

Лекция

Криптосистемы с открытым ключем

- Лектор: профессор Яковлев В.А.

Хронология развития систем ЭЦП

- 1976 г. – открытие М. Хэлменом и У. Диффи асимметричных криптографических систем;
- 1978 г. – Р. Райвест, А. Шамир, Л. Адельман – предложили первую систему ЭЦП, основанную на задаче факторизации большого числа;
- 1985 г. – Эль Гамаль предложил систему ЭЦП, основанную на задаче логарифмирования в поле чисел из p элементов;
- 1991 г.- Международный стандарт ЭЦП ISO/IEC 9796 (вариант РША);
- 1994 г. – Стандарт США FIPS 186 (вариант подписи Эль Гамалья);
- 1994 г. – ГОСТ Р 34.10-95 (вариант подписи Эль Гамалья);
- 2000 г. – Стандарт США FIPS 186 – 2;
- 2001 г. – ГОСТ Р 34.10-01 (ЭЦП на основе математического аппарата эллиптических кривых).

Односторонняя функция

Пусть X и Y дискретные множества. Функция $y=f(x)$, где $x \in X$, $y \in Y$ называется односторонней (однонаправленной),

если y легко вычисляется по любому x , а обратная функция $x=f^{-1}(y)$ является трудно вычислимой.

Пример ОФ.

$y=a^x \pmod{p}$, где p - простое число, x - целое число, a - примитивный элемент поля Галуа $GF(p)$. То есть a такое число, что все его степени $a^i \pmod{p}$, $i=1,2,\dots,p-1$, принимают все значения в множестве чисел от 1 до $p-1$.

Пример односторонней функции функции

Пусть $p=7$, $a=3$.

Проверим, что a примитивный элемент -

$a^1 = 3(\text{mod } 7)$, $a^2 = 2(\text{mod } 7)$, $a^3 = 6(\text{mod } 7)$, $a^4 = 4(\text{mod } 7)$,

$a^5 = 5(\text{mod } 7)$, $a^6 = 1(\text{mod } 7)$.

Если $x=4$, то $y=3^4(\text{mod } 7)=4$.

Сложность нахождения функции возведения в степень $N_v = O(2 \log p)$.

Обратная функция $x = \log_a y$ (функция дискретного логарифмирования) трудно вычислима.

Если p - сильно простое число, то $N_{\log} = O((p)^{1/2})$.

$$p = 2^{1000}$$

Оценки сложности вычислений прямой и обратной функций

- Пусть $p = 2^{1000}$ 1000 разрядное двоичное число, тогда для решения задачи возведения в степень числа x по mod p потребуется примерно $2000 = 2 \cdot 10^3$ операций, а для нахождения логарифма такого числа потребуется примерно $p^{1/2} = 2^{500} \sim 10^{170}$ операций, что вычислительно невозможно осуществить ни за какое реально обозримое время.

