One-Time Pad:

One of the goals of cryptography is perfect secrecy. A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain. This idea is used in a cipher called one-time pad, invented by Vernam.

- **The key has the same length as the plaintext and is chosen completely in random.**
- **A one-time pad is the perfect cipher, but it is almost impossible to implement commercially. If the key must be newly generated each time, how can Alice tell Bob the new key each time she has a message to send?**
- **However there are some occasions when a one-time pad can be used. For example: if the president of a country needs to send a completely secret message to the president of another country, she can send a trusted envoy with the random key before sending the message.**
- **The encryption and decryption algorithms each use a single exclusive-or operation. Based on the properties of the exclusive-or operation, the encryption and decryption algorithms are inverses of each other. It is important to note that in this cipher the exclusive-or operation is used one bit at a time. In other words, the operation is over 1-bit word and the field is GF(2).**

Security analysis:

- **There is no way that an adversary can guess the key or the plaintext and ciphertext statistics.**
- **There is no relationship between the plaintext and ciphertext, either. In other words, the ciphertext is a true random steam of bits even if the plaintext contains some pattern.**
- **Eve cannot break the cipher unless she tries all possible random key streams, which would be 2^n if the size of the plaintext is n bits.**

Implementation Issue:

How can the sender and the receiver share a one-time pad key each time they want to communicate? They need to somehow agree on the random key. So this perfect and ideal cipher is very difficult to achieve.