T-79.5501 Cryptology

http://www.tcs.hut.fi/Studies/T-79.5501/

Spring 2007

Lecture 1

Stinson 2.1-2.3.

Computational security

Example (fixed size):

It is currently believed that recovering the secret 128-bit key of the AES requires at least 2^{100} operations.

Example (variable size):

The discrete logarithm problem in a group of size t is said to be hard if solving it requires N(t) operations, where $N(t) \cong t$.

Provable security

Example: It is an open question if the security of the Diffie-Hellman key exchange can be reduced to the (conjectured) hardness of the Discrete Logarithm Problem. If such a reduction existed, then Diffie-Hellman key exchange would be provably secure.

On the other hand, the Diffie-Hellman problem itself has been around for about thirty years, and has achieved a position of a *well-studied problem that is thought to be difficult*.

Unconditional security

No upperbound to the computational effort (time, memory) of breaking the cryptosystem.

Cryptosystem is unconditionally secure if the probability of breaking it is small (negligible).

Example. Given a plaintext-ciphertext pair, AES maybe computationally secure. It is not unconditionally secure as the probability of success is equal to 1 given unlimited computational power.