

CS3441/9441 Tutorial 1

1. Solve the substitution cipher problem
2. Suppose $E(M, K)$ is M encrypted by one time pad K . Assume that M and K are binary strings and encryption is done by bitwise exclusive or. Show that for *every* plaintext M' of the same length as M , there exists a key K' such that

$$E(M', K') = E(M, K)$$

3. Consider the version of cipher block chaining where the plain-text blocks $P_1P_2P_3 \dots P_n$ are mapped to the ciphertext blocks $C_1C_2C_3 \dots C_n$ by the equations

$$C_1 = E(P_1, K)$$

$$C_{i+1} = E(P_{i+1} \otimes C_i, K)$$

Explain how to decrypt messages for this method, by giving the equations for decryption and proving that decryption is the inverse of encryption.