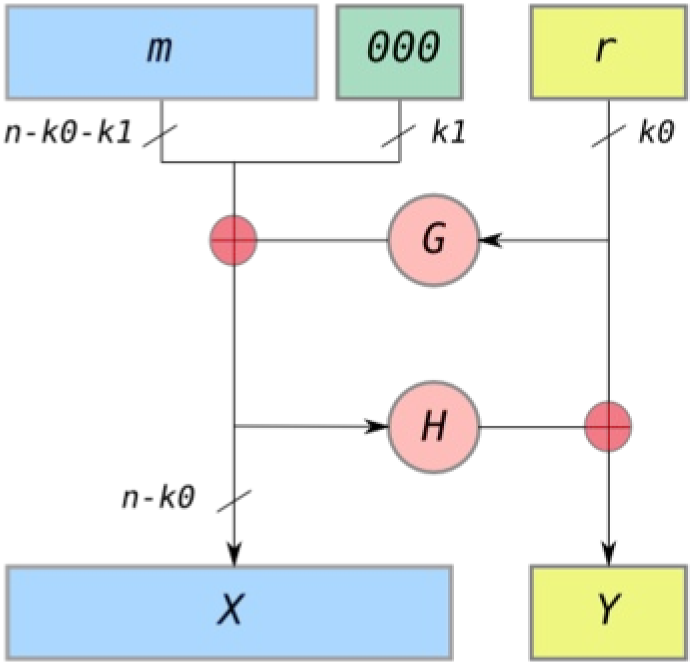
$e*d = 1 \bmod (p – 1)*(q – 1)$

(e,N) – открытый ключ, d – закрытый ключ

$c = m^e \bmod N$ – шифрование сообщения

$m = c^d \bmod N$ – расшифровывание сообщения

RSA–OAEP



Атака на основе подобранного шифротекста:

$c_1 = m_1^e \bmod N$, $c_2 = m_2^e \bmod N$.
Если $c_1 = c_2$, то $m_1 = m_2$.

Optimal Asymmetric Encryption Padding

$c = RSA(OAEP(m, r))$;
$m = OAEP^{-1}(RSA^{-1}(c))$.

Будем дополнять сообщение не нулями, а единицами, чтобы сервер отклонил пакет сразу после расшифровки и проверки дополнения.

Китайская теорема об остатках

$N = p*q$

$$\begin{cases} c^d \bmod p \\ c^d \bmod q \end{cases}$$

$c^d \bmod pq$

Метод повторяющихся возведения в квадрат и умножения

a^x – x итераций

a^{2x} – 2x итераций

$(a^x)^2$ – x+1 итерация

$a^{2x+1} = (a^x)^2 * a$ – x+2 итерации

$a^{1010110} = (a^{101011})^2 = (a^{101010} * a)^2 = ((a^{10101})^2 * a)^2 = \dots = (((((a^2)^2 * a)^2)^2 * a)^2 * a)^2$

a^b, $b = 1b_{k-1}b_{k-2}...b_2b_1b_0$

```
res = a
for (i = k-1; i > -1)
  если b_i == 0
    res = res^2   (1 операция)
  иначе
    res = res^2*a (2 операции)
  i--
```

в среднем 1.5*k умножений

Метод “скользящего окна”

q_mul		
0	0	0
1	a^{1}	a^{00001}
2	0	0
3	a^{3}	a^{00011}
4	0	0
5	a^{5}	a^{00101}
31	a^{31}	a^{11111}

$a^{1...0110101} = a^{1...0100000} * a^{10101} =$
$(((((a^{1...01})^2)^2)^2)^2)^2 * a^{10101} =$
$(((((a^{1...01})^2)^2)^2)^2)^2 * q\_mul[21]$

Умножений:

на создание массива: 16
на возведение в степень: k + k/5
всего: 16 + k + k/5

В общем случае:

размер окна: m
на создание массива: 2^{m-1}
на возведение в степень: k + k/m
всего: $2^{m-1} + k + k/m$

