Security

Security Requirements

- Confidentiality
  - Protection from disclosure to unauthorised persons
- Integrity
  - Maintaining data consistency
- Authentication
  - Assurance of identity of person or originator of data
- Non-repudiation
  - Originator of communications can’t deny it later
- Availability
  - Legitimate users have access when they need it
- Access control
  - Unauthorised users are kept out

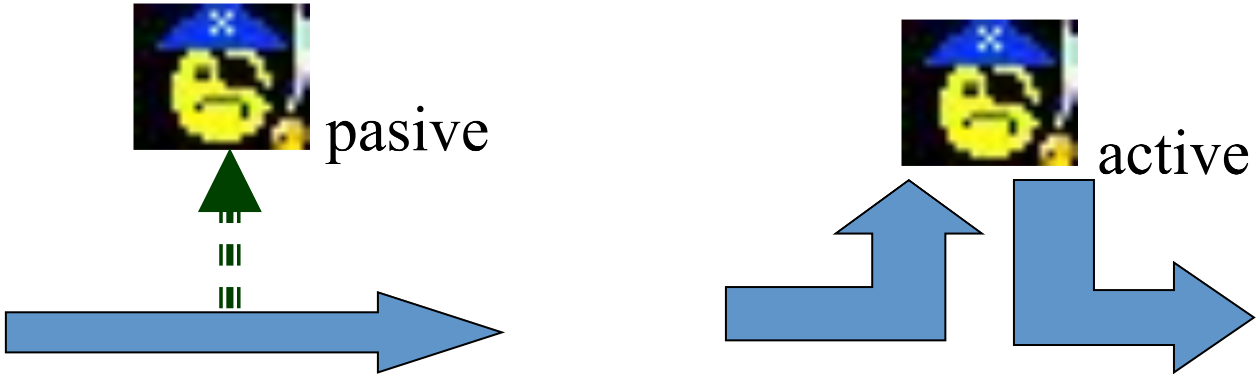
Security Requirements

- These are often combined
  - User authentication used for access control purposes
  - Non-repudiation combined with authentication

Security Threats

- Information disclosure/information leakage
- Integrity violation
- Masquerading
- Denial of service
- Illegitimate use
- Generic threat: Backdoors, trojan horses, insider attacks
- Most Internet security problems are access control or authentication ones
  - Denial of service is also popular, but mostly an annoyance

Attack Types



- Passive attack can only observe communications or data
- Active attack can actively modify communications or data
  - Often difficult to perform, but very powerful
    - Mail forgery/modification
    - TCP/IP spoofing/session hijacking

Security Services

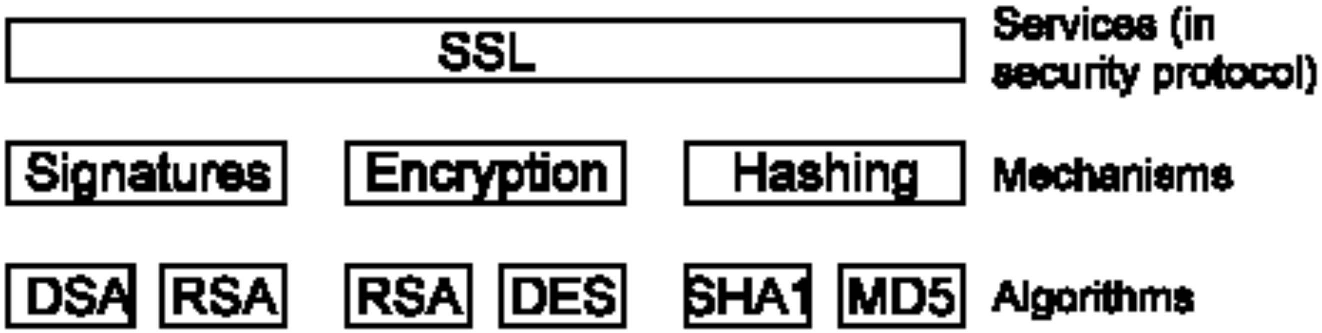
- From the OSI definition:
  - Access control: Protects against unauthorised use
  - Authentication: Provides assurance of someone's identity
  - Confidentiality: Protects against disclosure to unauthorised identities
  - Integrity: Protects from unauthorised data alteration
  - Non-repudiation: Protects against originator of communications later denying it

