



Data Communications and Networking

Lecturer: Toby Daniel

Encryption



Encryption

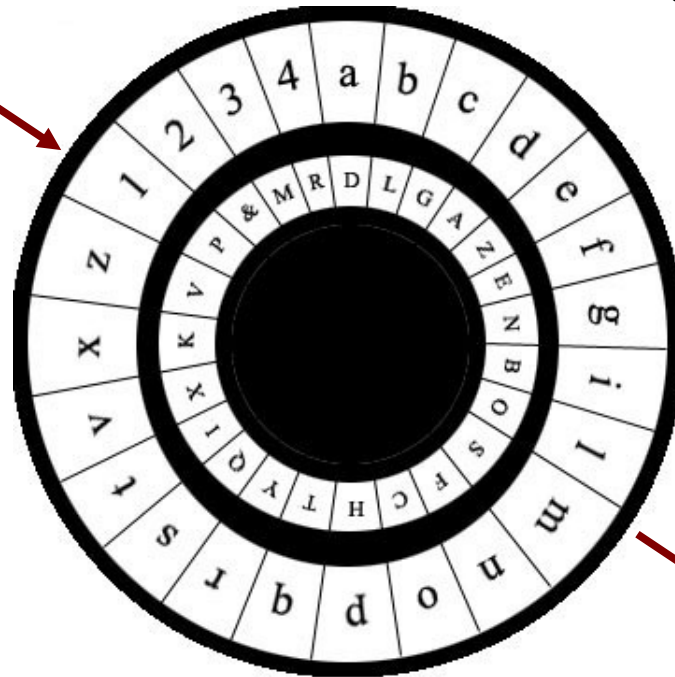
- Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge.
- Original Information = plaintext
- Algorithm = cipher
- Special knowledge = key
- Encrypted Information = ciphertext

Encryption

Cipher

Some very important or secret information that should not fall into the wrong hands.

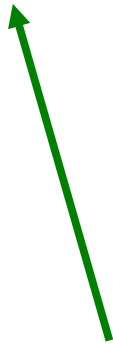
Plaintext



sthe jwkry iednmdklg ns
mvhsk ltyvybidds khise
uicjdk pj k psyy uest agj
dkdud kbnvm.

Ciphertext

Key



Encryption

- What reasons can you think of for using encryption in data communications and networking?



Encryption

- Encryption is used to secure data so that it can not be read by unauthorised people.
- There are two main locations where encryption is used:
 - Data storage
 - Data communication



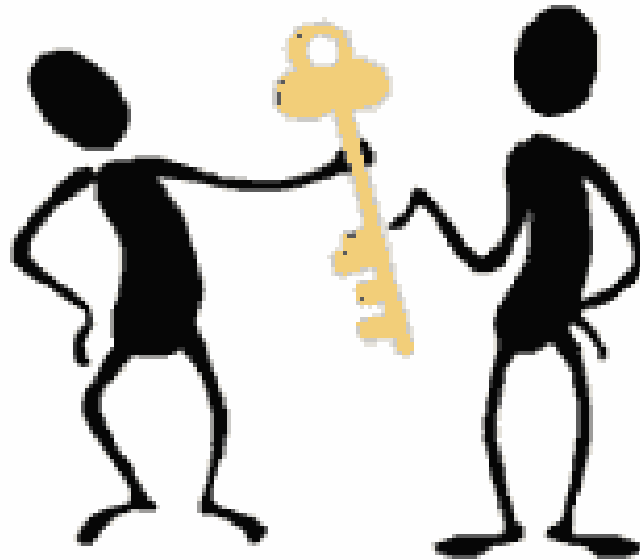
Computerised Encryption

- Most computer encryption systems belong in one of two categories:
- Symmetric-key encryption
- Public-key encryption

Symmetric-key Encryption

- In symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer.
- Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one.

Step 2: Give key and ciphertext to receiver.
(Separately!)



Step 3: Use key to decrypt ciphertext.

