**Definitions**

# **Cryptography terms**

Here are a few definitions of some terms relating to cryptography and cryptosystems:

**Plaintext**: The original message in its original legible form.

**Ciphertext**: Encrypted text that will appear to be a random string.

**Encryption**: The process of converting data into its cryptic form that prevents unauthorized access, i.e. converting plaintext to ciphertext. This process requires encryption keys which provide information regarding the specific implementation of a given encryption algorithm.

**Decryption**: The process of converting encrypted data back into its original form for use, i.e. converting ciphertext back to plaintext. Decryption requires a decryption key which provides the specific information required to ‘undo’ the encryption.

**Symmetric Key Cryptosystems**: Cryptosystems that use the same key for encryption as well as decryption. This key is assumed to be a shared secret between the two parties exchanging messages. A few examples of Symmetric Key Cryptosystems:

Cipher: A system of encryption that maps each character to a substitute.

Code: A system of encryption that maps each word or feature to a substitute.

Shift Cipher: A cipher that replaces each character with another chosen by moving forwards through the alphabet by some fixed shift factor.

**Asymmetric or Public Key Cryptosystems**: Cryptosystems that use public-private key pairs. This enables anyone to encrypt messages for sending to the publisher of the keys (using the public key) but only the holder of the private key will be able to decrypt the messages.

**Digital Signatures**: A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

# **Number theory terms**

The following are some important concepts required for cryptography from the field of number theory

**Modulo**: The remainder operator (e.g. 17 modulo 5 is 2, i.e. 17 when divided by 5 leaves a remainder of 2). This is often shortened to mod, we write 17 ≡ 2 (mod 5), read as "17 is congruent to 2, modulo 5".

**Coprime**: In number theory two values are said to be coprime or relatively prime if they do not share any common prime factors. That’s to say that their greatest common divisor (GCD) or highest common factor is 1.