# Цифровая подпись

Тукнов Алексей 25/10 2005

# План доклада

- 1. Введение в проблему. Какая подпись нас удовлетворяет.
- 2. Варианты реализации цифровой подписи. Дайджесты.
- 3. Обзор стандартов.

# 1. Введение в проблему.

2 проблемы: 1.Сохранение информации от несанкционированного доступа.

2. Подтверждение авторства (принадлежность информации определенному лицу).

# 1. Введение в проблему.

2 проблемы: 1.Сохранение информации от несанкционированного доступа

2. Подтверждение авторства (принадлежность информации определенному лицу)

Соответственно: 1. Шифрование

2. Электронная цифровая подпись

# Качества подписи.

# Качества подписи.

- 1. Подпись достоверна. Она убеждает получателя в том, что подписавший сознательно подписал документ.

# Качества подписи.

- 1. Подпись достоверна. Она убеждает получателя в том, что подписавший сознательно подписал документ.

- 2. Подпись неподдельна. Она доказывает, что именно подписавший сознательно подписал документ.

# Качества подписи.

- 1. Подпись достоверна. Она убеждает получателя в том, что подписавший сознательно подписал документ.
- 2. Подпись неподдельна. Она доказывает, что именно подписавший сознательно подписал документ.
- 3. Подпись не может быть использована повторно. Она – часть документа. Злоумышленник не сможет перенести подпись на другой документ.

# Качества подписи.

- 1. Подпись достоверна. Она убеждает получателя в том, что подписавший сознательно подписал документ.
- 2. Подпись неподдельна. Она доказывает, что именно подписавший сознательно подписал документ.
- 3. Подпись не может быть использована повторно. Она – часть документа. Злоумышленник не сможет перенести подпись на другой документ.
- 4. Подписанный документ нельзя изменить.

# Качества подписи.

- 1. Подпись достоверна. Она убеждает получателя в том, что подписавший сознательно подписал документ.
- 2. Подпись неподдельна. Она доказывает, что именно подписавший сознательно подписал документ.
- 3. Подпись не может быть использована повторно. Она – часть документа. Злоумышленник не сможет перенести подпись на другой документ.
- 4. Подписанный документ нельзя изменить.
- 5.От подписи невозможно отказаться. Подпись и документ материальны. Подписавший не сможет утверждать, что он не подписывал документ.

# Подпись с помощью RSA

- 1. Алиса шифрует документ своим секретным ключом.
- 2. Алиса посылает документ Бобу.
- 3. Боб расшифровывает документ открытым ключом.

Совпадение исходного и расшифрованного документа <=>
<=> подпись прошла успешно.

Нотариус: нужен лишь для подтверждения того, что открытый ключ принадлежит Алисе.

Подпись с RSA соответствует требованиям:
достоверность,
невозможность подделать(private key принадлежит Алисе),
невозможность использовать повторно (подпись – функция документа),
невозможно изменить подписанный документ,
от подписи нельзя отказаться.

Боб может мошенничать.

## Боб может мошенничать: повторное использование документа.

1. Контракт – не имеет значение количество его копий.
2. Чек на 150 000 $, посылаемый в Банк – имеет значение.

Боб может мошенничать: повторное использование документа.

1. Контракт – не имеет значение количество его копий.
2. Чек на 150 000 $, посылаемый в Банк – имеет значение.

Решение: метка времени, добавляемая к документу, и подписываемая вместе с сообщением.

При повторном приходе Боба – банк смотрит на метку и ловит Боба.

Боб может мошенничать: повторное использование документа.

1. Контракт – не имеет значение количество его копий.
2. Чек на 150 000 $, посылаемый в Банк – имеет значение.

Решение: метка времени, добавляемая к документу, и подписываемая вместе с сообщением.

При повторном приходе Боба – банк смотрит на метку и ловит Боба.

При подписи больших документов RSA неэффективен.

Решение: дайджест (хэш-функции).

p.s.: ФЕДЕРАЛЬНЫЙ ЗАКОН 10.01.2002 №-ФЗ ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Принят Государственной Думой 13 декабря 2001 года Одобрен Советом Федерации 26 декабря 2001 года

” Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.”…

# Дайджесты сообщений

Дайджест – представитель данных.