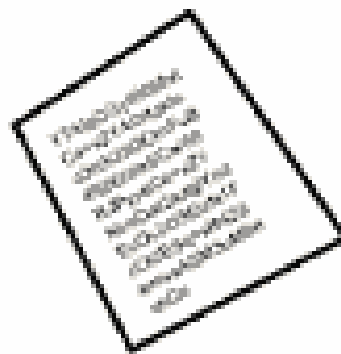
Step 1: Select key and encrypt.



plaintext



encryption



ciphertext



decryption



plaintext

Symmetric-key Encryption

- Which of the following would work best using symmetric-key encryption?
 - a. Data storage
 - b. Data communication
- What problems can you think of using symmetric-key encryption?

Key Management

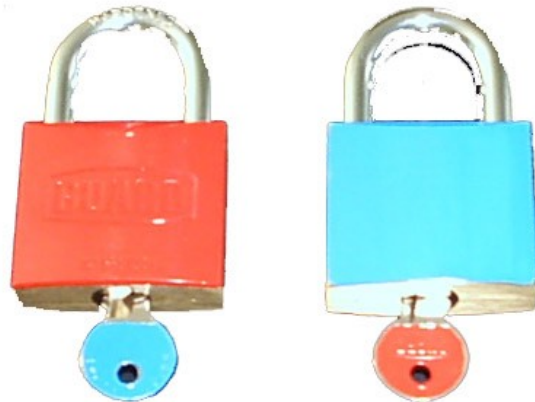
- To allow successful use of symmetric-key encryption for **data communications** you need to implement Key Management.
- Essentially both sending and receiving computers require a copy of the same key – this is a **shared secret key**.
- How do you distribute the keys?
- How do you keep the keys secure?
- How often do you need to change the keys?

Symmetric-key Algorithms

- Symmetric-key algorithms can be divided into **stream ciphers** and **block ciphers**.
- Stream ciphers encrypt the bits of the message one at a time.
- Block ciphers take a number of bits and encrypt them as a single unit.

Public-key Cryptography

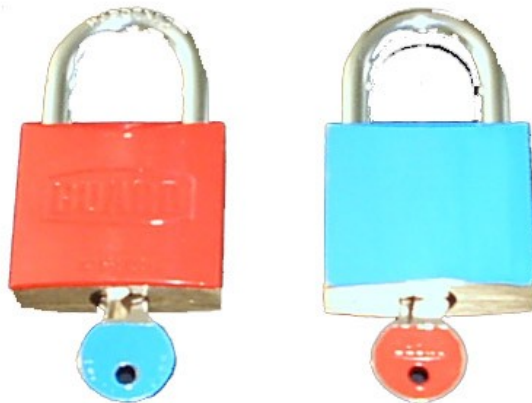
- Public-key cryptography is also known as asymmetric cryptography
- It is a form of cryptography in which each user has a **pair** of cryptographic keys—a public key and a private key.



- Data is encrypted and decrypted using a combination of two keys.

