Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 15 - ЭЦП

Система цифровой подписи в общем виде.
$G(), S(\cdot,\cdot), V(\cdot,\cdot,\cdot)$:

- $(pk, sk) := G()$
- $\sigma := S(sk, m)$
- $v := V(pk, m, s) \in \{0, 1\}$
- $\forall (pk, sk)\ V(pk, m, S(sk, m)) = 1$

pk всем известен.
Поэтому *каждый* может проверить подпись.

ЭЦП и MAC

$A \xrightarrow{m,\, t(m)} B$

$A \xrightarrow{m,\, \sigma(m)} B$

MAC	ЭЦП
A,B знают k_{AB} A создает $t_{AB} := MAC(k_{AB}, m)$ B проверяет целостность m	A знает (pk_A, sk_A); B знает pk_A A создает $\sigma_A := S(sk_A, m)$ B проверяет целостность m
$\forall m'$ B может создать $MAC(k_{AB}, m)$	B не может создать $S(sk_A, m')$
m двум получателям: $t_{AB} := MAC(k_{AB}, m)$ $t_{AC} := MAC(k_{AC}, m)$	m двум получателям: $\sigma_A := S(sk_A, m)$
	Арбитр тоже знает pk_A B м. предъявить арбитру (s, m)

MAC:
- целостность сообщения при передаче
- проверяется приватно
- могут создать обе стороны

ЭЦП:
- целостность сообщения при передаче
- проверяется любым желающим
- невозможность отказа от авторства документа

Эксперимент:

1. $(pk, sk) := G()$, n - параметр длины ключа
2. $pk \to A$ и доступ к ч.я. (оракулу) $S(sk, \cdot)$ - создает подписи сообщений
3. A получает подписи сообщений $m_1, ..., m_q$.
4. A выбирает $m \neq m_i$, создает $\sigma(m)$.
5. $b = V(pk, m, \sigma)$

Опр.

Алгоритм ЭЦП (G, S, V) наз. *стойким к атаке с выбором сообщения* (existentially unforgeable), если $\forall A \in \mathrm{BPP}$ $P(b = 1) < \varepsilon(n)$

Раздел 15 - ЭЦП

Общий вид

ЭЦП RSA

ЭЦП по Эль Гамалю

ЭЦП DSA

Подпись “RSA из учебника”

1. $(N, e, d) := G()$. При ЭЦП d - секретный ключ, (N, e) - о.к.
2. $m \in \mathbb{Z}_N^*$, $\sigma := m^d \bmod N$
3. $V(e, m, \sigma):\ \sigma^e \bmod N \stackrel{?}{=} m$
4. Корректность очевидна.

Атаки на "RSA из учебника"

1. Создание новой верной пары сообщение, подпись. Значение сообщения зависит от подписи.

Зл-к знает (N, e). Возьмет $\forall x \in \mathbb{Z}_n$. $m := x^e \bmod N$. Пара (m, x) - верная: $x^e \equiv m \bmod N$.

Подпись "RSA из учебника" не стойкая.

2. Коммутативное свойство подписей.

Если $m = m_1 m_2$ и известны подписи σ_1, σ_2 для m_1, m_2, то $\sigma(m) = \sigma_1 \cdot \sigma_2 \bmod N$

Проверка: $\sigma^e = (\sigma_1\sigma_2)^e = m_1^{de} m_2^{de} = m_1 m_2 = m \bmod N$.

Если получили у оракула подписи для t сообщ., т.о. можно создать подписи для $2^t - t$ новых сообщений.

Hashed RSA

1. $(N, e, d) := G()$. Здесь e - секретный ключ.
2. $H : \{0, 1\}^* \to \mathbb{Z}_N^*$. $\sigma := (H(m))^d \bmod N$
3. $V(e, m, \sigma) :\ \sigma^e \bmod N \stackrel{?}{=} H(m)$
4. Корректность очевидна.

Теорема 1

Hashed RSA стойкая к атаке с выбором сообщения в модели со случайным оракулом.