Пример: при k = 500, m = 5
ПКУ – 1.5*k = 750
СО – $2^{m-1} + k + k/m = 632$

Преобразование Монтгомери

$a*b \bmod q$

$R = 2^k$
$a_0 = a*R \bmod q \qquad a = a_0/R \bmod q$
$b_0 = b*R \bmod q \qquad b = b_0/R \bmod q$

$a_0*b_0 \bmod q = a*R*b*R \bmod q$
$a_0{}^{o}b_0 \bmod q = a_0*b_0/R \bmod q = a*b*R \bmod q$
$a*b = a_0{}^{o}b_0/R \bmod q$

$c^d \bmod q = c*c*...*c \bmod q$
$c_0 = c*R \bmod q$
$m = c_0{}^{o}c_0{}^{o}...{}^{o}c_0 \bmod q$
$c^d = m/R \bmod q$

$a_0{}^{o}b_0 \bmod q = a_0*b_0/R \bmod q$

$a_0*b_0 + x*q = ***00...0 \bmod q$

$x*q$ – быстрее деления, медленнее умножения

Если $a_0{}^{o}b_0 > R$, то производится дополнительное сокращение

Если вычисляется c^d, то вероятность дополнительного сокращения на каждом шаге равна:

P(доп.сокр) = (c mod q) / (2*R)

Метод Карацубы

$A_{512} * B_{512} = A1_{256}A2_{256} * B1_{256}B2_{256}$

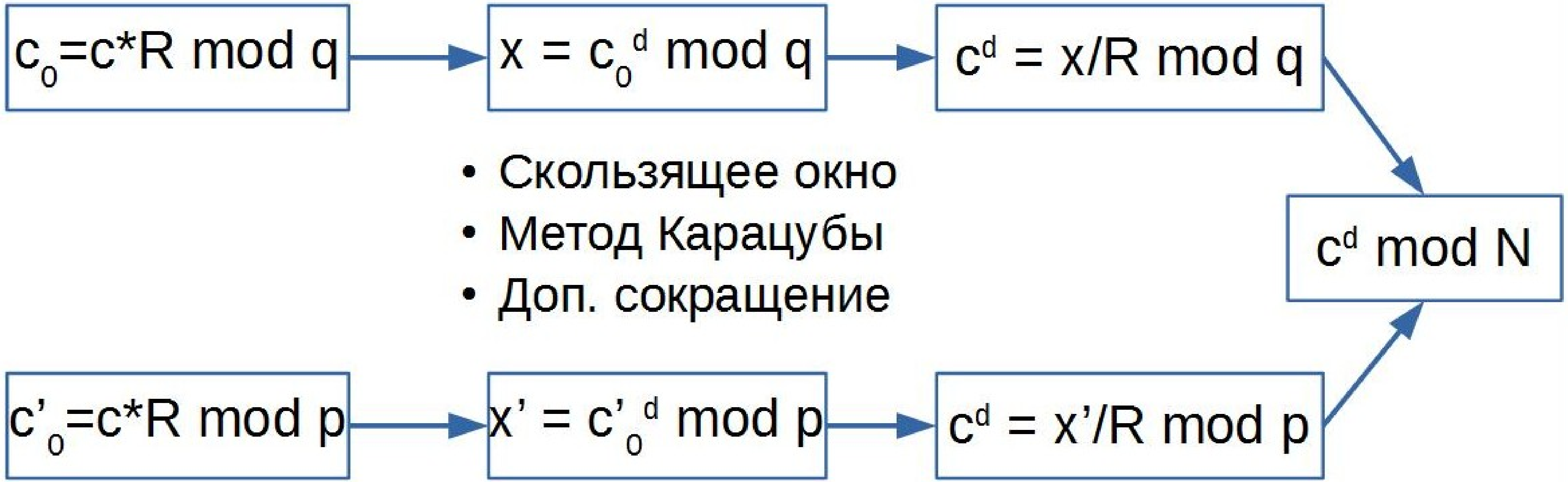
$A1_{256}A2_{256} * B1_{256}B2_{256} =$
$(2^{256} * A1 + A2) * (2^{256} * B1 + B2) =$
$2^{512} * A1 * B1 + 2^{256} * (A1 * B2 + A2 * B1) + A2 * B2$