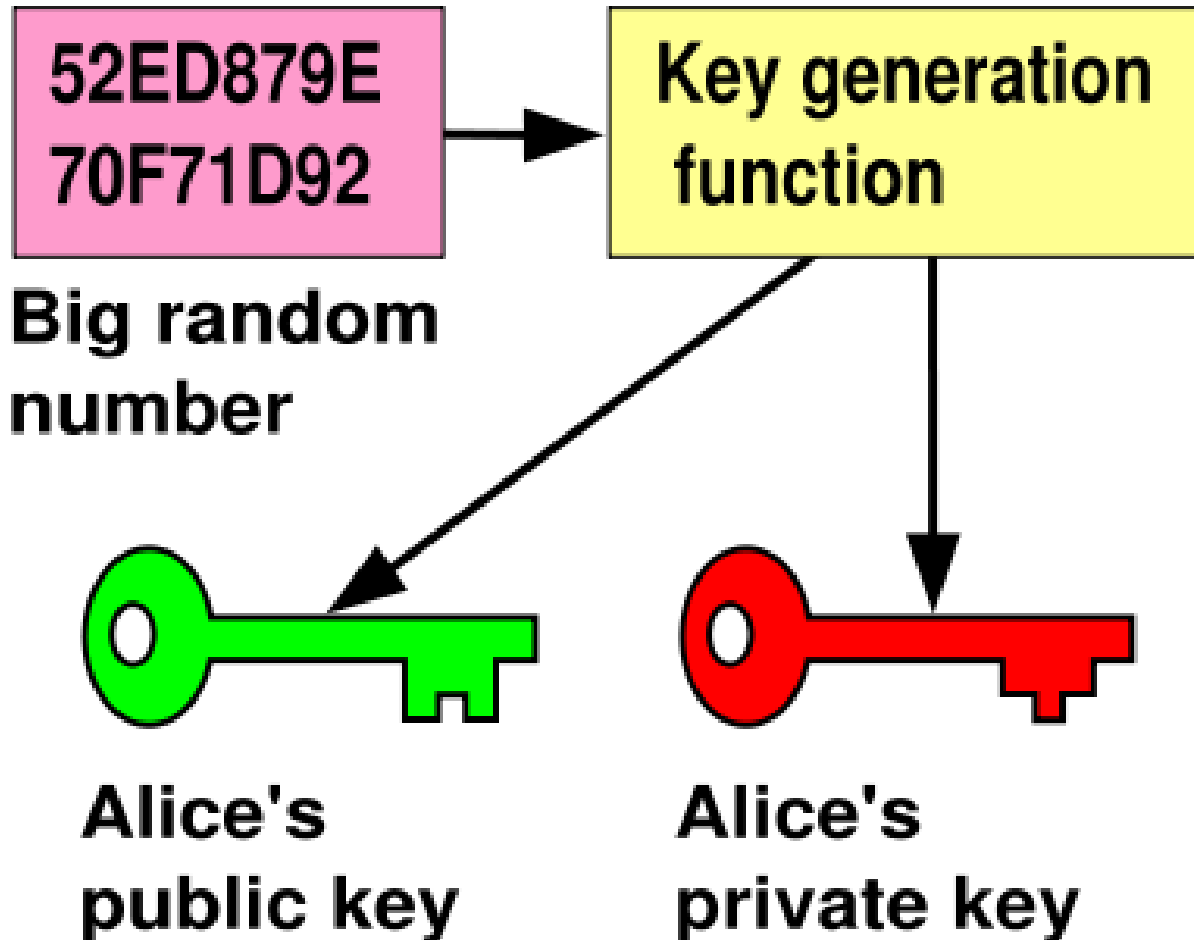
Public and Private Keys

- Each user has a **pair** of cryptographic keys—a public key and a private key.
- The keys are related in such a way that a message encrypted with the public key can only be decrypted with the corresponding private key.