Security Mechanisms

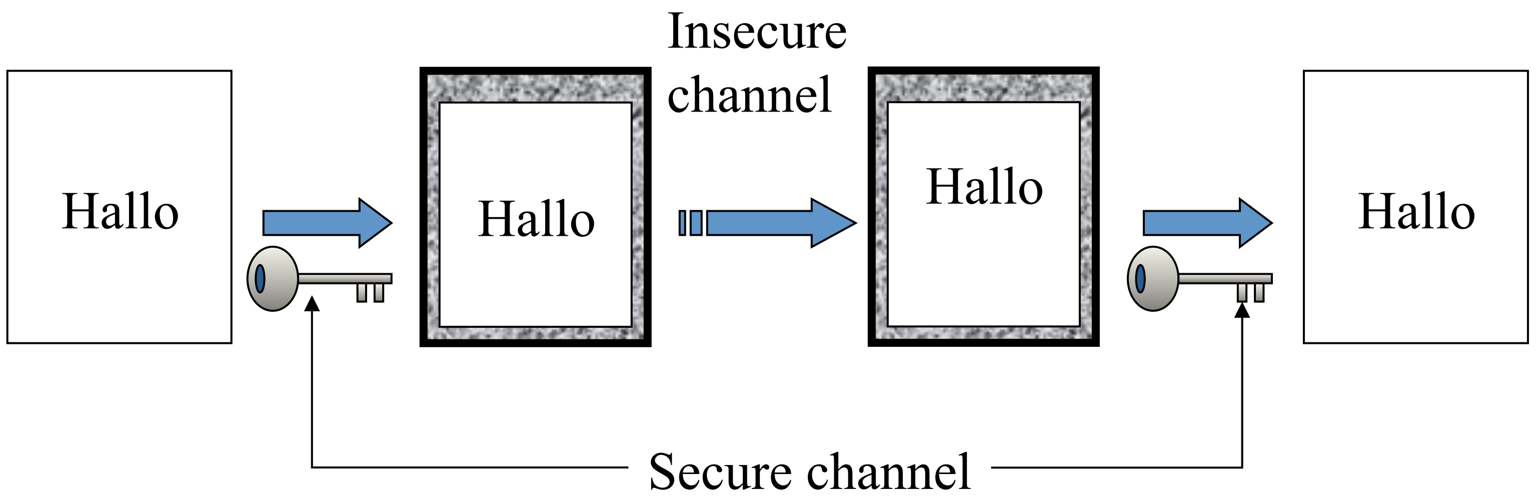
- Three basic building blocks are used:
  - Encryption is used to provide confidentiality, can provide authentication and integrity protection
  - Digital signatures are used to provide authentication, integrity protection, and non-repudiation
  - Checksums/hash algorithms are used to provide integrity protection, can provide authentication
- One or more security mechanisms are combined to provide a security service

Services, Mechanisms, Algorithms

- A typical security protocol provides one or more services
  - Services are built from mechanisms
  - Mechanisms are implemented using algorithms