$A1*B1, A1*B2, A2*B1, A2*B2$ – 4 умножения

$A1_{256}A2_{256} * B1_{256}B2_{256} =$
$(2^{512} + 2^{256}) * (A1 * B1) - 2^{256} * ((A1 - A2) * (B1 - B2)) + (2^{256} + 1)(A2 * B2)$

$A1*B1, (A1 - A2) * (B1 - B2), A2*B2$ – 3 умножения

Процесс вычислений



Восстановление q

Пусть восстановлены старшие j бит в q и разрядность q.

$c_0 = q_0q_1q_2...q_j000...$ проверяется за время t_0

$c_1 = q_0q_1q_2...q_j100...$ проверяется за время t_1

P(доп.сокр) = (c mod q) / (2*R)

$q_{j+1} = 1$, если $t_1 \approx t_0$

$q_{j+1} = 0$, если $t_1 < t_0$

Атака по энергопотреблению

Корреляция случайных величин

Теория вероятности

X, Y – случайные величины

M_X – математическое ожидание X

D_X – дисперсия X

$\sigma_X = D_X^{1/2}$ – стандартное отклонение X

$cov_{XY} = M((X - M_X)(Y - M_Y))$ – ковариация X и Y

$$r_{XY} = \frac{cov_{XY}}{\sigma_X \sigma_Y}$$ -

коэффициент линейной корреляции (коэффициент корреляции Пирсона)

Математическая статистика

$X = \{x_1,\ldots,x_N\}$, $Y = \{y_1,\ldots,y_N\}$ – выборки

$\overline{X} = \frac{1}{n}\sum x_i$ - выборочное среднее

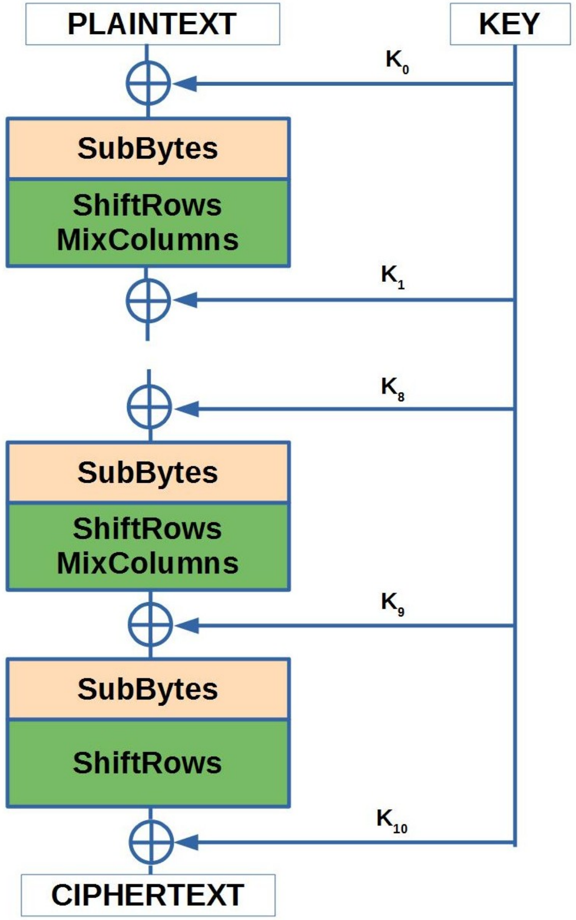
$S_X^2 = \frac{1}{n}\sum(x_i - \overline{X})^2$ - выборочная дисперсия