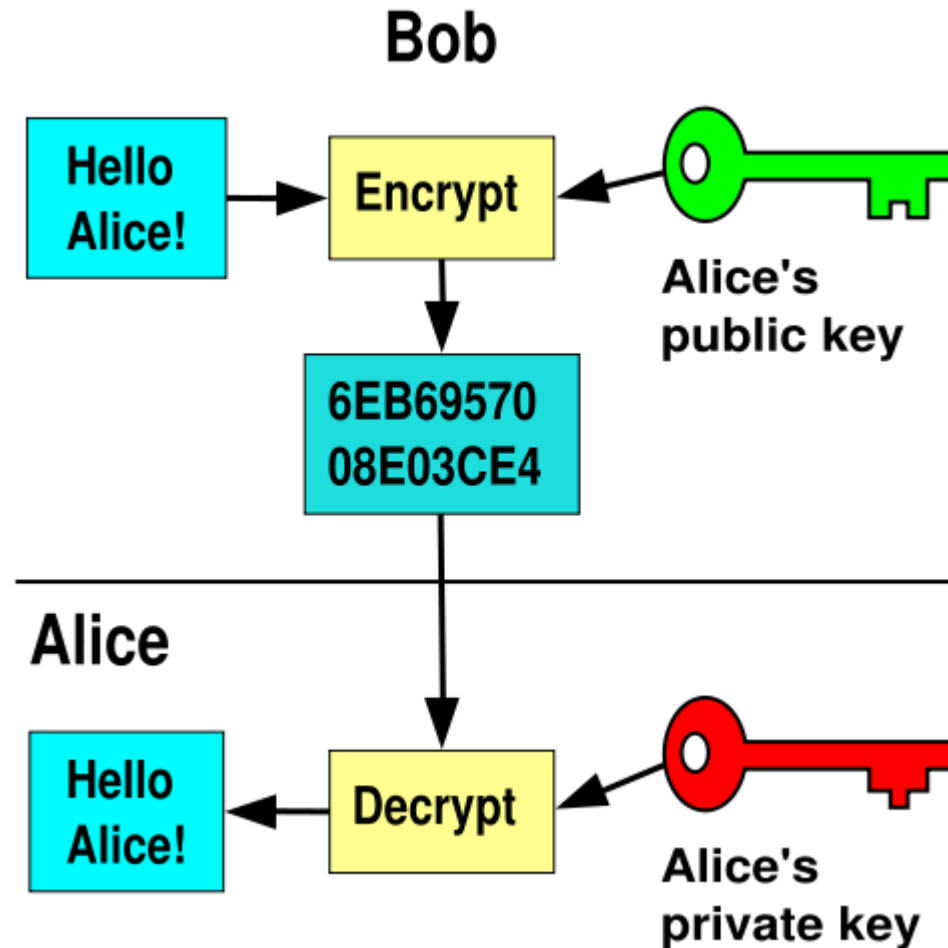


Generating a key pair

Alice

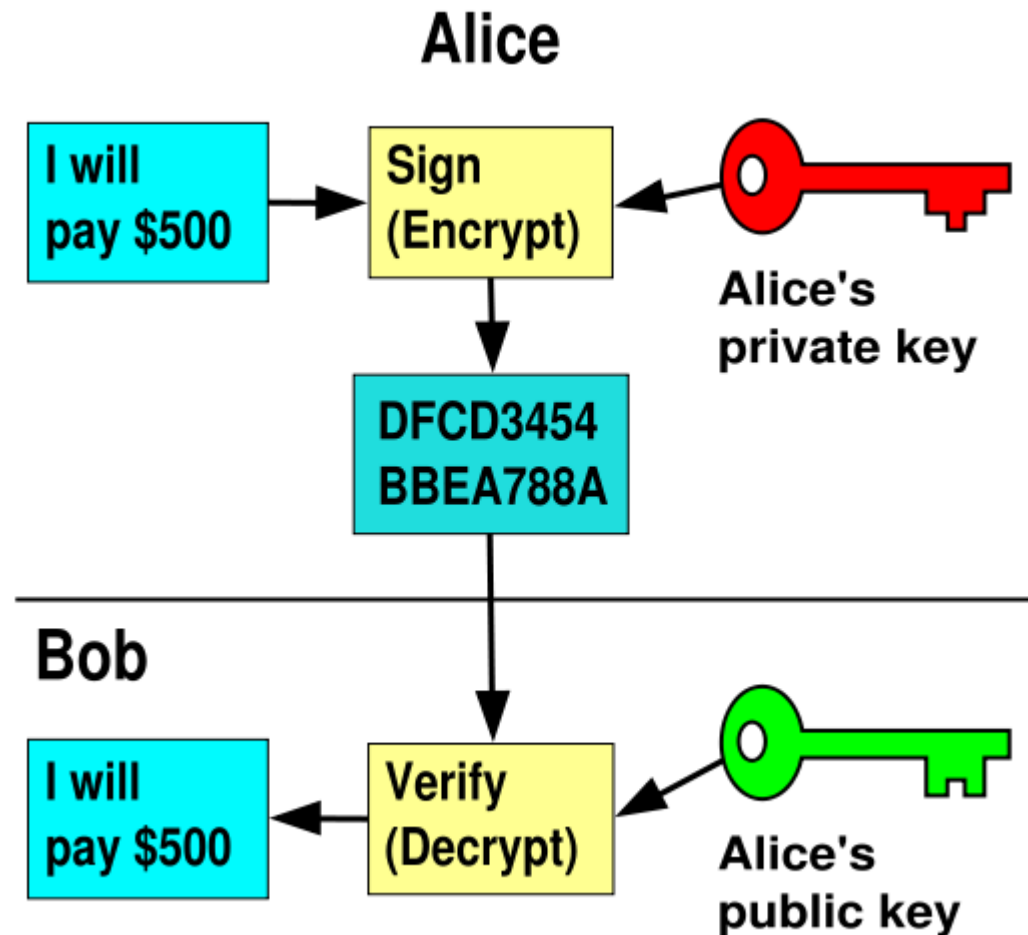


Encrypting communications with the public key



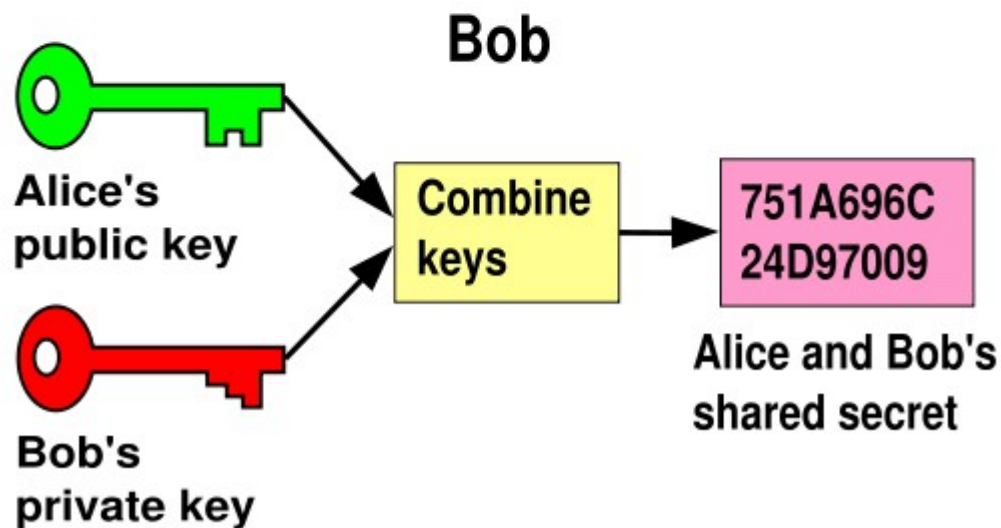
