Cryptography Lab 1

Jordi Nadeu Ferran

1 Many time pad attack

The many time pad attack exploits the reuse of a key in encryption systems that rely on XOR operations, such as the One Time Pad (OTP). The OTP is theoretically secure when each key is used only once and is as long as the plaintext. However, when the same key is used to encrypt multiple plaintexts, it introduces vulnerabilities that can be exploited to recover the plaintexts and potentially the key itself.

The many time pad attack works because XOR encryption has the following property, that the XOR operation is symmetric, meaning if the same key is used to encrypt multiple plaintexts, the ciphertexts become predictable making it possible to deduce parts of the plaintext.

The main mitigation strategy, are ensure that each encryption operation uses a unique key. This can be achieved through proper key management systems or using cryptographic schemes like stream ciphers with unique initialization vectors (IVs). Another thing we can do to mitigate this kind of attack is using modern encryption methods like AES (Advanced Encryption Standard) that don't rely on key reuse for security.