University of York
Europe Campus
CITY College

Public Key Cryptography
Primer

CCS3341 Cloud Computing

Dr S. Veloudis

Cryptography

Symmetric Cryptography

- Uses a single key
- Encrypts clear text (i.e., transforms it into ciphertext) through an algorithm that uses a this key

The same algorithm uses the same key to decrypt

Asymmetric Cryptography

Uses a key pair
Encrypts clear through an algorithm that use the one key

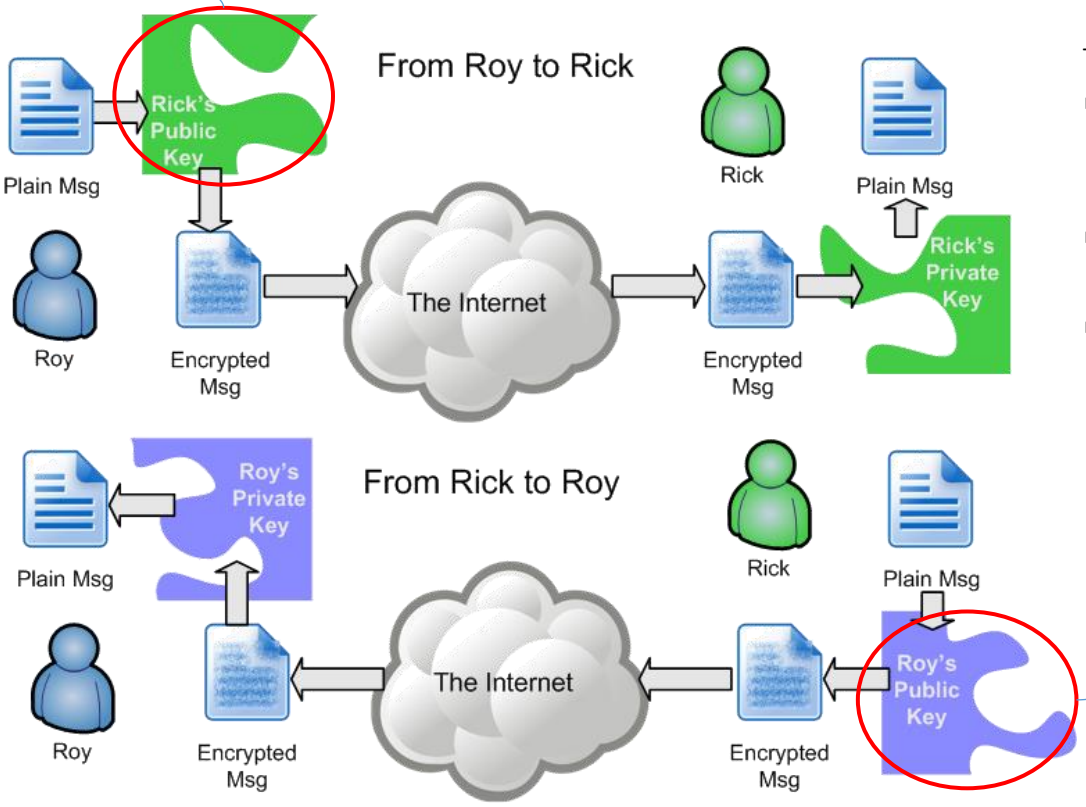
The same algorithm uses the other key to decrypt

- The key pair comprises a public and a private key
- The public key is accessible to anyone
- The private key is kept secret

Public Key Cryptography

The public key may:

