TLS (Transport Layer Security)

Client A

1. Phase (Initialization)
   - Request RNc
   - Handshake, session parameters
   - B's certificate and public key

2. Phase (Server Identification)
   - Authentication of server (by checking certificate)
   - Server generates pre-master key
   - Encrypted pre-master key (RSA)
   - Signed piece of session & handshake data (known to B)
   - & A's certificate and public key

3. Phase (Client Identification & Session Key Generation)
   - Decrypt pre-master key
   - Generate session key ks from pre-master key

4. Phase (Encrypted Communication)
   - Data is encrypted & decrypted by same symmetric key, ks
     (e.g. AES)

0: - May intercept traffic
    - 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 number 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

\[ D_1, \ldots, D_n \]

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 \( k, n \) with \( k \leq n \).

Find a prime \( p : p > D, \ p \equiv n \mod k \) (obviously \( n \geq k \)) and \( p \) big enough against brute force. Define

\[ g(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}_p[x] \] with \( a_0 = 0 \) and \( a_1, \ldots, a_{k-1} \) shall be random integers in \( \mathbb{F}_p \).

We have \( D = g(0) \) and we since \( (i, D_i) \) with \( D_i = g(i), \ i = 1, \ldots, k \) Then again if an attacker knows \( k-1 \) pieces \((i, D_i)\), there exists exactly one \( k-1 \)-degree polynomial \( g' \) such that \( g'(0) = p \) and \( g'(i) = D_i \) for each \( D_i \). Hence, knowledge of \( k-1 \) pieces yields no information. But having \( k \) pieces reveals \( D \).
Elliptic Curve Cryptography (ECC)

Generalization of Diffie-Hellman key exchange to a general additive cyclic group \( G \) with generator \( P \):

\[ |G| = n \text{ neutral element } \mathcal{O} \]

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

Protocol actions:

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

\( A \) and \( B \) compute the joint key:

\[ K = a \cdot b \cdot P \] \( (g^{ab}) \)

Required properties of \( G \):

- DLP IDHP must be hard to solve
- Group operation needs to be efficiently computable

Protocols relying on DLP or IDHP, 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 Kothe suggested independently the group of points on elliptic curves over finite fields.

Advantages:
- Less memory, computing power,
- Particularly suited for smart cards.

See slides on ECC.