Односторонняя функция с потайным ХОДОМ

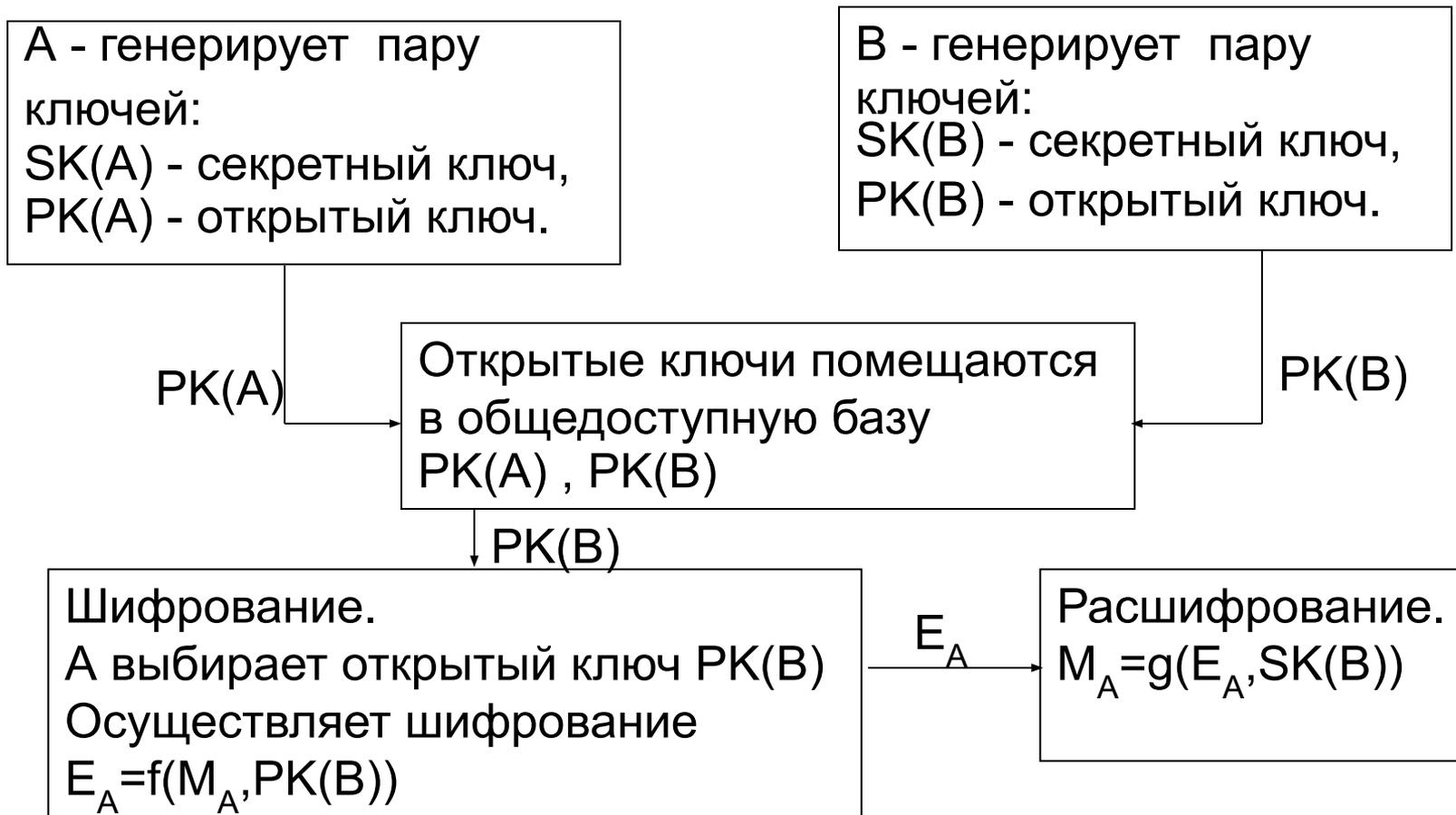
Это не просто ОФ, обращение которой невозможно, она содержит потайной ход (trapdoor), который позволяет вычислять обратную функцию, если известен секретный параметр - ключ.

$y=f(x,s)$ – легковычислима;

$x=f^{-1}(y)$ – трудновычислима;

$x=f^{-1}(y,s)$ - легковычислима.

Общий принцип построения криптосистемы с открытым ключем

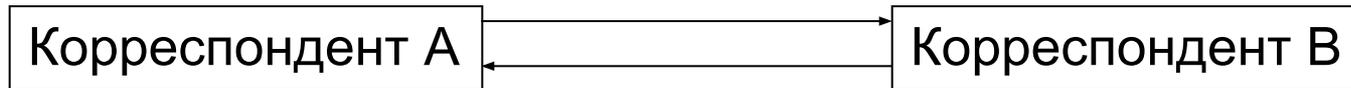


Требования к системам с открытым ключем

1. Вычисление пары ключей PK, SK должно быть просто решаемой задачей;
2. При известном ключе шифрования PK вычисление криптограммы $E=f(M,PK)$ должно быть простым;
3. При известном ключе расшифрования SK восстанавливает сообщение $M=g(E,SK)$ должно быть простым;
4. При известном ключе шифрования PK вычисление ключа расшифрования SK должно быть сложным;
5. При известном ключе шифрования PK , но неизвестном ключе расшифрования SK вычисление M по известной криптограмме E должно быть весьма сложным.