$cov_{XY} = \frac{1}{n}\sum(x_i - \overline{X})(y_i - \overline{Y})$ - выборочная ковариация

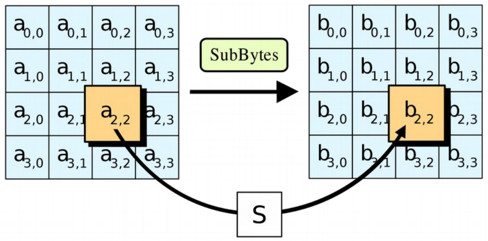
$$r_{XY} = \frac{cov_{XY}}{S_X S_Y} = \frac{\sum(x_i - \overline{X})(y_i - \overline{Y})}{\sqrt{\sum(x_i - \overline{X})^2 \sum(y_i - \overline{Y})^2}}$$

коэффициент корреляции Пирсона

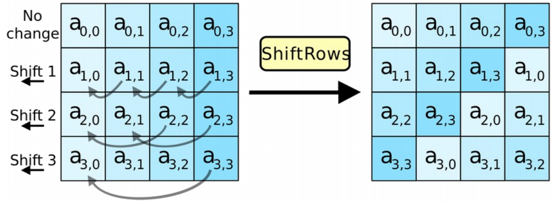
AES



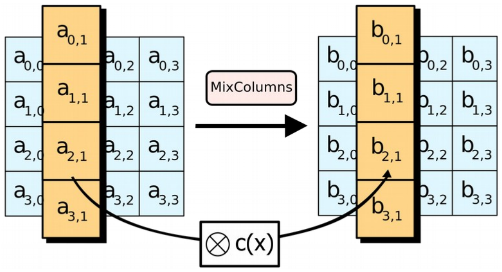
SubBytes



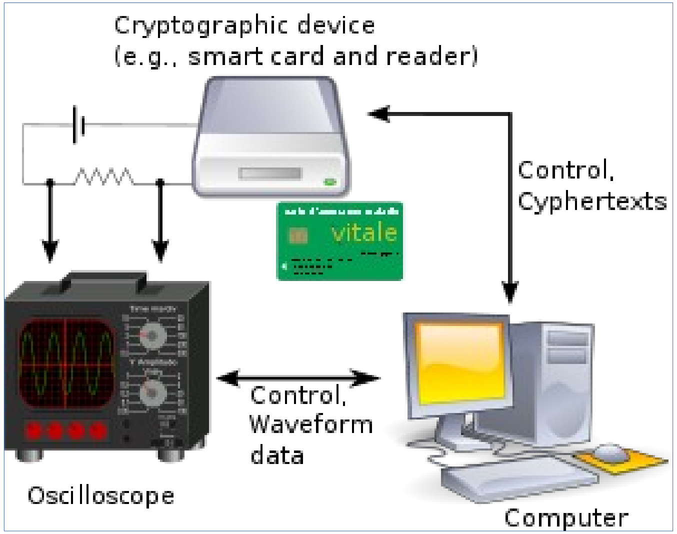
ShiftRows



MixColumns



Измерительная установка

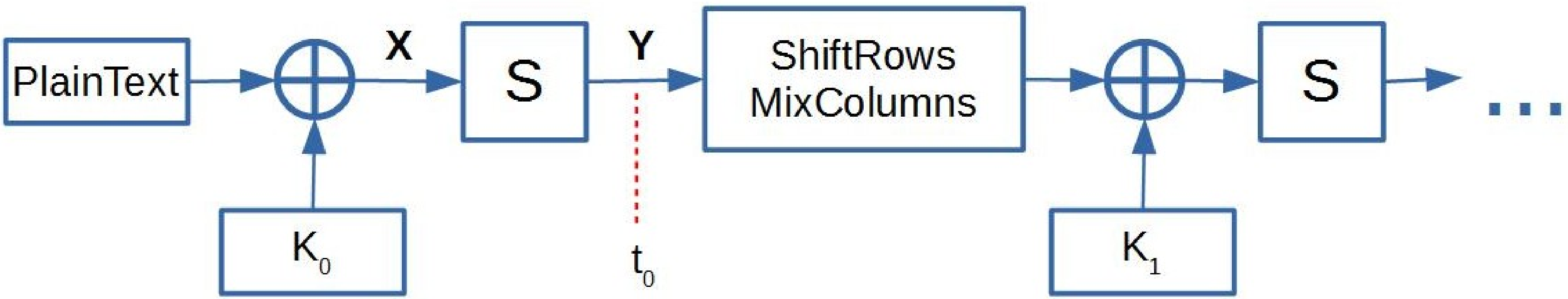


T=	0	1	2		t		M
PT_0	U_{00}	U_{01}	U_{02}	...	U_{0t}	...	U_{0M}
PT_1	U_{10}	U_{11}	U_{12}	...	U_{1t}	...	U_{1M}
...				...			
PT_N	U_{N0}	U_{N1}	U_{N2}	...	U_{Nt}	...	U_{NM}

В момент подачи команды на шифрование осцилограф начинает считывать напряжение на карте.

M ~ 100000, N ~ 1000

Исследуемая корреляция



$Y = S(X) = S(PT \wedge K_0)$

$Y[0] = S(PT[0] \wedge K_0[0])$

$U(t_0) \sim U(Y[0]) \sim HW(Y[0])$ (Hamming weight)

Восстановление первого байта ключа

Текст	Выходное напряжение						
PT_0	U_{00}	U_{01}	U_{02}	...	U_{0t}	...	U_{0M}
PT_1	U_{10}	U_{11}	U_{12}	...	U_{1t}	...	U_{1M}
...				...			
PT_N	U_{N0}	U_{N1}	U_{N2}	...	U_{Nt}	...	U_{NM}

Текст	HW(S(PT[0] ^ K_0[0]))					
PT_0	$HW_{0,0}$	$HW_{0,1}$	…	$HW_{0,k}$	…	$HW_{0,255}$
PT_1	$HW_{1,0}$	$HW_{1,1}$	…	$HW_{1,k}$	…	$HW_{1,255}$
