TLS (Transport Layer Security)

Client A | **Server B**

handshake, session parameter → RN_C

← handshake, session parameter RN_S

← B's certificate [request A's certificate] + Public Key

1. Phase (Initializatio

Authenticate server (by checking certificate)

2. Phase (Server Identi

generate pre master key & encrypt with public key of B

encrypted pre-master key (RSA) →

3. Phase (Client Identity + Session key generation)

signed piece of session & handshake data (known to B) & A's certificate + Public Key →

Authenticate client

decrypt pre-master key

generate session key from pre-master key K

generate session key from pre-master key K

← data is encrypted & decrypted by same symm. key K →
(e.g. AES)

4. Phase (encrypted comm.)

O: - May intercept traffics
- Impersonate B by sending the certificate
- cannot decrypt the pre-master key
- cannot establish the communication

12.5 Threshold Cryptography

Consider the problem:

11 Scientists want to lock up some documents in a cabinet. It should be opened, if and only if at least 6 scientists come together. What is the smallest number of locks needed? What is the smallest number of keys each scientist must carry?

The answer ~~is~~ is: 462 locks, 252 keys per scientist.

Def 12.1 Let D be some secret. If D is divided into n parts $D_1, \dots, D_n$ such that

- knowledge of any k or more D_i pieces make D easily computable
- knowledge of $k-1$ or fewer pieces yields no information on D

How to construct such a scheme?

Given integers k, n and D

Find a prime p $\quad p > D$, $p > n$ and p big enough (against brute force)

$$g(X) = \sum_{i=0}^{k-1} a_i X^i \in \mathbb{F}_p[X]$$

with $a_0 = D$ and $a_1, \dots, a_{k-1}$ shall be random integers

We have $D = g(0)$ and we define $D_i = g(i)$, $i = 1, \dots, n$

Then again if an attacker knows $k-1$ pieces D_i, there exists exactly one $k-1$ degree polynomial g' such that $g'(0) = D'$ and $g'(i) = D_i$ for each D'. Hence knowledge of $k-1$ pieces yield no information. But having k pieces reveals D.

13. Elliptic Curve Cryptography (ECC)

Generalisation of Diffie-Hellman key exchange to a general additive cyclic group G with generator P,
$|G| = n$, neutral element O,

$$G = \{O, P, 2P, 3P, \ldots, (n-1)P\}$$

Protocol actions

A chooses a random $a \in \{2, \ldots, n-1\}$ $A \to B : aP$ (g^a)
B chooses a random $b \in \{2, \ldots, n-1\}$ $B \to A : bP$ (g^b)

A and B compute the joint key $K = abP$ (g^{ab})

Required properties of G

- DLP / DHP must be hard
- group operations shall be efficiently computable

Protocols relying on DLP or DHP, which can be carried over to general cyclic groups

- Diffie Hellman key exchange
- El Gamal PK encryption
- El Gamal signature, DSA

In 1985, Miller and Koblitz suggested independently the group of points on elliptic curves over finite fields.

Advantage: less memory, computing power. Particularly suited for smart cards.

13.1 Foundations and Definitions

Let K be a field (e.g., $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_{p^k}$)

If $K = \mathbb{F}_{p^k}$, then $p > 3$ in the following.

Def 13.1 An elliptic curve E/K over the field K is described by an equation:

$$E: y^2 = x^3 + ax + b \quad a, b \in K$$

or $f(x,y) = y^2 - x^3 - ax - b = 0$

provided the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$

For an algebraic extension field $L \supseteq K$ we call

$$E(L) = \{ (x,y) \in L \times L \mid f(x,y) = 0 \} \cup \{ O \}$$

the set of L-rational points on E. O denotes the point at infinity.

Remarks: a) E/K means $a, b \in K$

b) Since $L \supseteq K$, also $a, b \in L$. Hence, E/K is also E/L

c) For $p = 2, 3$ the curve equation is more complicated

d) Condition $\Delta \neq 0$ avoids singularities

Examples a) $E_1: y^2 = x^3 - x$ over $\mathbb{R}$, $a = -1, b = 0$

$\Delta = -16(-4) = 64 \neq 0$

Hence E_1 describes an elliptic curves

b) $E_2: y^2 = x^3 + 2x + 2$ over $\mathbb{F}_5$, hence $a = 2, b = 2$

$\Delta = -16(4 \cdot 2^3 + 27 \cdot 2^2) = -16(2 + (-2)) = 0$

Hence, E_2 is not an elliptic curves