TLS (Transport Layer Security)

Client A | **Server B** | mutual authentication parts

handshake, session parameters → RN_c

← handshake, session parameters RN_s

← B's certificate + public key, request A's certificate

} 1. Phase (Initialization)

$\boxed{\text{Authentication of server}}$ (by checking certificate) } 2. Phase (Server Identif.)

$\boxed{\text{generates pre-master key \& encrypts it with public key of B}}$

encrypted pre-master key (RSA) →

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

$\boxed{\text{Authentication of client}}$

$\boxed{\text{decrypt pre-master key}}$

$\boxed{\text{generate session key } K_S \text{ from pre-master key } K}$ $\boxed{\text{generate session key } K_S \text{ from pre-master key } K}$

} 3. Phase (Client identif. + Session key generation)

← data is encrypted & decrypted by same symm. key K_S (e.g. AES) → } 4. Phase (encrypted comm.)

O: - May intercept traffic
- Impersonate B by sending the certificate
- O cannot decrypt the pre-master key
- O 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 " " of keys each scientist must carry?
The answer 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, D.
Find a prime p: $p > D$, $p > n$ (obviously $n \geq k$) and p big enough against brute force. Define

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

$a_0 = D$ and $a_1, \dots, a_{k-1}$ shall be random integers in $\mathbb{Z}_p$.
We have $D = g(0)$ and we issue (i, D_i) with $D_i = g(i)$, $i = 1, \dots, n$.
Then again if an attacker knows $k-1$ pieces (i, 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 yields no information. But having k pieces reveals D.

13. Elliptic Curve Cryptography (ECC)

Generalization of Diffie-Hellmann key exchange to a general additive cyclic group G with generator P,
$|G| = n$, neutral element $\mathcal{O}$

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

Protocol actions:

A chooses a random number $a \in \{2, \dots, n-1\}$ $A \to B : aP$ (g^a)
B chooses a random number $b \in \{2, \dots, n-1\}$ $B \to A : b\cdot P$ (g^b)
A and B compute the joint key $K = a\cdot b\cdot P$ (g^{ab})

Required properties of G

- DLP / DHP must be hard to solve
- group operation needs to be efficiently computable

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

- Diffie-Hellman key exchange protocol
- 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.

→ See slides on ECC.