**Discuss how cryptography uses codes and ciphers to turn plain text into cipher text. Give at least three different types of cryptographic algorithms, as well as how cryptographic keys work.**

According to Wills, “*Cryptographic algorithms* are the formal definition of the processes we use to encrypt plaintext into ciphertext and then decrypt ciphertext back to plaintext.” (2019). By assigning symbols, whether they are pictures, letters, numbers, or other characters, to represent to correlate with the alphabet being used for the plain text, it obscures the original data. Without knowing the key used to create the encoded data, it can be challenging, at best, to decode the original data. These keys (cryptographic keys) are the tools used to lock and unlock (encode and decode) data so that only those with access to the key is able to make any meaningful sense out of the data. Cryptographic key systems come in two types, symmetric (the same key is used by everyone with proper access) and asymmetric (public/private keys).

Some common encryption algorithms are Triple DES ( Triple Data Encryption Standard or TDES), Advanced Encryption Standard (AES), RSA Security, Blowfish, and Twofish. TDES uses three 56 bit keys (total key length of 168 bit) and is slowly being phased out and replaced by AES. AES, which is the most trusted by the US government, uses key lengths of 128, 192, and 256 bits. RSA security is an asymmetric key algorithm (using public and private keys) and is the standard for encryption over the internet. Blowfish is a freely available, public domain algorithm that splits data into 64 bit blocks and encrypts each block individually. Twofish is the successor to Blowfish. Twofish is also public domain but the blocks may be up to 256 bits in length.

**References**

Wills, M. (2019). *(ISC)2 SSCP Systems security certified practitioner: Official study guide (2nd ed.)*. John Wiley & Sons.