CIPHERS

In a stream cipher, each byte of data in the plaintext is encrypted one at a time. This is suitable for encrypting communications where the total length of the message is not known. The plaintext is combined with a separate randomly generated message, calculated from the key and an initialization vector (IV). The IV ensures the key produces a unique ciphertext from the same plaintext. The keystream must be unique, so an IV must not be reused with the same key. The recipient must be able to generate the same keystream as the sender and the streams must be synchronized. Stream ciphers might use markers to allow for synchronization and retransmission. Some types of stream ciphers are made self-synchronizing. – COMPTIA TOPIC 5A

In a block cipher, the plaintext is divided into equal-size blocks (usually 128-bit). If there is not enough data in the plaintext, it is padded to the correct size using some string defined in the algorithm. For example, a 1200-bit plaintext would be padded with an extra 80 bits to fit into 10 x 128-bit blocks. Each block is then subjected to complex transposition and substitution operations, based on the value of the key used. – COMPTIA TOPIC 5A

Symmetric encryption is usually faster than asymmetric because it there is less calculations involved, this is why symmetric is better for encrypting large amounts of data.

Hashing algorithms contribute to integrity by making sure that no data has been altered.