Encryption with a one-time pad is a type of symmetric-key encryption that uses a randomly generated key to encrypt a plaintext message. A one-time pad is considered to be an unbreakable encryption technique, as long as the key is truly random and is used only once.

History

The one-time pad encryption technique was first proposed by Gilbert Vernam in 1917, and it was later independently discovered by Joseph Mauborgne and AT&T engineer Joseph O. Baker. The one-time pad encryption technique was first used by the US Army during World War I, and it has been used in various contexts since then.

Encryption Process

The one-time pad encryption technique uses a randomly generated key that is at least as long as the plaintext message. The key is generated using a truly random process, such as a hardware random number generator or a physical process that generates random data, such as atmospheric noise.

To encrypt a plaintext message using a one-time pad, each letter of the plaintext message is converted to a numerical value based on its position in the alphabet (e.g. A=1, B=2, C=3, etc.). The corresponding letter in the key is also converted to a numerical value. The two numerical values are added together modulo 26 to produce the ciphertext letter.

To decrypt the ciphertext message, the same process is followed in reverse. Each letter of the ciphertext message is converted to a numerical value, and the corresponding letter in the key is also converted to a numerical value. The two numerical values are subtracted modulo 26 to produce the plaintext letter.

Security

Encryption with a one-time pad is considered to be unbreakable, as long as the key is truly random and is used only once. This is because each key can only be used to encrypt a single message, and there is no pattern or repetition in the key that an attacker could use to decipher the ciphertext message. However, if the key is not truly random or is used more than once, the encryption may be vulnerable to various cryptanalytic attacks.

Despite its theoretical security, the use of one-time pads can be impractical in many contexts due to the requirement for truly random and secure key generation, as well as the need for secure key distribution. As a result, other encryption techniques, such as the Advanced Encryption Standard (AES), are typically used in practical applications.