Система шифрования Эль-Гамала

Пусть p - простое число; a - примитивный элемент.



Генерирование пары открытых ключей

А - генерирует число x_A ,
вычисляет открытый ключ
 $y_A = a^{x_A} \pmod{p}$. (SK = x_A , PK = y_A).

y_A передается корр. В.

Шифрование сообщения

Пусть корр. В хочет послать корр. А сообщение $m < p$.

Генерирует случайное число $k < p$.
Формирует криптограмму $E = (c_1, c_2)$
 $c_1 = a^k \pmod{p}$, $c_2 = m \cdot (y_A^{-1})^k$.

Отправляет E корр. А.

Система шифрования Эль-Гамала

Расшифрование сообщения.

Корр.А вычисляет $c_1^x \pmod{p} = a^{kx} \pmod{p}$,

Затем находит

$$c_2 a^{kx} \pmod{p} = m \cdot (y_A^{-1})^k a^{kx} \pmod{p} = m \cdot a^{-xk} a^{kx} \pmod{p} = m$$

Замечание.

Как найти y_A^{-1} ?

$$y_A^{p-2} \pmod{p} = y_A^{p-1} \pmod{p} \cdot y_A^{-1} \pmod{p} = y_A^{-1} \pmod{p}$$

Стойкость системы Эль-Гамала

1. Раскрытие секретного ключа эквивалентно решению задачи дискретного логарифмирования.
2. Нахождение m без знания ключа возможно, если случайное число k используется дважды и в одном случае нарушитель знает открытый текст

$$c_2 = m \cdot (y_A^{-1})^k \pmod{p}, \quad c'_2 = m' \cdot (y_A^{-1})^k \pmod{p}$$

Зная c_2, c'_2 и m несложно найти m' $m' = c'_2 \cdot m \cdot c_2^{-1} \pmod{p}$

k должно меняться случайным образом при шифровании нового сообщения.

Пример системы Эль-Гамала

$p=11$, $a=4$, a - примитивный элемент $GF(2^p)$

Пусть $x=3$ – закрытый ключ

$y=4^3(\bmod 11)=64(\bmod 11)=9$ открытый ключ

у

у

Шифрование сообщения $m=6$

Генерирование СЧ $k=4$

Вычисление:

$$C_1 = a^k(\bmod p) = 4^4(\bmod 11) = 256(\bmod 11) = 3$$

$$y^{-1} = y^{p-2}(\bmod p) = 9^9(\bmod 11) = 9^2 9^2 9^2 9^2 9(\bmod 11) = 4 * 4 * 4 * 4 * 9(\bmod 11) = 5 * 5 * 9(\bmod 11) = 5$$

$$C_2 = m y^{-1k}(\bmod p) = 6 * 5^4(\bmod 11) = 6 * 3 * 3(\bmod 11) = 10$$

C_1, C_2

C_1, C_2

Расшифрование

$$C_1^x(\bmod p) = 3^3(\bmod 11) = 5$$

$$C_2 * C_1^x(\bmod p) = 10 * 5(\bmod 11) = 50(\bmod 11) = 6$$

Система RSA (1978г.)

Генерирование ключей.

Случайно выбираются два простых числа p и q . Находится модуль $N=pq$. Находится функция Эйлера $\phi(N)=(p-1)(q-1)$.

Выбираем число e такое, что $\text{НОД}(e, \phi(N))=1$.

Находим d , как обратный элемент к e , $de=1(\text{mod } \phi(N))$.

Объявляем $d=SK$, $(e,N)=PK$. PK сообщается всем корреспондентам.

Шифрование.

Корр. А передает зашифрованное сообщение корр.В
(использует открытый ключ корр. В)

$$E=m^e(\text{mod}N)$$

Расшифрование.

Корр. В расшифровывает принятую криптограмму от корр.А,используя свой секретный ключ.

$$m=E^d(\text{mod}N)$$

Доказательство обратимости операции дешифрования операции шифрования

Покажем, что $E^d(\text{mod } N) = (m^e)^d(\text{mod } N) = m$

По т. Эйлера $m^{\phi(N)} \equiv 1(\text{mod } N)$ для любого m взаимно простого с N .