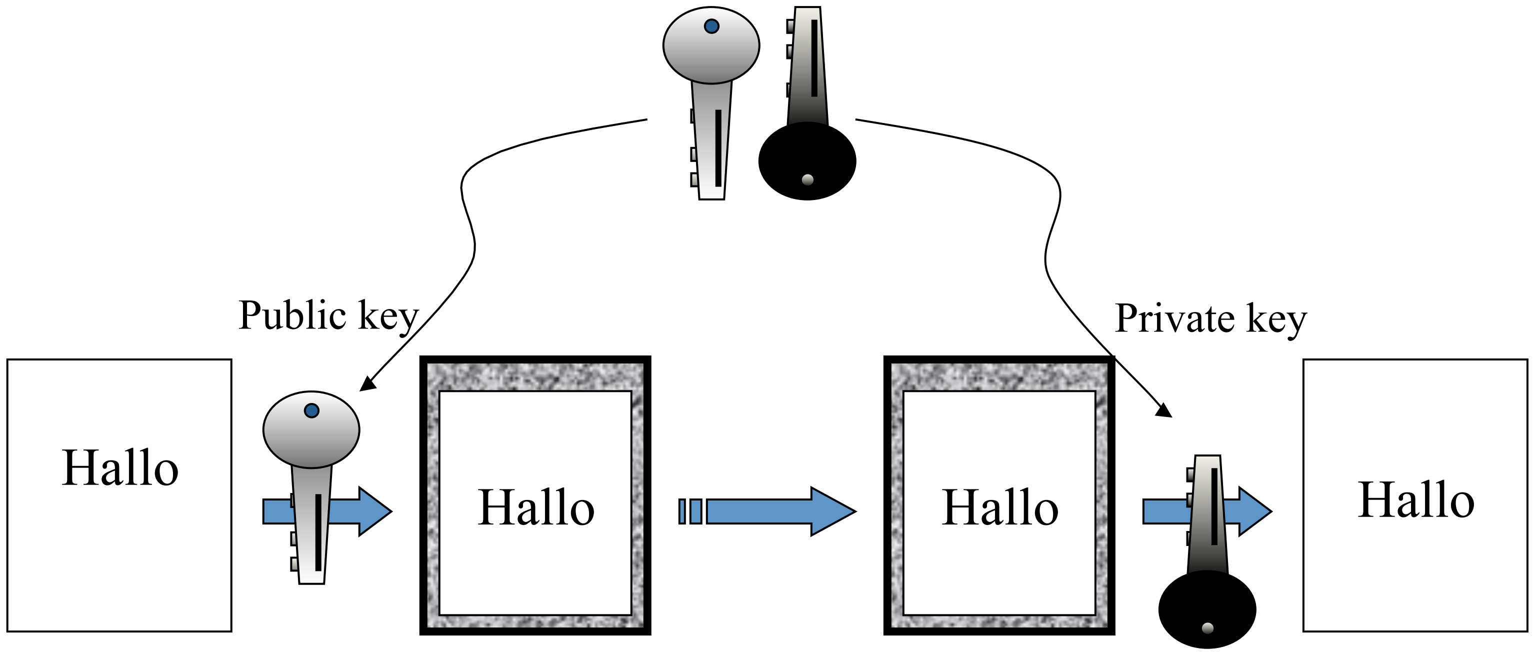


Conventional Encryption



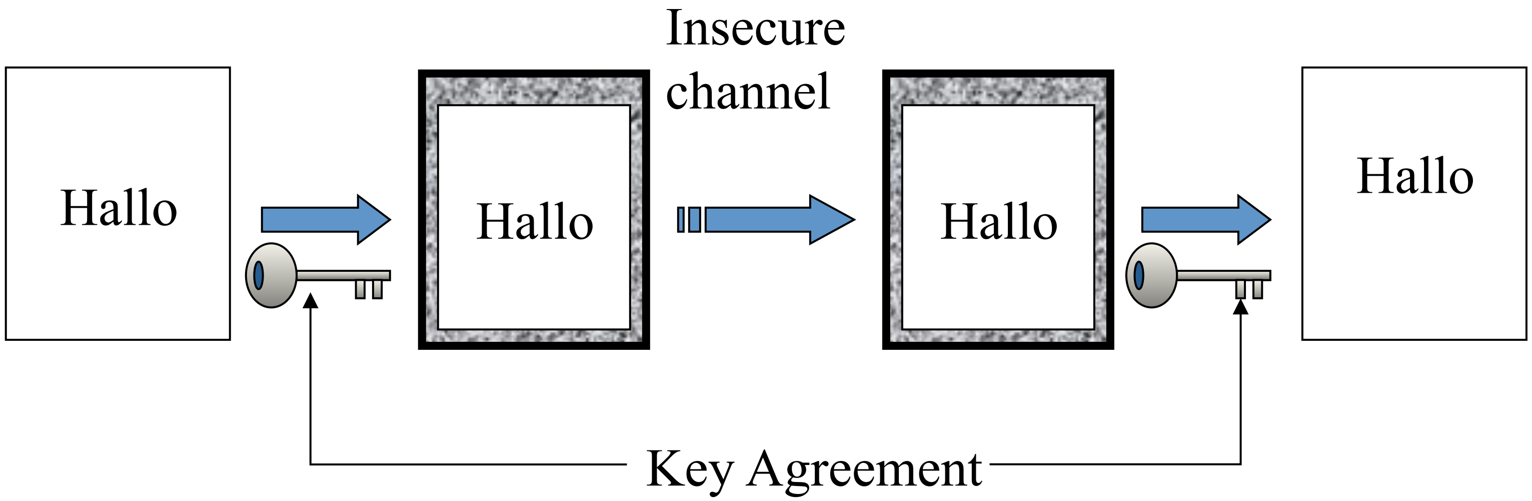
- Uses a shared key
- Problem of communicating a large message in secret reduced to communicating a small key in secret

Public-key Encryption



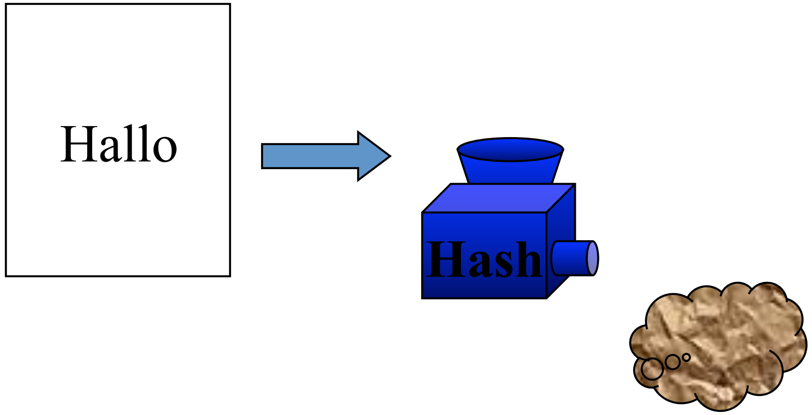
