Symmetric and asymmetric cryptography overview

- Modern cryptographic methods use a key to control encryption and decryption
- Two classes of key-based encryption algorithms
  - symmetric (secret-key)
  - asymmetric (public-key)
- Symmetric: same key used for encryption and decryption
- Asymmetric: for encryption a different key is used for encryption and decryption.
  - decryption key cannot be derived from encryption key

Symmetric ciphers

- Main problem: key distribution
- Symmetric ciphers can be devided into **stream ciphers** and **block ciphers**
- Stream ciphers
  - can encrypt a single bit of plaintext at a time
- Block ciphers
  - take a number of bits and encrypt them as a single unit

Asymmetric ciphers

- Said to be the most significant new development in cryptography in the last 300-400 years
  - first described publicly by Hellman and Diffie in 1976
- The encryption key is public, decryption key secret
  - anyone can encrypt a message but only the one who knows the corresponding private key can decrypt it
- In practise asymmetric and symmetric algorithms are often used together, called **hybrid encryption**

Algorithm requirements

- The algorithm itself should be known, only the key is secret
- Key should be random
- With a good algorithm it's impossible to find the key even if the plaintext and ciphertext are known
  - impossible = takes far to long to go through the keyspace

Confusion and diffusion

- Shannon: strong ciphers could be built by combining substitution with transposition repeatedly
- He described the properties of a cipher as being **confusion** and **diffusion**
  - diffusion means spreading the plaintext information through the ciphertext
- Easiest block ciphers were simple networks that combined substitution and permutation cicuits, so called SP-networks

DES – Digital Encryption Standard

- Widely used symmetric algorithm
- Encrypts a 64-bit block using a 56-bit key
- DES uses diffusion and confusion in many stages. The algorithm is quite complicated.
- Challange first broken in 1997, took 14000 PCs four months, in 1998 in under a day
- Use the algorithm multiple times with different keys: 3DES [triple-DES]

AES (Advanced Encryption Standard)

- Search for a replacement to DES started in January 1997
- Based on winning algorithm **Rijndael**, AES was officially adopted in December 2001
- AES contains a subset of Rijndael's capabilities (e.g., AES only supports a 128-bit block size)

AES (Rijndael) overview

- Designed by Belgian cryptographers Rijmen and Daemen
- Can operate over a variable-length block using variable-length keys
- Iterated block cipher
  - meaning that the initial input block and cipher key undergoes multiple rounds of transformation before producing the output

Other common secret key algorithms

- *International Data Encryption Algorithm (IDEA)*
  - DES-like 64-bit block cipher using 128-bit keys
- *RC5*
  - a block-cipher supporting a variety of block sizes, key sizes, and number of encryption passes over the data
- *Blowfish*
  - symmetric 64-bit block cipher. Key lengths can vary from 32 to 448 bits in length
- *Twofish*
  - 128-bit block cipher using 128-, 192-, or 256-bit keys

Asymmetric algorithm techniques

- One-way functions
  - mathematical functions that are easy to calculate whereas their inverse function is relatively difficult to calculate
- **factorization** or **descrete logarithms**
  - 9 x 16 = 144 vs 144 = 9 x 16
  - $3^6 = 729$ vs finding x and y so that $\log_x y = 729$

RSA (Rivest, Shamir, Adleman)

- One of the more commonly used public key algorithms
- The RSA algorithm is user to do public key encryption and digital signatures based on factoring. The formula is simple, but takes a long time to calculate.
- RSA is used in most web-browsers as part of SSL.

Strength of asymmetric cryptographic primitives.

- Asymmetic crypthographic primitives are believed to require at least twice the block length of a symmetric algorithm with corresponding key length
- Future quantum computers -> factoring and descrete logarithm computations easy -> asymmetric cryptography would have to be abandoned