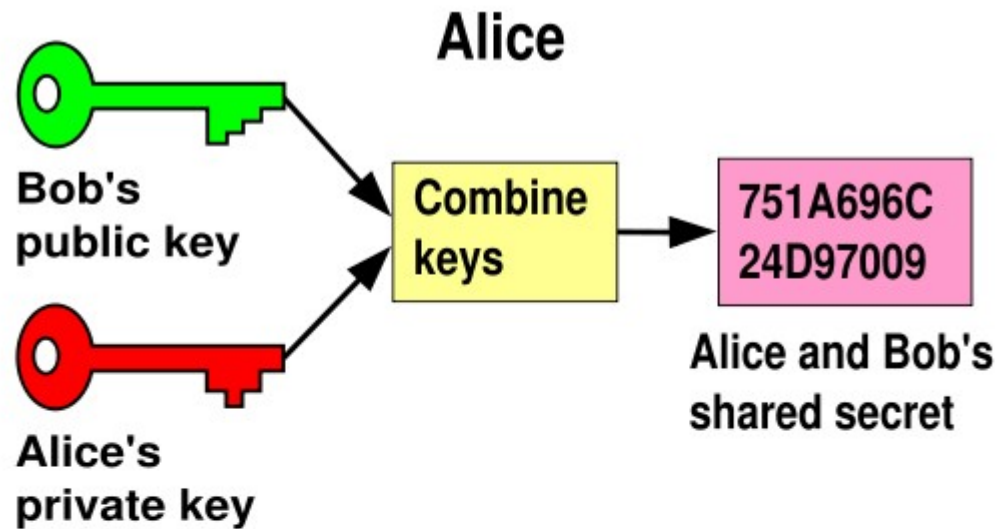
Anyone can encrypt using the public key, but only the holder of the private key can decrypt.
Secrecy depends on the secrecy of the private key.