При больших объемах документа Алиса подписывает значение хэш-функции для документа (SHA-1, MD5).

Document.length = x;

For any document: digest(document).length = y; //для SHA-1 20 байт

1. Алиса вычисляет Hash(document). Шифрует его секретным ключом. Посылает Бобу.
2. Боб расшифровывает сообщение публичным ключом. Сравнивает с Hash(document), вычисленным им самим.

+ требуется меньше памяти для хранения подписанных документов

# Как A и B подписать документ одновременно?

1. Алиса подписывает Hash(document).
2. Боб подписывает Hash(document).
3. Боб посылает свою подпись Алисе.
4. Алиса посылает нотариусу document, свою подпись, подпись Боба.
5. Нотариус проверяет подписи.

## Как A и B подписать документ одновременно?

1. Алиса подписывает Hash(document).
2. Боб подписывает Hash(document).
3. Боб посылает свою подпись Алисе.
4. Алиса посылает нотариусу document, свою подпись, подпись Боба.
5. Нотариус проверяет подписи.

Алиса мошенничает! : подписывает документ, теряет свой секретный ключ и утверждает, что ее подпись скомпрометирована.

- Метки времени.

DSA

Эль-Гамаль

RSA

ГОСТ Р 34.10-94

Elliptic Curves Cryptography

# Схема шифрования ElGamal.

Пусть $p$ – большое простое число, $g$ – примитивный элемент мультипликативной группы GF($p$),
$x$ случайное число, $x < p$-1.

$y = g^x \pmod p$ -открытый ключ,

$\boldsymbol{x}$ –секретный ключ.

Пусть надо зашифровать сообщение $M<p$:

1. Выбирается случайное число $k$, взаимно-простое с $p$ - 1.
2. Затем вычисляется

$$a = g^k \pmod p$$

$$b = y^k \cdot M \pmod p$$

Шифртекстом является пара ($a$, $b$).

При расшифровании вычисляется $a^x$ **и** $b/a^x \pmod p$,

$$b/a^x \equiv y^k \cdot M/a^x \equiv g^{k \cdot x}\, M/g^{k \cdot x} \equiv M \pmod p$$

# Подпись ElGamal.

Для генерации ключевой пары выбираются большое простое число $p$ и примитивный элемент g мультипликативной группы GF(p).
Выбирается случайное число $x$ такое, что $x < p$-1.

Открытым ключом является $y = g^x \pmod p$; секретным ключом является $x$.

Схема ElGamal может быть использована для подписи в электронных деньгах и для зашифрования.
Стойкость основана на сложности дискретного логарифмирования.

Пусть $A$ должен подписать сообщение $M$. Выбирается случайное число $k$, взаимно-простое с $p$-1: НОД($k$; $p$-1) = 1. Затем вычисляется

$a = g^k \pmod p$.

Рассмотрим уравнение

$M = (x \cdot a + k \cdot b) \pmod{(p-1)}$.

По теореме о вычетах $\exists\, k^{-1}$: $(M - xa)\, k^{-1} \equiv b \pmod{(p-1)}$. Подписью под $M$ является пара ($a$, $b$).

Проверка подписи:

Вычисляем $g^M (p)$ и $y^a \cdot a^b (p)$. Проверяем

$$y^a \cdot a^b \pmod p = g^{a \cdot x} \cdot g^{k \cdot b} \pmod p = g^{a \cdot x + k \cdot b} \pmod p =$$

$$= g^{ax + kk^{-1}(M - xa) + (p-1)nk} \pmod p = g^{M + (p-1)nk} \pmod p = g^M \pmod p.$$

# *DSA (DSS)*

В основе DSA(DSS) (Digital Signature Algorithm (Digital Signature Standard )) [DSS 94] лежит подпись El число, $q$ – простое число, такое, что $q|(p\text{-}1)$ и $g$ имеет мультипликативный порядок $q$, то есть $g^q = 1(\mathrm{mod}p)$.

