Математические и компьютерные основы защиты информации

Лекция 9

Антон Николаевич Гайдук | УНИВЕР

vk.com/gaidukedu

06 апреля 2023 г.

Содержание дисциплины

Раздел I Введение

- Тема 1. Введение. История. Основные понятия.

Раздел II Симметричная криптография

- Тема 2 Классические шифры.
- Тема 3 Поточные алгоритмы шифрования.
- Тема 4 Блочные алгоритмы шифрования.

- Тема 5 Функции хэширования.
- Тема 6 Математические методы криптоанализа.

Раздел III Асимметричная криптография

- Тема 7 Протокол Диффи-Хэллмана.
- Тема 8 Криптосистемы с открытым ключом.
- Тема 9 Электронная цифровая подпись.

Раздел III Асимметричная криптография

Тема 9 Электронная цифровая подпись.

- ЭЦП
- Модель ЭЦП
- Схемы ЭЦП
- ECC

ЭЦП

ЭЦП — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием алгоритма выработки электронной цифровой подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость) (алгоритм проверки электронной цифровой подписи).

Алгоритм выработки ЭЦП — алгоритм криптографический вычисления электронной цифровой подписи сообщения с использование ключа секретного (личного), являющийся составной частью системы (схемы) подписи цифровой. Это алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое сообщение, ключ секретный, а также открытые параметры схемы подписи цифровой. Результатом работы алгоритмы является электронная цифровая подпись.

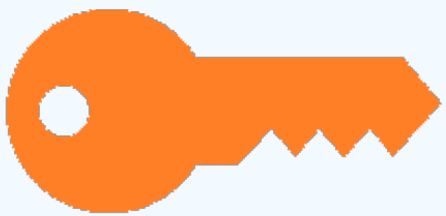
Классификация схем ЭЦП

- С аппендиксом: для выработки и проверки ЭЦП требуется подписываемое сообщение;
- С восстановлением сообщения: сообщение требуется только для выработки ЭЦП, при проверке ЭЦП сообщение восстанавливается из подписи.

- Детерминированные;
- Рандомизированные.

Асимметричная криптография: ЭЦП

Открытый ключ (Public key)



Для проверки подписи

Личный ключ (Private Key)

Для выработки подписи

Модель ЭЦП

- Задание алгоритма генерации (выработки) ключей;
- Задание функции выработки подписи;
- Задание функции проверки подписи;
- Обоснование работоспособности и надежности.

Выработка и проверка подписи ЭЦП

m — сообщение, s — подпись.

Выработка ЭЦП

- Обеспечить доступность открытого ключа k_e для любого желающего проверить подпись.
- Используя некоторую хэш-функцию h вычислить $h(m)$ и затем вычислить $s = sign(h(m), k_d)$, где $sign$ — алгоритм выработки ЭЦП, а k_d — личный (секретный) ключ.

Проверка ЭЦП

- Определить открытый ключ k_e пользователя для которого проверяется подпись.
- Используя хэш-функцию h вычислить $h(m)$ и затем вычислить $verify(h(m), s, k_e)$, где $verify$ — алгоритм проверки ЭЦП s, а k_e — открытый ключ.

Основные требования к ЭЦП

- Получение пары ключей (k_e, k_d) является легко вычислимой задачей.
- Для каждой пары ключей (k_e, k_d) и каждого открытого текста $p \in \mathcal{P}$ функции $sign$, $verify$ легко вычислимы.
- Решение задачи нахождения открытого текста p и соответствующей ему подписи s не зная личный (секретный) ключ является вычислительно трудной задачей.

Схемы ЭЦП

Используемые сегодня схемы ЭЦП можно классифицировать в зависимости от сложности математической задачи, которая лежит в основе их стойкости:

- схемы основанные на трудности факторизации целых чисел, примерами таких схем являются: ЭЦП RSA и ЭЦП Рабина.
- схемы ЭЦП, стойкость которых основана на неразрешимости задачи дискретного логарифмирования над конечным полем, примерами таких схем являются: ЭЦП ElGamal, ЭЦП Шнора, DSA, и ЭЦП Nyberg-Rueppel.
- схемы ЭЦП на основе эллиптических кривых, стойкость которых основана неразрешимости задачи дискретного логарифма на эллиптической кривой.

Схемы ЭЦП

Схемы ЭЦП на основе эллиптических кривых получили широкое распространение благодаря тому, что сравнимый с другими схемами ЭЦП (например, RSA) уровень стойкости достигается при меньших размерах ключа и они более эффективны в реализации.
Криптография на эллиптических кривых основана на предположении, что задача дискретного логарифмирования на эллиптической кривой является трудоемкой. Хотя задача дискретного логарифмирования считается экспоненциальной сложности, в настоящее время не существует доказательств того, что она не решается за полиномиальное время. На сегодняшний день только очень специфический класс эллиптических кривых, те, которые определены над двоичными полями, по мнению некоторых экспертов, допускают субэкспоненциальную сложность задачи дискретного логарифмирования.