Без док-ва.

Раздел 15 - ЭЦП

ЭЦП по Эль Гамалю (Taher ElGamal, 1984)

H - крипт. х/ф, p - большое простое, g - $\forall$ генератор $\mathbb{Z}_p^*$,
m - любое.

1. Создание ключа
$x \xleftarrow{R} \{1, ..., p-1\}$
$y := g^x \bmod p$
(p, g, y) - о.к., x - с.к.

2. Подпись.

$k \xleftarrow{R} \mathbb{Z}_{p-1}^*$

$r := g^k \bmod p$

$s := (H(m) - xr)k^{-1} \bmod (p-1)$

если $s = 0$, выбрать другое k

$(r, s) = (g^k \bmod p, s)$ - подпись m.

3. Проверка.
$0 < r < p$,
$0 < s < p - 1$,
$g^{H(m)} \stackrel{?}{=} y^r r^s \bmod p$

4. Корректность.
$H(m) \equiv xr + sk \bmod (p-1)$.
$y^r r^s \bmod p \equiv g^{xr} g^{ks} \equiv g^{H(m)} \bmod p$.

k - случайный, секретный, не повторяется (иначе узнаем x).

Утверждение

Без х/ф ElGamal - не стойкая подпись.

Док-во

По условию, алгоритм $s(m) = (\mathbf{m} - xr)k^{-1} \bmod (p-1)$.

Создадим новую верную пару сообщение, подпись.
Цель: $y^r r^s \equiv g^m \bmod p$.
Пусть $k \xleftarrow{R} \mathbb{Z}_{p-1}^*$. Выберем одновременно r, s, m.

Избавимся от y^r в левой части: хотим $r^s \equiv y^{-r} z \bmod p$ для нек. z.

Док-во (Продолжение.)

Пусть $r := yg^k \bmod p$,
$s := -r \bmod p-1$.

Тогда $y^r r^s \equiv y^r (yg^k)^{-r} \equiv g^{-kr} \bmod p-1$.
Чтобы все сошлось, $m := -kr \bmod p-1$.

Значит, $(r, -r \bmod p-1)$ - верная подпись для
$m \equiv -kr \bmod (p-1)$,
где $r \equiv yg^k \bmod p$,
для произв. фикс. $k \in \mathbb{Z}^*_{p-1}$.

Теорема 2 (О стойкости подписи по ЭльГамалю к атаке с выбором сообщения)

Если зл-к может создать новую подпись по ЭльГамалю в модели со случайным оракулом с не пренебрежимо малой вероятностью, то задача дискретного логарифма может быть решена за полиномиальное время.

Без док-ва.

Замеч.: Т.о. свели решение задачи дискретного логарифма к атаке на подпись. Считается, что дискретный логарифм - трудная задача.

Пример (Подпись по Эль-Гамалю)

$p = 11, g = 2, x = 8$
$y = g^x \bmod p = 2^8 \bmod 11 = 3$
о.к: 11, 2, 3.

Подпишем сообщение m: $H(m) = 5$.
Выберем случайное $k = 9$, НОД$(9, 11 - 1) = 1$.
$a = g^k \bmod p = 2^9 \bmod 11 = 6$
$5 = (8 * 6 + 9 * b) \bmod 10 \ \Rightarrow b = 3 \ \ (ExtGCD)$
Подпись: пара $a = 6, b = 3$.

Проверка: $y^a a^b \bmod\ p \overset{?}{=} g^{H(m)} \bmod\ p$, т.е.
$3^6 * 6^3 \bmod 11 \overset{?}{=} 2^5 \bmod 11$ - верно.

Раздел 15 - ЭЦП

DSA - стандарт цифровой подписи США. (DSS: 1991, FIPS 186, -1, -2, -3 (2009))
В ее основе - подпись по ElGamal.

1. Создание ключа
p - простое длины L бит, (от 512 до 3072)
q - простое, длины N бит (от 160 до 256), делитель $p-1$.
(NSA предл. спец. алгоритм генерации p, q.)

