**Encryption notes:**

Encrypted with computer 2’s public key.

Public Keys are exchanged

Computer 2

Public Key

Private key

Interceptor also gets hold of both computers public keys

Computer 1

Computer 1 wants to send a plain text document to computer 2 but without it being read by the interceptor. So computer 1 encrypts it with computer 2’s public key.

As the Document sent from computer 1 was encrypted with computer 2’s public key. Computer 2 can decrypt it with his own private key. Computer 2 is the only person who can decrypt the document.

Public Key

Private key

Interceptor

Interceptor can’t decrypt the Document because he does not have computer 2’s private key

Encryption can be used for encrypting datagrams (packets) across the internet to stop a hacker using a packet sniffer to find out information like bank account details, passwords usernames, and reading your emails. When you buy something online you enter your bank account details, the packets containing your bank account details are sent to the websites host server. From there you’re the packet will be decrypted with the servers private key. If this is the first time you have entered your bank account details, the server will hash the data (convert to unreadable form), and salt (add random digits).

Key words:

Encryption

Decryption

Decipher

Cipher

Key public / private

Plain text

Cipher text

Decrypted by server

Encrypted Packets containing bank account details

Hashed, salted

Data base

Sender

HTTP server port (80)

TCP decrypts the packets

Server