TLS (Transport Layer Security)

Client A

1. Handshake, version parameter
2. Handshake, version parameter
3. B's certificate [request A's certificate] + Public key
4. Authenticate server (by checking certificate)

Server B

1. Phase (Certificate)
2. Phase (Server Hello)
3. Phase (Client Hello + Server Hello + generation)
4. Phase (Encrypted Client Hello)

Data is encrypted & decrypted by some symm. key $K$ (e.g. AES)

O: 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:

17 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: 462 locks, 252 keys per scientist.

Def 12.1 Let D be some secret. If D is divided into n parts
\( D_1, \ldots, D_n \) and 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?

Calculate integers \( b, m \) and \( D \)

Find a prime \( p \) \( p > D \), \( p > m \) and \( p \) big enough (say 1024 bits)

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

with \( a_0 = D \) and \( a_1, \ldots, a_{b-1} \) shall be random integers

We have \( 0 = g(0) \) and we define \( D_i = g(i) \), \( i = 0, \ldots, m \)

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 
\[ g'(i) = D_i \text{ for each } D_i \]. Hence knowledge of \( k-1 \) pieces yield no information. But knowing \( k \) pieces reveals \( D \).
Elliptic Curve Cryptography (ECC)

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

$G = \{ 0, P, 2P, 3P, \ldots, (n-1)P \}$

Protocol actions:

A chooses a random $a \in \{2, \ldots, n-1\}$, $A \rightarrow B : aP \ (g_a)$  
B chooses a random $b \in \{2, \ldots, n-1\}$, $B \rightarrow A : bP \ (g_b)$  

$A$ and $B$ compute the point key

$k = abP \ (g_{ab})$

Required properties of $G$:

- DLG/IDHP must be hard
- Group operations shall be efficiently computable

Protocol, relying on DLG or IDHP, 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 useful 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 $p \geq 3$ 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 $f(t, t) = t^2 - t^3 - at - b = 0$

provided the discriminant $\Delta = -16(4a^3 + 2b^2) \neq 0$.
For an algebraic extension field $L \supseteq K$ we call

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

the set of $L$-rational points on $E$. 0 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, $E/L$ is also $E/L$.

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

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

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

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

Hence $E_1$ describes an elliptic curve.

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

$\Delta = -16(4.2^3 + 2.2^2) = 16(2 + (-2)) = 0$,

Hence $E_2$ is not an elliptic curve.