Digital Signing



Using a private key to encrypt a message; anyone can read and check the signature using the public key.
This verifies that only the holder of the private key sent the message.

Two-way private communication



Digital Certificates

- To implement public-key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in. A digital certificate is basically a bit of information that says that the Web server is trusted by an independent source known as a certificate authority. The certificate authority acts as a middleman that both computers trust. It confirms that each computer is in fact who it says it is, and then provides the public keys of each computer to the other.

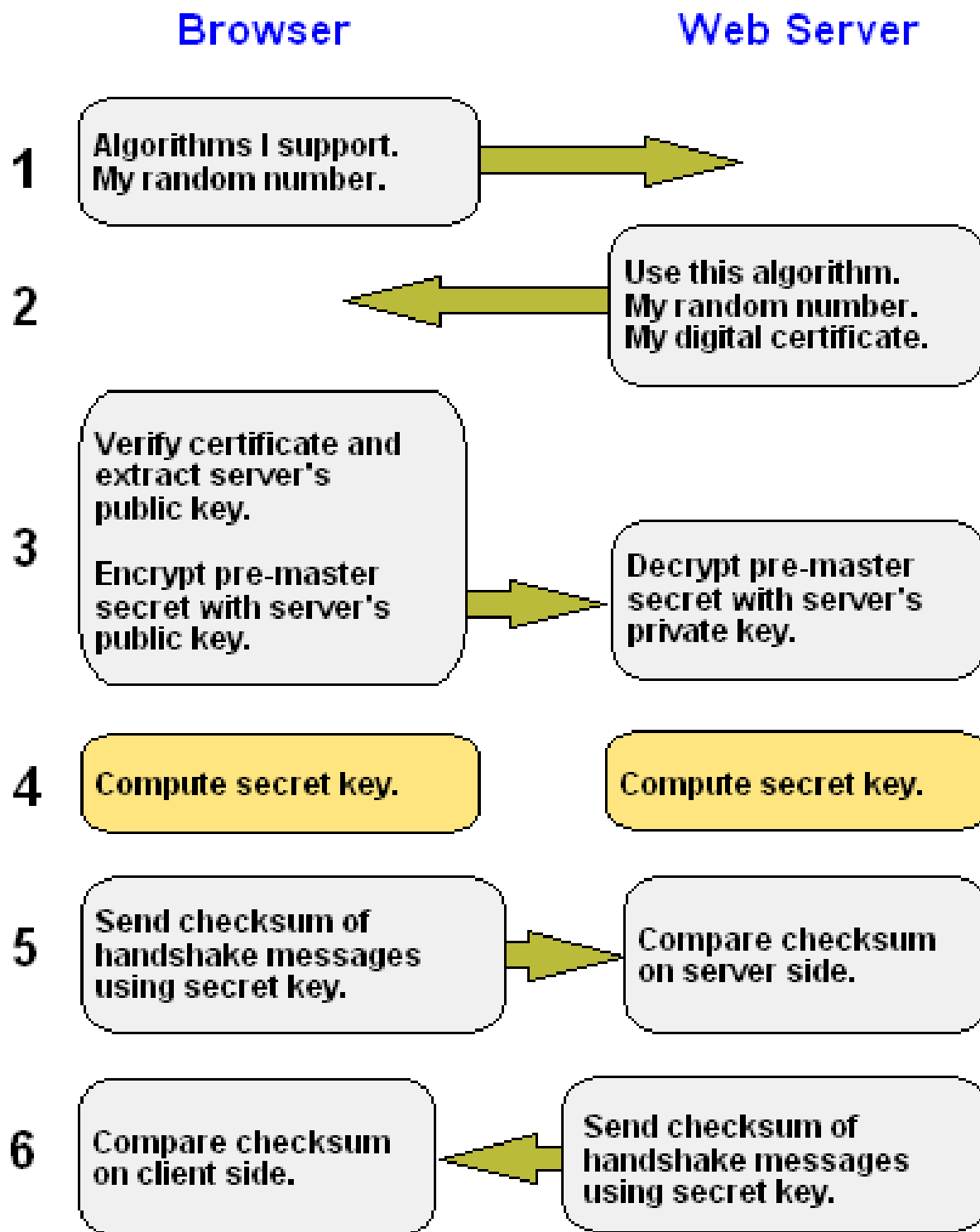
Public Key: SSL

- A popular implementation of public-key encryption is the Secure Sockets Layer (SSL).
- Originally developed by Netscape, SSL is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information, ie credit card details.



SSL Handshake

These steps take place to negotiate an SSL session before any user data is transmitted.



