The One-Time Pad (OTP)

- This is a special case of the substitution cipher, invented near the end of WWI and was mathematically proven unbreakable by Claude Shannon during WWII (published in the late 1940s).

- Typically, the plaintext letter is combined (not substituted) in some manner (e.g., XOR) with the key character at that position.

- The one-time pad can be called a substitution cipher only as a special case, that being that typically, the plaintext letter is combined (not substituted) in some manner (e.g., XOR) with the key material character at that position.

- Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or **pad**) of the same length as the plaintext, resulting in a ciphertext.

- In order for the unbreakable property of OTP is to hold true, the following conditions must be unconditionally met:

    - The key must be truly random
    - The key must be as large as or greater than the plaintext
    - The key must never reused in whole or part, and must be kept secret from everyone except the sender and receiver.

- If the above conditions hold true, then the ciphertext will be impossible to decrypt or break without knowing the key.

- The OTP is not very practical since the strict conditions listed above are very difficult to not violate.

- Although traditional OTP method provides an infinite key space to increase the uncertainty factor, this method has drawback that length of key should be as long as the plaintext.

- The sample program is a POC that illustrates the use of OTP techniques. It generates a random key each time it is run and produces the ciphertext.

- The same key is then used to decrypt ciphertext and produce the plaintext.

- The algorithm associates numerical values to each character and then uses the keystream to encrypt the plaintext using the numerical values as indices (or offsets).

- This algorithm can be improved and made more secure by incorporating bit-manipulation into the cipher. This is the topic for your next assignment.