- Uses matched public/private key pairs
- Anyone can encrypt with the public key, only one person can decrypt with the private key

Key Agreement



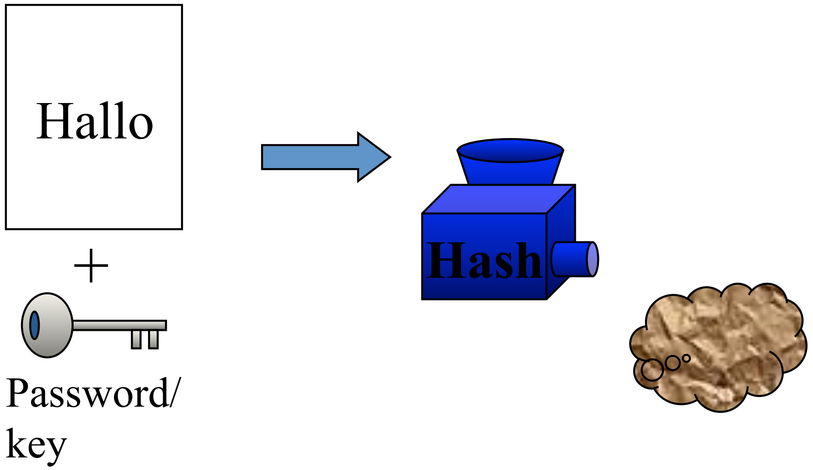
- Allows two parties to agree on a shared key
- Provides part of the required secure channel for exchanging a conventional encryption key