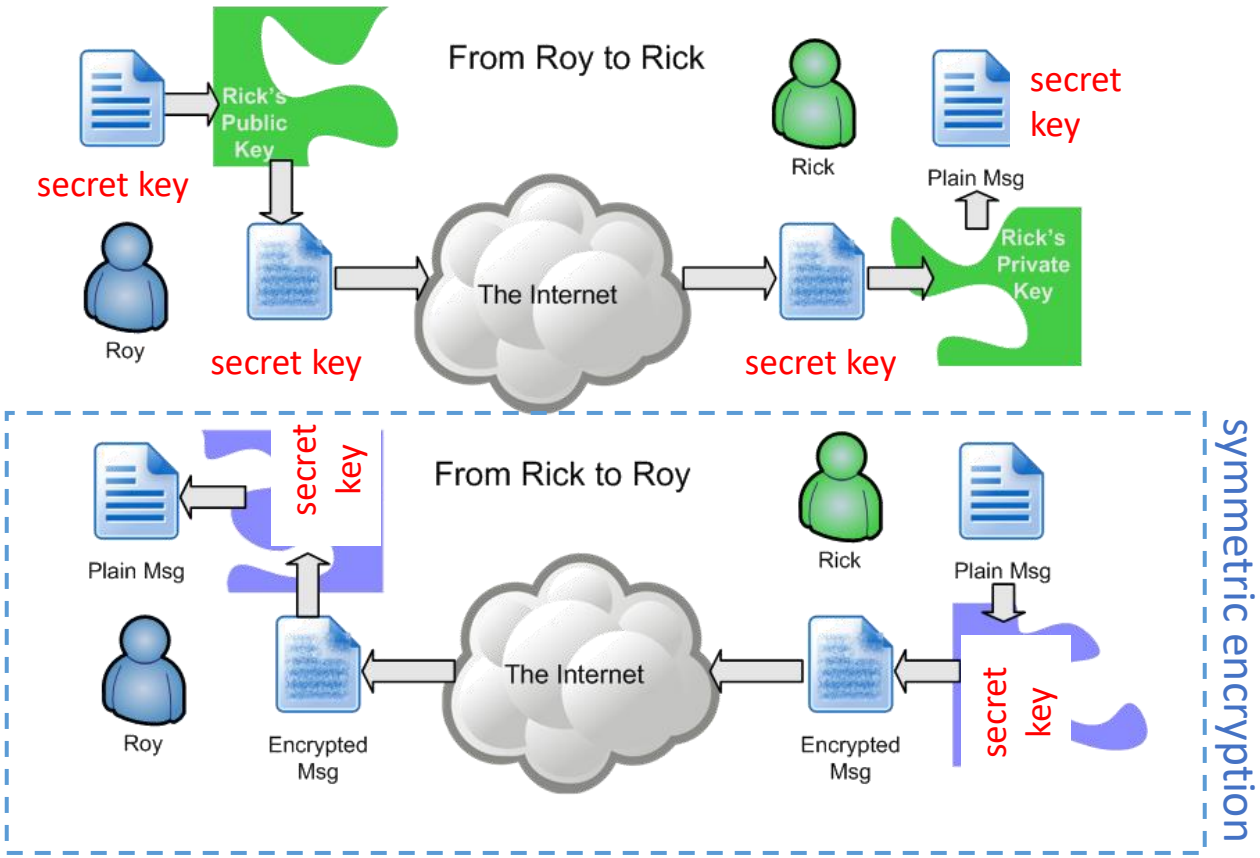
- Be provided directly from Rick to Roy
- Be found on Rick's website
- Be found on a Public Key Server (PKS)



The public key may:

- Be provided directly from Roy to Rick
- Be found on Roy's website
- Be found on a Public Key Server (PKS)