Public Key: SSL

- When two computers initiate a secure session, one computer creates a symmetric key and sends it to the other computer using public-key encryption.
- The two computers can then communicate using symmetric-key encryption.
- Once the session is finished, each computer discards the symmetric key used for that session.
- New sessions require that a new symmetric key be created, and the process is repeated.

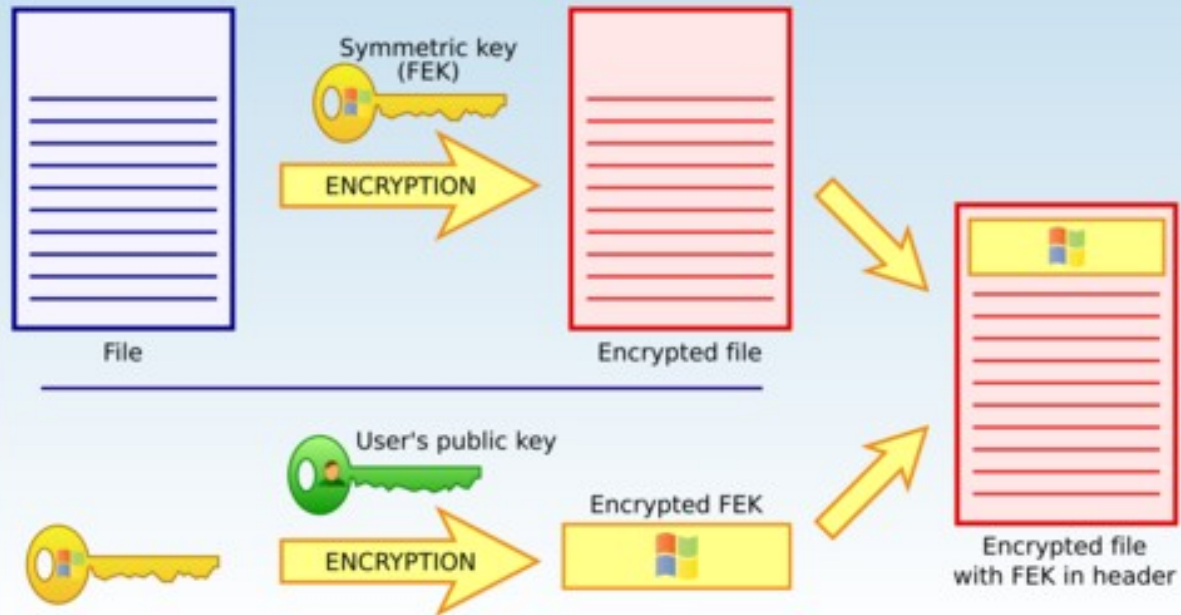
EFS

- EFS – Encrypted File System
- is used to encrypted stored data onto a hard drive or removable media.
- EFS uses a combination of symmetrical and public key encryption.

EFS

- The file encryption key (FEK) — a symmetric bulk encryption key — is used to encrypt the file.
- The FEK is then itself encrypted by using the public key of the user.
- The encrypted FEK is stored with the encrypted file and is unique to it.
- To decrypt the FEK, EFS uses the users private key which only the file encryptor has.

FILE ENCRYPTION



FILE DECRYPTION

