# Computing Y11 – Preventing cyber security threats & Encryption

The de Ferrers Trust

| Key Vocab | |
|---|---|
| **Antimalware** | Software designed to protect a computer in one of 3 ways: preventing installation of harmful software, preventing important files from being changed, scanning for virus activity on the system and removing as appropriate. Antimalware protects against worms, Trojan Horses, spyware, adware and keyloggers. |
| **Antivirus** | Software designed to protect against viruses. |
| **Update** | New malware is released regularly and so anti-malware definitions must be up-to-date to protect form the latest viruses. |
| **Firewall** | Hardware or software designed to prevent unauthorised access to or from a private network or intranet. All messages entering or leaving the network will pass through the firewall to be examined. |
| **Password Protection** | In a networked environment such as a school or a company, multiple users use many of the computers. Passwords should be strong (Not easy to guess, lower and uppercase letters, numbers, symbols). |
| **Access Levels** | Part of an access control procedure for computer systems, which allows a system administrator to set up a hierarchy of users. Thus, the low-level users can access only a limited set of information. |
| **Encryption** | Changing data before transmission so someone can only decipher it with the appropriate key to unlock information. Interceptors would find the message unintelligible. |
| **Key** | A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. |
| **Symmetric Key encryption** | A secret key algorithm (sometimes called a symmetric algorithm) is a cryptographic algorithm that uses the same key to encrypt and decrypt data. |
| **Asymmetric key encryption** | Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data.<br>The keys are simply large numbers that have been paired together but are not identical (asymmetric). |

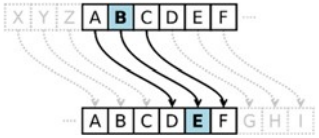


*Figure 3 – Symmetric encryption methods such as the Caesar cipher involve shifting letters along the alphabet.*

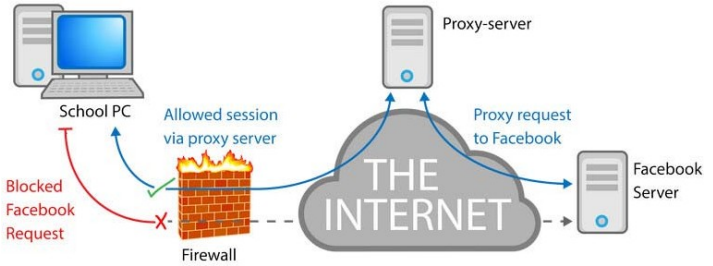


*Figure 1 - A firewall sits on the edge of a network and chooses which traffic to allow through using a set of rules. As shown above the rules may not always be strong enough.*

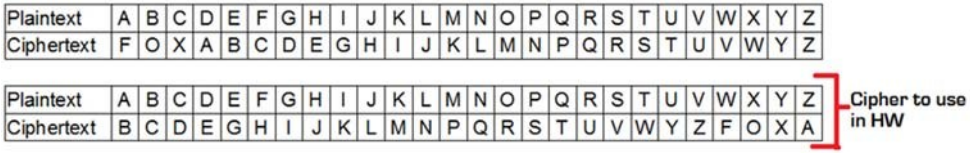


*Figure 2 - Keyword encryption involves using a keyword to begin filling up the alphabet, then the rest is filled with remaining letters.*

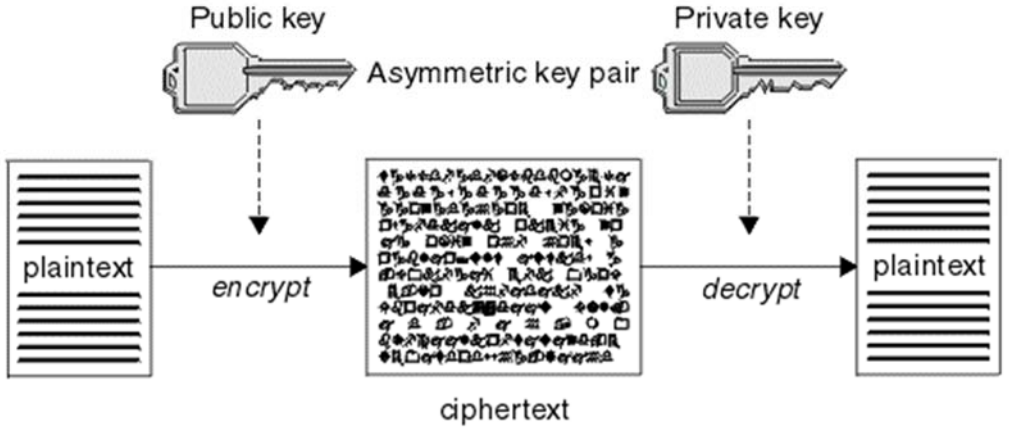


*Figure 4 - Asymmetric key encryption uses public keys to encrypt data for somebody who then uses their private key to decrypt it.*