Public Key Cryptography



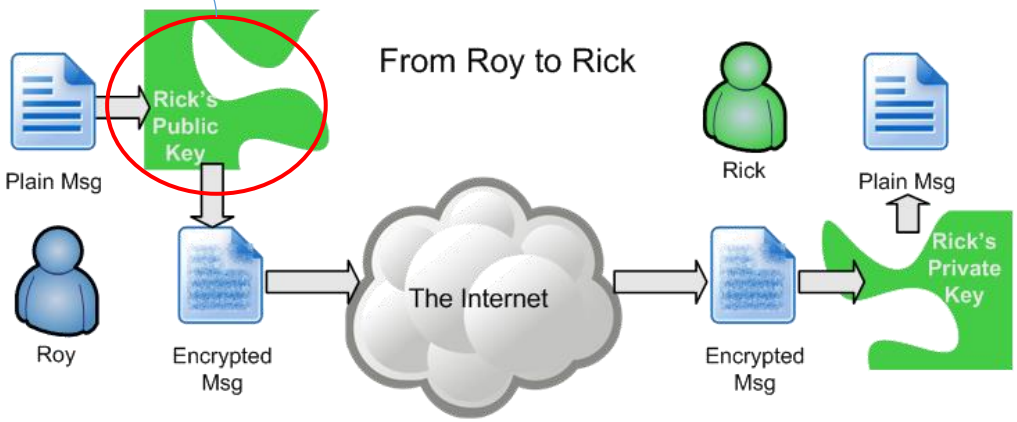
Note: Asymmetric encryption/decryption with public and private keys is inefficient (performance-wise) for an entire conversation, so symmetric encryption/ decryption based on a single shared secret key is used instead. Asymmetric encryption/decryption is only used initially for exchange confidentially the shared secret key.

Public Key Cryptography

The public key may:

- Be provided directly from Rick to Roy
- Be found on Rick's website
- Be found on a Public Key Server (PKS)

But how do we trust that this is really Rick's public key?

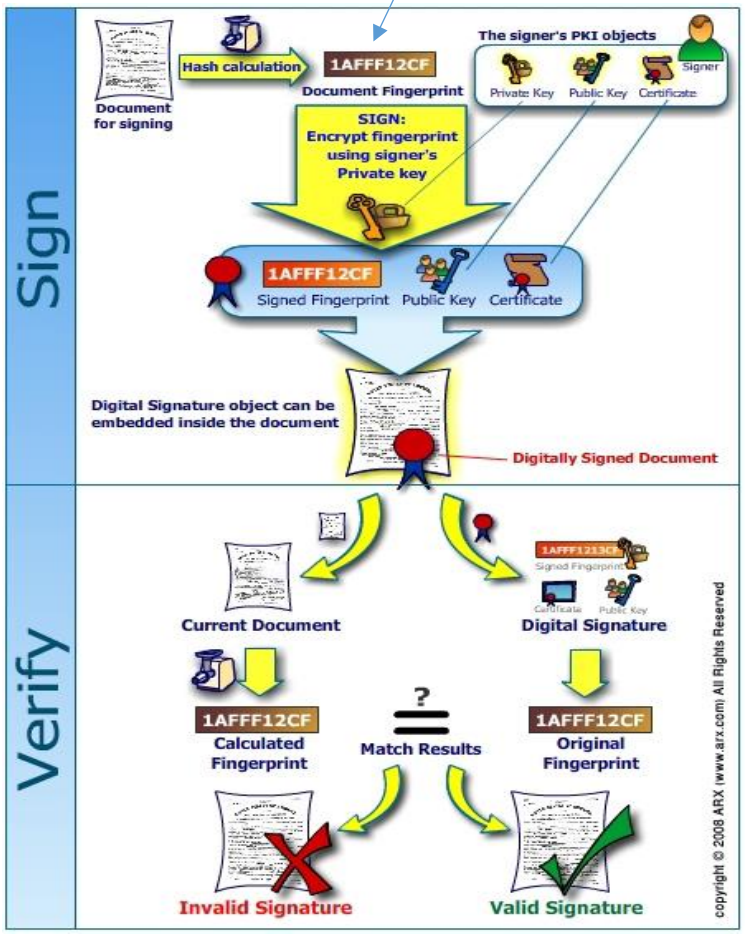


Public keys come in digital certificates

Public Key Cryptography

- Digital certificates and digital signing
  - Aims at:
    - Message integrity
    - Message authentication
  - A digital certificate may be provided by a Certification Authority (CA)
    - X.509 protocol – hierarchical trust
      - The CA needs to be trusted or needs to provide a certificate that is signed by another trusted CA
      - A recursive process which ends at a trusted root CA
  - Another way to obtain a trusted digital certificate is through the so-called web of trust

Hashing produces a message digest (fingerprint) which is unique for each different message (algorithms: SHA-256/384/512, MD5,…)



source: www.arx.com