-p gp.tree.print-style=latex

Symmetric vs Asymmetric Cryptosystems (cont’d)

# Advantages of asymmetric cryptosystems:

Easier to manage:

Only 1 key of the key-pair must be kept secret.

Better scalability:

For communication among n participants only their n public keys are needed.

Flexibility:

Encryption technology can be naturally used for electronic signatures.

Stability:

Keys can remain unchanged over a long period of time

Disadvantages of asymmetric cryptosystems:

Performance:

Public-key algorithms are significantly slower

Key sizes:

Keys are typically much longer

Foundations:

No public-key scheme has been proven to be secure

Pragmatics:

Shorter history.

Symmetric vs Asymmetric Cryptosystems

# Advantages of symmetric cryptosystems:

Performance:

Symmetric crypto-algorithms are typically much faster than asymmetric ones, and achieve higher throughput.

Compositionality:

Ciphers can be combined to achieve stronger encryption.

Key sizes:

Due to sophisticated ciphers, keys can be shorter

Pragmatics:

Long history

# Disadvantages of symmetric cryptosystems:

Management:

Communication key must remain secret

Scalability:

For secure communication a separate key is needed for every pair of communication

Stability:

Keys should be changed frequently

# Steam cipher

WEP (wifi)

# Block cipher

Use substitution to add confusion

Use transpositions to add diffusion

Apply rounds consisting of substitution and transposition steps to improve both