Elliptic curve cryptography (ECC)

ECC

Кубическая кривая $\Gamma(\mathbb{F})$ над полем $\mathbb{F}$ определяется многочленом $f(x, y)$ степени 3 от двух переменных. Будем говорить, что точка $P = (x, y) \in \mathbb{F} \times \mathbb{F}$ является *точкой на кривой* $\Gamma(\mathbb{F})$, тогда, когда выполнено

$$f(x, y) = 0,$$

где $f(x, y)$ многочлен задающий кубическую кривую.
Кубическая кривая задаваемая многочленом $f(x, y)$ над полем $\mathbb{F}$

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0, \tag{1}$$

называется эллиптической кривой.

ECC

Точка эллиптической кривой $P = (x_P, y_P) \in \Gamma(\mathbb{F})$ называется сингулярной, если

$$\frac{\partial f}{\partial x}(x_P, y_P) = \frac{\partial f}{\partial y}(x_P, y_P) = 0$$

Эллиптическая кривая не имеющая сингулярных точек называется неособой (несингулярной).
Дискриминантом эллиптической кривой называется величина

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$

где

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1 a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

ECC

j-м инвариантом эллиптической кривой при $\Delta \neq 0$ называется величина

$$j = \frac{c_4^3}{\Delta},$$

где $c_4 = b_2^2 - 24b_4$.

Теорема

Эллиптическая кривая является неособой (несингулярной) тогда и только тогда, когда ее дискриминант ненулевой.

Над конечным полем, производя замену переменных, уравнение эллиптической кривой (1) возможно свести к одному из следующих видов (в зависимости от характеристики конечного поля):

- $y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}$ для полей характеристики не равной два и три.
- $y^2 + xy = x^3 + ax^2 + b$ или $y^2 + cy = x^3 + ax + b$, для полей характеристики равной два.
- $y^2 = x^3 + ax^2 + b$ или $y^2 = x^3 + ax + b$, для полей характеристики равной три.

ECC

На множестве точек эллиптической кривой можно ввести бинарную операцию, которая позволит образовать структуру группы. Для этого к множеству точек эллиптической кривой дополнительно присоединяют точку $\mathcal{O}$, выполняющую роль нейтрального элемента:

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} | y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\mathcal{O}\}.$$

Принято получающуюся при этом группу рассматривать как аддитивную группу, а операцию называть операцией сложения и обозначать, как обычно, знаком плюс.

ECC

Рассмотрим эллиптическую кривую $E : y^2 = x^3 + ax + b$, над полем $\mathbb{F}$ характеристики не равной 2,3

- Для любой точки $P \in E(\mathbb{F})$ выполнено $P + \mathcal{O} = \mathcal{O} + P = P$;
- Для точки $P = (x, y)$ точка $-P$ определена следующим образом $-P = (x, -y)$ и $P + (-P) = \mathcal{O}$;
- Для точек $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ при $P \neq Q$ определим $P + Q = (x_3, y_3)$, где

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ и } y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1;$$

- Для точки $P = (x_1, y_1)$ при $P \neq -P$ определим точку $2P = (x_3, y_3)$, где

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \text{ и } y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

ECC

Введем обозначение для k-кратного сложения произвольной точки P эллиптической кривой $E(\mathbb{F})$:

$$\underbrace{P + P + \cdots + P}_{k \text{ раз}} = kP.$$

Порядком эллиптической кривой $E(\mathbb{F})$ называется число всех ее точек вместе с точкой $\mathcal{O}$.
Порядком точки P эллиптической кривой называется наименьшее натуральное число $n \neq 0$ для которого $nP = \mathcal{O}$.

Задача дискретного логарифмирования на эллиптической кривой состоит в том, чтобы для заданных двух точек P, Q на эллиптической кривой $E(\mathbb{F})$ найти целое число a, такое, что $Q = aP$, если такое a существует.

Пример

Рассмотрим эллиптическую кривую $y^2 = x^3 + 2x + 10$ над полем $\mathbb{F}_{23}$. Здесь $a = 2$ и $b = 10$ и дискриминант эллиптической кривой равен:

$$-16(4a^3 + 27b^2) = -43712 \neq 0 \pmod{23}.$$

Точки (множество пар $(x, y), x, y \in \mathbb{F}_{23}$) на эллиптической кривой следующие:

(1, 6)	(1, 17)	(4, 6)	(4, 17)	(6, 10)
(6, 13)	(8, 3)	(8, 20)	(10, 8)	(10, 15)
(11, 11)	(11, 12)	(13, 5)	(13, 18)	(17, 9)
(17, 14)	(18, 6)	(18, 17)	(20, 0)	

ECC

Пример

Рассмотрим эллиптическую кривую $y^2 = x^3 + 2x + 10$ над полем $\mathbb{F}_{23}$. Для точки $P = (6, 13)$ точка $2P = (1, 17)$. Для точек $P = (6, 13)$ и $Q = (11, 12)$ точка $P + Q = (18, 17)$.