Умножая обе части сравнения на m , получаем сравнение

$m^{\phi(N)+1} \equiv m(\text{mod } N)$ справедливое уже для любого целого m .

Перепишем соотношение $ed \equiv 1(\text{mod } \phi(N))$ в виде $ed = 1 + k\phi(N)$

для некоторого целого k .

Тогда $E^d = (m^e)^d = m^{1+k\phi(N)} = m^{1+\phi(N)} m^{(k-1)\phi(N)} =$
 $= m \cdot m^{(k-1)\phi(N)} = m^{1+(k-1)\phi(N)} = m^{1+\phi(N)} m^{(k-2)\phi(N)} =$
 $\dots = m^{1+\phi(N)} = m$

Что и требовалось доказать.

Пример системы RSA

$$p=3, q=11 \quad N=33 \quad \varphi(N) = 20$$

Генерирование ключей

$$e=7, \text{НОД}(7,20)=1$$

$$d=7^{-1}(\text{mod}20) = 3$$

Шифрование

$$m=6 \quad E=m^e(\text{mod}N)=6^7(\text{mod}33)=6^2 6^2 6^2 6^1(\text{mod}33)=3*3*3*3*2=30$$

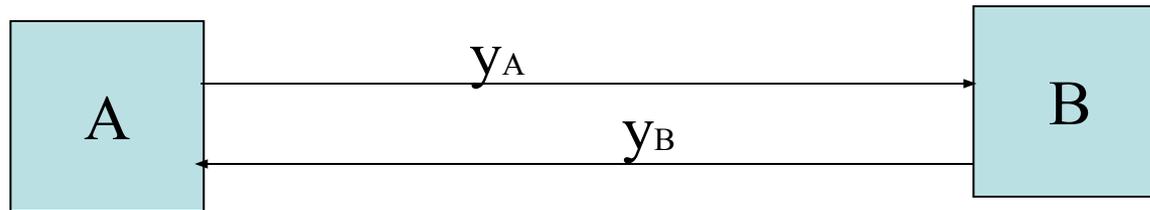
Расшифрование

$$E^d(\text{mod}N)=30^3(\text{mod}33)=900*30(\text{mod}33)=9*30(\text{mod}33)=6$$

Оценки стойкости системы RSA

1. Нахождение чисел p и q по известному модулю N . Задача факторизации имеет сложность $O((N)^{1/2})$.
2. Будем последовательно возводить полученную криптограмму в степень равную значению открытого ключа т.е. $(((((E^e)^e) \dots)^e)^e$. Если при некотором шаге окажется, что $E_i = E$, то это означает, что $E_{i-1} = m$. Доказывается, что данная атака требует непереборно большого числа шагов.
3. Поиск слабых ключей, для которых $m^{e'} = m$, т.е. возведение в степень не меняет сообщения. Эта атака имеет малую вероятность успеха, если p и q выбираются среди сильно простых чисел. Сильно простое число, это число, для которого $p-1$ не содержит в разложении маленьких сомножителей, и имеет в разложении хотя бы один большой сомножитель.
- 4.

Алгоритм формирования ключей на основе однонаправленных функций (алгоритм Диффи-Хеллмана)



А генерирует большое случайное число x_A , $1 \leq x_A \leq p-1$, p - простое число. Число x_A сохраняется в секрете. Вычисляет число $y_A = \alpha^{x_A} \pmod{p}$, где α - примитивный элемент поля $GF(p)$, которое передает корреспонденту В.

В генерирует x_B , аналогичным образом вычисляет число y_B , которое передает корреспонденту А.

А, приняв от В y_B , вычисляет

$$K_A = (y_B)^{x_A} \bmod p = (\alpha^{x_B})^{x_A} \bmod p = \alpha^{x_B x_A} \bmod p .$$

В, приняв y_A , вычисляет

$$K_B = (y_A)^{x_B} \bmod p = (\alpha^{x_A})^{x_B} \bmod p = \alpha^{x_A x_B} \bmod p .$$

$$K_A = K_B = K .$$

Ключ K может быть использован в симметричной системе шифрования.

Гибридные системы шифрования

