CS5285: Information Security for eCommerce Autumn, 2024
Tutorial 3, Week 4 (September 29)

Questions:

1. **Block Cipher**: What are the advantage and disadvantage of *stream cipher* vs. *block cipher*?

2. **3DES**: Consider 3DES:
$$C = \mathrm{DES}_{K_1}(\mathrm{DES}^{-1}_{K_2}(\mathrm{DES}_{K_1}(M)))$$
where C, M are the ciphertext and plaintext, respectively, and $K = (K_1, K_2)$ is the key. How many keys on average do we have to try in a bruteforce attack?

3. **DESX**: Let AESX-192 be a block cipher which is similar to DESX but has the DES being replaced by AES and the AES key size is 192 bits. Compute the total effective key length of the AESX-192.

4. **3AES**: Change 3DES to 3AES with two 128-bit keys; then compare 3AES and AES-256 (i.e. the AES with 256-bit keys) in terms of security (resistance to brute force) and performance (execution time).

5. **CBC Mode**: Consider a block cipher with CBC mode.

CBC Encryption	CBC Decryption
$C_0 = E(K; IV \oplus P_0)$	$P_0 = IV \oplus D(K; C_0)$
$C_1 = E(K; C_0 \oplus P1)$	$P_1 = C_0 \oplus D(K; C_1)$
$C_2 = E(K; C_1 \oplus P2)$	$P_2 = C_1 \oplus D(K; C_2)$
...	...

   (a) During *encryption*, if one block of the *plaintext* input is different (two indentical messages, except for 1 bit), how many blocks of the corresponding ciphertext will be effected?

   (b) During *decryption*, if one block of the *ciphertext* input is incorrect (an error occurs during transmission), how many blocks of the corresponding plaintext will be effected?

   (c) What happens if the receiver has an incorrect IV when decrypting blocks of ciphertext in CBC mode?