...				...		
PT_N	$HW_{N,0}$	$HW_{N,1}$	…	$HW_{N,k}$	…	$HW_{N,255}$
$K_0[0]$ =	0	1	…	k	...	255

Если $K_0[0] = k$ и выбираем момент съема t, то

$$r(U_t, HW_k) = \frac{\Sigma(U_{it} - \overline{U}_t)(HW_{ik} - \overline{HW}_k)}{\sqrt{\Sigma(U_{it} - \overline{U}_t)^2 \Sigma(HW_{ik} - \overline{HW}_k)^2}}$$

Восстановление первого байта ключа

1. Вычислить $r(U_t, HW_k)$ для всех $0 \le t \le M$, $0 \le k \le 255$ (всего $256 * (M + 1)$ значение).
2. Выбрать наибольший коэффициент корреляции $r(U_{t0}, HW_{k0})$.
3. Тогда первый байт ключа шифрования $K_0[0] = k0$, а преобразование $S(PT[0] \wedge K_0[0])$ происходит в момент времени $t0$.

Аналогично восстанавливаются остальные байты ключа.

Стеганография

Классическая стеганография

Скрытие носителя информации

Симпатические чернила

Микронадписи и микроточки

Литературные приемы

- пустышечный шифр – читаются некоторые буквы или слова
- акростих – первые буквы строк стиха
- решетка Кардано – трафарет для чтения нужных букв
- аллюзия – определенные фразы, которые понимает получатель

Семаграммы – сообщение из любых символов кроме букв и цифр

Компьютерная стеганография

- Передача конфиденциальной информации.
- Преодоление систем мониторинга.
- Камуфлирование программного обеспечения.
- Защита авторских прав.

https://sesc-infosec.github.io/