***Лемма.*** Мультипликативные вычисления степеней $g$ по модулю $p$ эквивалентны арифметическим вычи модулю $q$.

**Доказательство.**

$g^x g^y \pmod{p} = g^{x+y} \pmod{p} = g^{(x+y)(\mathrm{mod}q)+qn} \pmod{p} =$

$= g^{(x+y)(\mathrm{mod}q)} g^{qn} \pmod{p} = g^{(x+y)(\mathrm{mod}q)} \pmod{p}.$

Аналогично

$(g^x)^y \pmod{p} = g^{xy(\mathrm{mod}q)} \pmod{p},$

что и требовалось доказать.

В DSS выбирают $p\sim$ 512 бит, $q\sim$ 160 бит. Пусть $x$ $x< p\text{-}1$. Тогда $x$ – секретный ключ, а

$y = g^x(\mathrm{mod}p)$ –

открытый ключ. Алгоритм подписи сообщения $M$ выглядит следующим образом.

1. Выбирается случайное число $k<q$. Так как НОД$(k,q)$ $\exists\ k^{-1}(\mathrm{mod}q)$.
2. Вычисляется $r = [g^k(\mathrm{mod}p)](\mathrm{mod}q)$.
3. Вычисляется $s = k^{-1}(M + xr)(\mathrm{mod}q)$.

Подписью сообщения $M$ является пара $(r,s)$.

Проверка подписи осуществляется следующим образом. Вычисляется

$w = s^{-1}(\mathrm{mod}q).$

Это можно сделать, так как $q$ простое число.

$u_1 = (Mw)(\mathrm{mod}q),$

$u_2 = (rw)(\mathrm{mod}q), \quad v = [(g^{u_1} y^{u_2})(\mathrm{mod}p)](\mathrm{mod}q).$

Если выполняется равенство $v = r$, то подпись подтверждена.

**Доказательство.**

$v = [(g^{u_1} y^{u_2})(\mathrm{mod}p)](\mathrm{mod}q).$

Тогда по лемме

$v = [(g^{M\cdot s^{-1}(\mathrm{mod}q)} g^{xr\cdot s^{-1}(\mathrm{mod}q)})(\mathrm{mod}p)](\mathrm{mod}q) = [(g^{s^{-1}(M+xr)(\mathrm{mod}q)})(\mathrm{mod}p)](\mathrm{mod}q) = [g^k(\mathrm{mod}p)](\mathrm{mod}q) = r.$

# *ГОСТ 3410.94.*

Пусть $p$ – простое число размера 509÷512 бит,
$q$ простое число такое, что $q|(p-1)$.
Число $g<p-1$ имеет мультипликативный порядок $q$, то есть $g^q = 1(\mathrm{mod}p)$.

$p$, $q$, $g$ открыты.
Число $x$, $x<q$, –секретный ключ, открытым ключом является $y = g^x(\mathrm{mod}p)$.

Алгоритм подписи сообщения $M$ выглядит следующим образом:

1. Выбирается случайное число $k$.
2. Вычисляется
$r = [g^k(\mathrm{mod}p)](\mathrm{mod}q)$.
3. Вычисляется
$s = (Mk + xr)(\mathrm{mod}q)$.

Подписью сообщения $M$ является пара $(r,s)$.

Проверка подписи осуществляется следующим образом. Вычисляются
$v = M^{q-2}(\mathrm{mod}q)$,
$z_1 = (sv)(\mathrm{mod}q)$,
$z_2 = ((q-r)v)(\mathrm{mod}q)$,
$u = [(g^{z_1} y^{z_2})(\mathrm{mod}p)](\mathrm{mod}q)$.
Если выполняется равенство $u = r$, то подпись подтверждена.

**Доказательство:**

$$u = [(g^{z_1} y^{z_2})(\mathrm{mod}p)](\mathrm{mod}q) =$$
$$= [(g^{(xr+kM)M^{q-2}(\mathrm{mod}q)+x(q-r)M^{q-2}(\mathrm{mod}q)})(\mathrm{mod}p)](\mathrm{mod}q) =$$
$$= [(g^{xrM^{q-2}(\mathrm{mod}q)+k-xrM^{q-2}(\mathrm{mod}q)})(\mathrm{mod}p)](\mathrm{mod}q) = [g^k(\mathrm{mod}p)](\mathrm{mod}q) = r.$$ **Доказано.**

# Используемая литература


- 1. “Современная прикладная криптография” Андрей Чмора 2002
- 2. “Официальное руководство RSA Security. Криптография.” С. Бернет, С. Пэйн