ЭЦП на эллиптических кривых

Существует несколько различных стандартов ЭЦП на эллиптических кривых например: ANSI X9.63 (1999), IEEE P1363 (2000), SEC 2(2000), NIST FIPS 186-2 (2000), Brainpool (2005), NSA Suite B (2005), Certicom SEC 2 v2 (2010), OSCCA SM2 (2010), NIST FIPS 186-4 (2013), СТБ 34.101.45-2013.

ECDSA

ECDSA, состоит из трех различных алгоритмов:

- алгоритм генерации ключей;
- алгоритм выработки подписи;
- алгоритма проверка подписи.

Для всех трех алгоритмов эллиптическая кривая E задается над полем $\mathbb{F} = F_q$, где $q = p$ — простое нечетное число или $q = 2^m$, базовая точка $P \in E(\mathbb{F}_q)$ выбирается так, чтобы порядок точки P равный n удовлетворял соотношению $n > 4\sqrt{q}$ и $n > 2^{160}$.
Алгоритм генерации ключей генерирует пару ключей (Q, d), где Q — открытый ключ, а d — личный (секретный) ключ.
Алгоритм генерации ключей состоит из следующих шагов:

1. Выбрать случайно и равновероятно целое число d так, что $0 < d < n$.
2. Вычислить $Q = dP$.

ECDSA

Входными параметрами алгоритма выработки ЭЦП являются личный ключ d и сообщение m. Выходом является подпись (r, s) сообщения m. Алгоритм выработки подписи состоит из следующих шагов:

1. Выбрать случайно и равновероятно целое число k так, что $0 < k < n$.
2. Вычислить $kP = (x_1, y_1)$.
3. Вычислить $r = x_1 \mod n$, если $r = 0$ перейти к Шагу 1.
4. Вычислить $k^{-1} \mod n$.
5. Вычислить $h = hash(m)$.
6. Вычислить $s = k^{-1}(h + dr) \mod n$, если $s = 0$ перейти к Шагу 1.
7. Вернуть подпись (r, s) для сообщения m.

ECDSA

Входными параметрами алгоритма проверки ЭЦП являются открытый ключ Q сообщение m и подпись (r, s). Алгоритм проверки подписи состоит из следующих шагов:

1. Проверить, что $0 < r < n$ и $0 < s < n$.
2. Вычислить $h = hash(m)$.
3. Вычислить $w = s^{-1} \mod n$.
4. Вычислить $u_1 = hw \mod n$ и $u_2 = rw \mod n$.
5. Вычислить $X = (x_1, y_1) = u_1 P + u_2 Q$.
6. Если $X = \mathcal{O}$, тогда отвергнуть подпись.
7. Если $x_1 \mod n = r$, тогда подпись корректна, иначе отвергнуть подпись.

ЭЦП RSA

Сертификаты

Структура сертификата X.509

- версия (v1, v2, v3);
- серийный номер;
- идентификатор алгоритма подписи;
- имя издателя;
- период действия;
- имя субъекта;
- информация об открытом ключе субъекта (алгоритм открытого ключа, открытый ключ субъекта);
- уникальный идентификатор издателя (обязательно только для версий v2 и v3);
- уникальный идентификатор субъекта (обязательно только для версий v2 и v3);
- дополнения (для версий v2 и v3);
- алгоритм подписи сертификата (обязательно только для версии v3);
- подпись сертификата (обязательно для всех версий).

Структура сертификата X.509

```
Version: 3 (0x2)
 Serial Number:
     5c:0c:6b:05:c5:e3:b7:b4:0a:e0:18:6b:51:82:32:33
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
 Validity
     Not Before: Mar 13 08:18:01 2023 GMT
     Not After : Jun  5 08:18:00 2023 GMT
 Subject: CN = *.google.com
 Subject Public Key Info:
     Public Key Algorithm: id-ecPublicKey
         Public-Key: (256 bit)
         pub:
             04:a2:39:de:c3:aa:f3:bd:08:b5:cf:6e:0d:d1:da:
             18:f3:e5:d3:ab:55:7e:fd:af:76:c2:8c:4a:a4:47:
             9b:9c:d7:bb:ae:5b:80:a6:25:7f:5d:06:f4:b0:9a:
             d9:99:fc:37:6f:e6:bd:b0:79:a2:00:27:f7:08:86:
             00:25:a9:cf:e3
         ASN1 OID: prime256v1
         NIST CURVE: P-256
```