Hash Functions



- Creates a unique “fingerprint” for a message
- Anyone can alter the data and calculate a new hash value
  - Hash has to be protected in some way

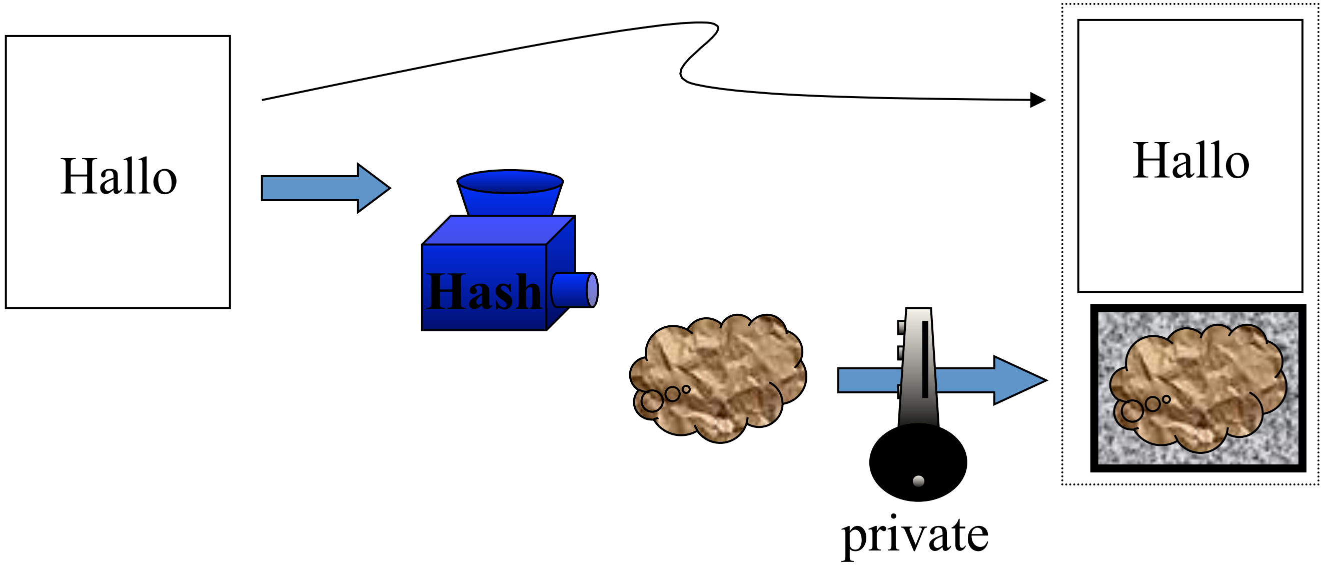
MAC’s



- Message Authentication Code, adds a password/key to a hash
- Only the password holder(s) can generate the MAC

