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 Гамаля);**
- **1994 г. – ГОСТ Р 34.10-95 (вариант подписи Эль Гамаля);**
- **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.
$y=a^x(\mathrm{mod}\,p)$, где p- простое число, x - целое число,
a -примитивный элемент поля Галуа GF(p). То есть a такое число, что все его степени $a^i(\mathrm{mod}\,p)$, i= 1,2…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(mod7), a^2 =2(mod7), a^3 =6(mod7), a^4 =4(mod7), a^5 =5(mod7), a^6 =1(mod7).
Если x=4, то y=34(mod7)=4.

Сложность нахождения функции возведения в степень $N_в$=O(2logp).
Обратная функция $x=\log_a y$ (функция дискретного логарифмирования) трудно вычислима.
Если p - сильно простое число, то $N_{лог}=O((p)^{1/2})$.

$$p = 2^{1000}$$

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 modp потребуется примерно 2000 = $2*10^3$ операций , а для нахождения логарифма такого числа потребуется примерно

$p^{1/2}=2^{500}\sim10^{170}$ 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-Гамаля

Пусть p -простое число; a - примитивный элемент.

Корреспондент A $\rightleftarrows$ Корреспондент B

Генерирование пары открытых ключей

A - генерирует число x_A,
вычисляет открытый ключ
$y_A=a^x$ (modp). (SK= x_A , PK= y_A).

y_A передается корр. B.

Шифрование сообщения

Пусть корр. B хочет послать корр.A сообщение m<p.
Генерирует случайное число k<p.
Формирует криптограмму $E=(c_1c_2)$
$c_1=a^k(\mathrm{mod}p)$, $c_2=m\cdot(y_A^{-1})^k$.
Отправляет E корр. A.

Система шифрования Эль-Гамаля

Расшифрование сообщения.
Корр.А вычисляет c_1^{x} (modp) = a^{kx} (modp) ,
Затем находит
$c_2 a^{kx}$ (modp)= $m \cdot (y_A^{-1})^k a^{kx}$ (modp)= $m \cdot a^{-xk} a^{kx}$ (modp)=m

Замечание.
Как найти y_A^{-1} ?

y_A^{p-2} (modp)= y_A^{p-1} (modp) $\cdot$ y_A^{-1} (modp) = y_A^{-1} (modp)

Стойкость системы Эль-Гамаля

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' $\quad m' = c'_2 \cdot m \cdot c_2^{-1} \pmod p$

k должно меняться случайным образом при шифровании нового сообщения.

Пример системы Эль-Гамаля

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

Пусть $x=3$ – закрытый ключ

$y=4^3(mod11)=64(mod11)=9$ открытый ключ

$\boxed{y} \longrightarrow \boxed{y}$

Шифрование сообщения $m=6$

Генерирование СЧ $k=4$

Вычисление:

$C_1=a^k(modp)=4^4(mod11)=256(mod11)=3$

$y^{-1}=y^{p-2}(modp)= 9^9(mod11)=9^2 9^2 9^2 9^2 9(mod11)=$

$4*4*4*4*9(mod11)=5*5*9(mod11)=5$

$C_2=my^{-1k}(modp)=6*5^4(mod11)=6*3*3(mod11)=10$

$\boxed{C_1,C_2} \longleftarrow \boxed{C_1,C_2}$

Расшифрование

$C_1^x\ (modp)=3^3(mod11)=5$

$C_2*C_1^x\ (modp)=10*5\ (mod11)=50(mod11)=\mathbf{6}$

Система РША (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 НОД(e, $\phi(N)$)=1.

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

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

Шифрование.

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

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

Расшифрование.

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

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

Доказательство обратимости операции дешифрования операции шифрования

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

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

Умножая обе части сравнения на m, получаем сравнение

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

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

для некоторого целого k.

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

$= m \cdot m^{(k-1)\phi(N)} = m^{1+(k-1)\phi(N)} = m^{1+\phi(N)}\, m^{(k-2)\phi(N)} =$

$\ldots = m^{1+\phi(N)} = m$

Что и требовалось доказать.

Пример системы РША

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

Генерирование ключей
e=**7**, НОД(7,20)=1
$d=7^{-1}(mod20)$ = **3**

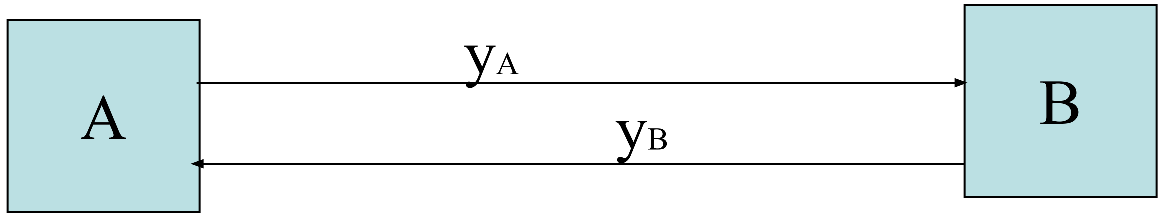
Шифрование
m=**6** $E=m^e(modN)= 6^7(mod33)=6^2\,6^2\,6^2\,6^1(mod33)=$
=3*3*3*3*2=30

Расшифрование
$E^d(modN)=30^3(mod33)=900*30(mod33)=9*30(mod33)=$**6**

Оценки стойкости системы РША

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. $(((((E^e)^e)\ldots..)^e$. 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**,** $1 \le x_A \le p-1$**,** p **- простое число. Число** x_A **сохраняется в секрете. Вычисляет число** $y_A = \alpha^{x_A} (\mathrm{mod}\, p)$**, 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