Нужен $\forall$ элемент $g \in \mathbb{Z}_p^*$ порядка q.
Найдем его: если $h^{(p-1)/q} \bmod p \neq 1$, тогда
$g := h^{(p-1)/q} \bmod p$.
Поиск - перебором h.

$x \xleftarrow{R} \{1, q-1\}$ - с. к.,
$y := g^x \bmod\ p$. (p, q, g, y) - о.к.

Утверждение

$g^{x+y} \bmod p = g^{(x+y) \bmod q} \bmod p,$
$g^{x \cdot y} \bmod p = g^{x \cdot y \bmod q} \bmod p$

Док-во

$g^{x+y} \bmod p = g^{(x+y) \bmod q + qn} \bmod p \overset{g^q = 1}{=} g^{(x+y) \bmod q} \bmod p.$
Аналогично для произведения.

с.к. $x \xleftarrow{R} \{1, q-1\}$, о.к. $y := g^x \bmod p$.

2. Подпись.
$k \xleftarrow{R} \{1, q-1\}$
$r := (g^k \bmod p) \bmod q$
$s := (H(m) + xr)k^{-1} \bmod q$
Подпись - это пара (r, s).

3. Проверка:
$u_1 = (H(m) \cdot s^{-1}) \bmod q$
$u_2 = (rs^{-1}) \bmod q$
$v = (g^{u_1} \cdot y^{u_2} \bmod \ p) \bmod q.$
$v \stackrel{?}{=} r$

4. Корректность:
$k = (H(m) + xr)s^{-1} \bmod q$
Т.к. $g^q = 1 \bmod p$, то
$g^k = g^{H(m)s^{-1}} g^{xrs^{-1}} = g^{H(m)s^{-1}} y^{rs^{-1}} = g^{u_1} y^{u_2} \bmod p$

$r = (g^k \bmod p) \bmod q = g^{u_1} y^{u_2} \bmod p \bmod q = v$ - верно.

k - случайный, секретный, не повторяется (иначе узнаем x).

Пример

Sony Playstation 3 (2010): $k = const$. Хакеры нашли секретный ключ подписи ECDSA.

Задача

Пусть k известно и фиксировано. Найти x.

Теорема 3 (О стойкости DSA к атаке с выбором сообщения)

Если зл-к может создать новую подпись DSA в модели со случайным оракулом с не пренебрежимо малой вероятностью, то задача дискретного логарифма в группе $\mathbb{Z}_p^*$ может быть решена за полиномиальное время.

Без док-ва.

Следствие:

Необх. условия стойкости подписи DSA и Эль-Гамаль:
- k - выбир. случайно, равномерно, не повторяется
- H - уст. к коллизиям
- задача дискретного логаримфа сложная в группе $\mathbb{Z}_p^*$.

"Побочный эффект": перестановка RSA с пом. DSA. (*)

Пусть $DSAsign(p, q, g, k, x, r, s)$ - функция подписи DSA.
n - модуль, $m \in \mathbb{Z}_n$ - сообщение.
Пусть e - открытый ключ. RSA-шифр-е:
$DSAsign(n, n, m, e, 0, r, 0)$. r - шифротекст.

$r := (m^e \bmod n) \bmod n$
$s := e^{-1} \cdot H(m) \bmod n$

Пусть d - секретный ключ. Тогда расшифр-е:
$DSAsign(n, n, m, d, 0, r, 0)$. m - сообщение.

Литература к лекции

1. Pointcheval, Stern. "Security Proofs for Signature Schemes" (Описание и стойкость подписи ElGamal)
http://www.di.ens.fr/~pointche/Documents/Papers/1996_eurocrypt.pdf

2. Vaudenay, "The Security of DSA and ECDSA",
https://www.iacr.org/archive/pkc2003/25670309/25670309.pdf

3. Обзор разных протоколов ЭЦП:
http://courses.cs.tamu.edu/pooch/665_spring2008/Australian-sec-2006/less19.html