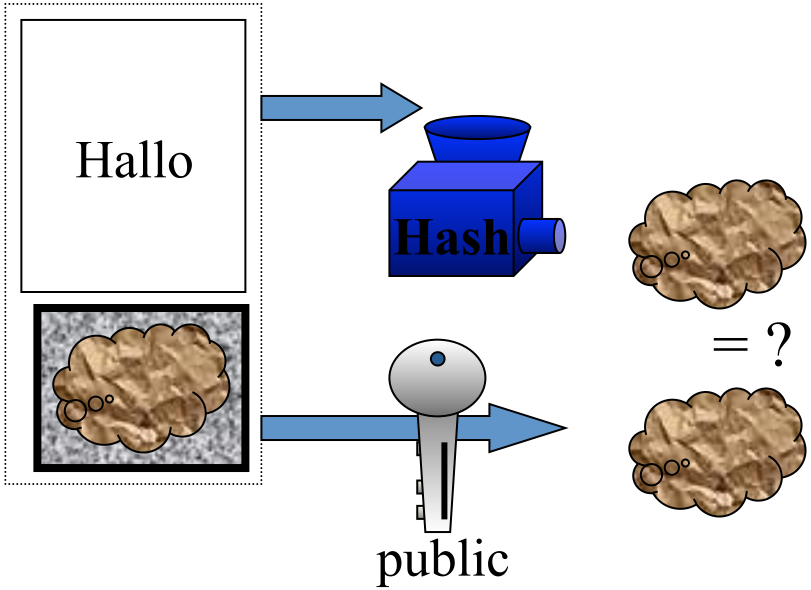
Digital Signatures

- Combines a hash with a digital signature algorithm



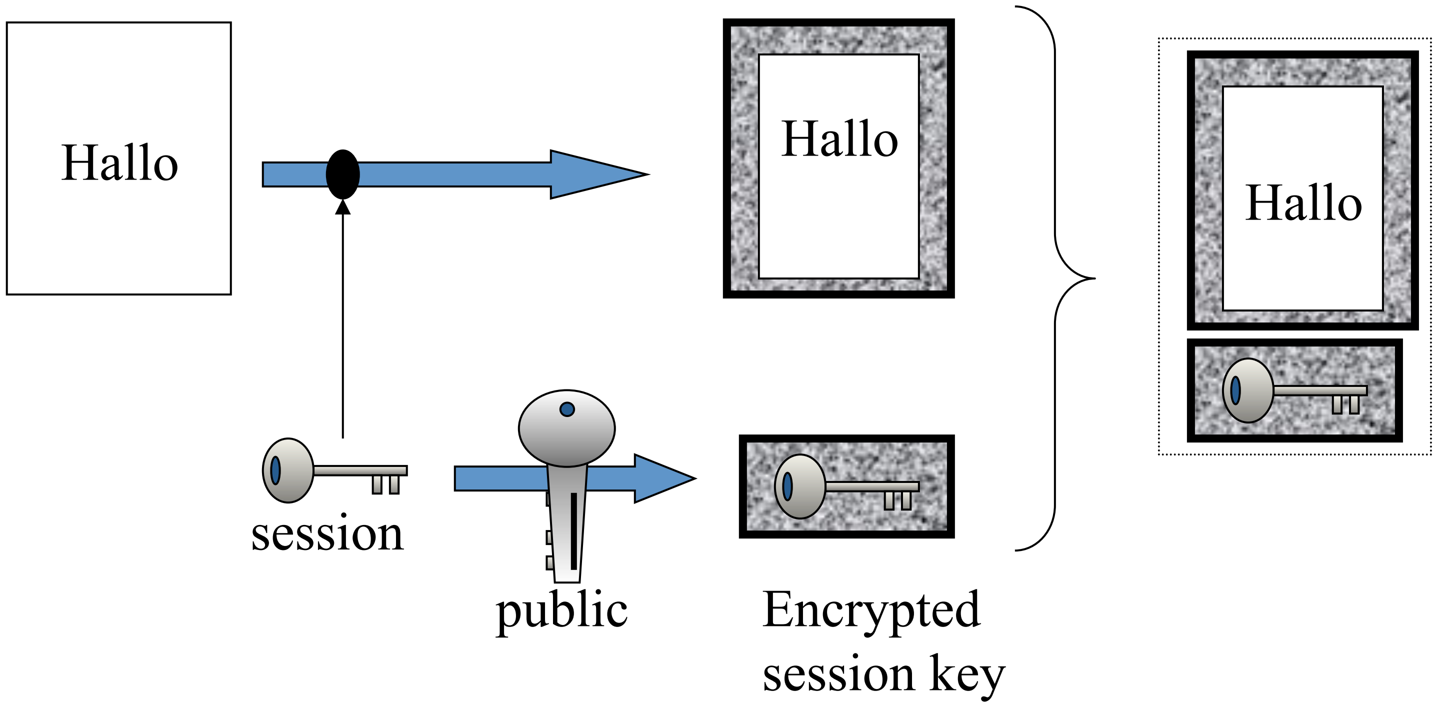
Digital Signatures

- Signature checking:



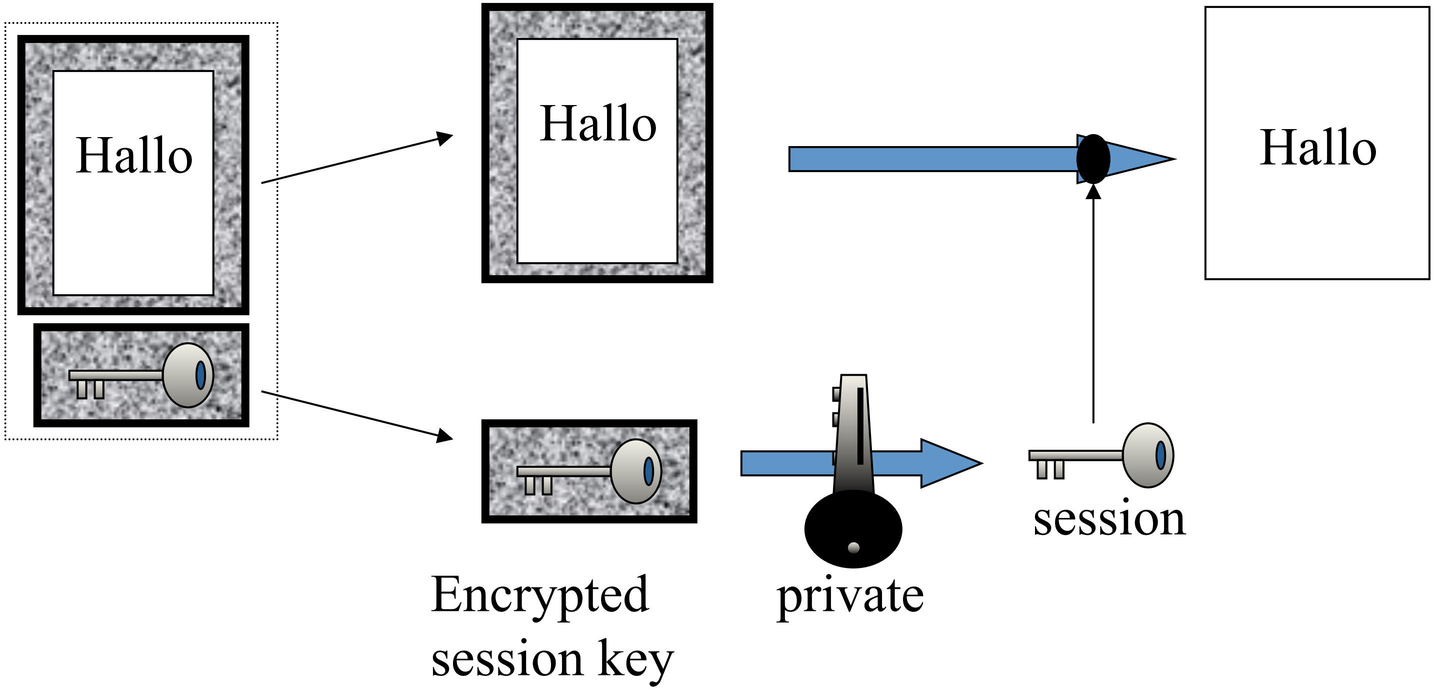
Message Encryption

- Combines conventional and public-key encryption

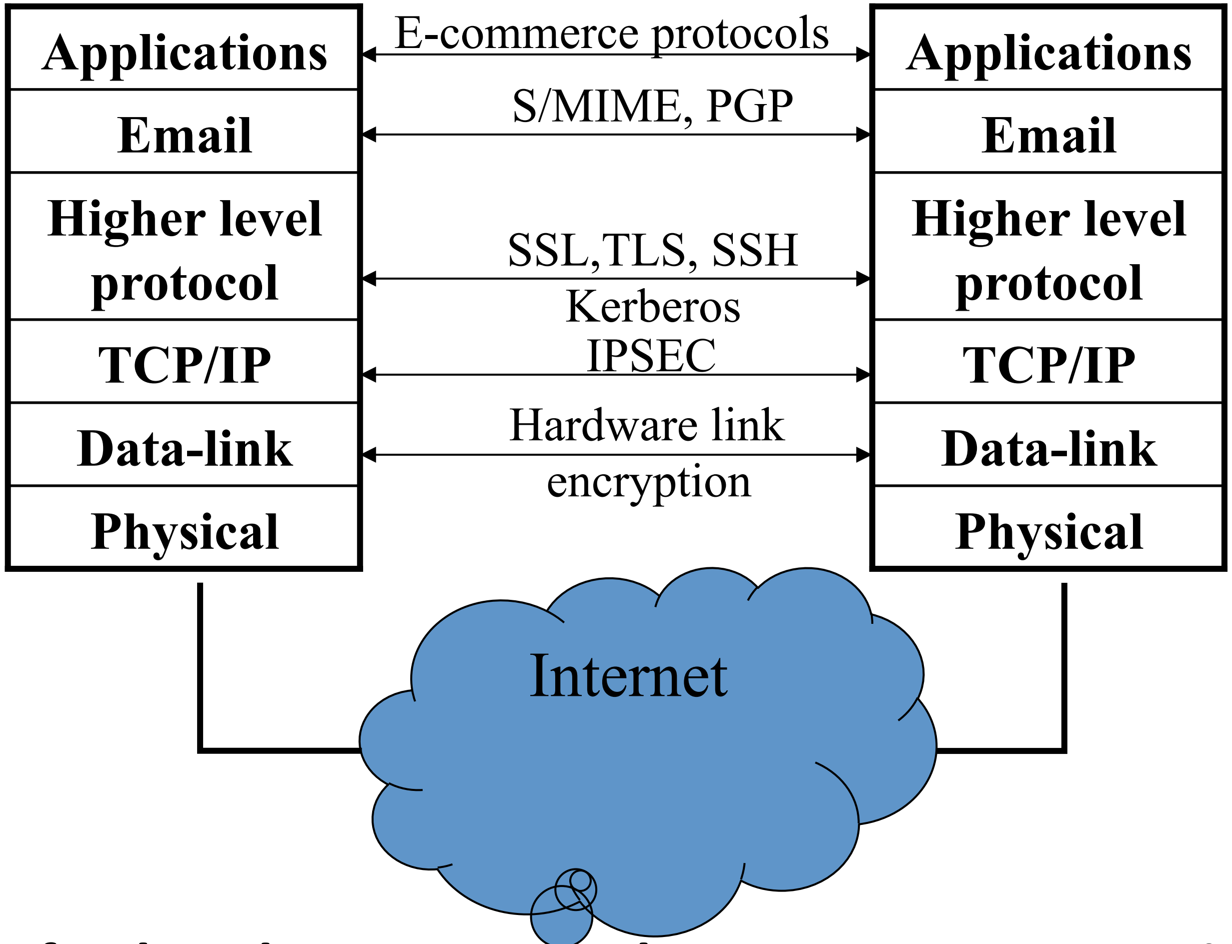


Message Encryption

- Public-key encryption provides a secure channel to exchange conventional encryption keys



Security Protocol Layers



- **The further down you go, the more transparent it is**
- **The further up you go, the easier it is to deploy**