# Introduction to Information Security

# Assignment 2

Total Marks: 110

Deadline: February 23, 2023 (Thursday), 5:00 PM (in Class Room)

1. Using the inverse MixColumns transformation of the Advanced Encryption Standard (AES), calculate the bytes of a state matrix $(S)$ whose first column contains the byes $\{88\}$, $\{6F\}$, $\{49\}$ and $\{A6\}$.

   [4 * 5 = 20]

2. Suppose that the round key for round $9$ for AES algorithm is AF D2 76 22 B5 7D BC DD 31 2B F6 69 FF 8D 28 2F. Then, using the expandkey algorithm, compute the round key for round $10$.

   [20]

3. (a) In RSA public key cryptosystem, if $n = p \times q = 274279$ and $\phi(n) = 272376$ are known to an adversary, find the primes $p$ and $q$. Hence, prove that if the public key $(e, n)$ is known to the adversary, he/she can easily derive the private key $(d, n)$.

   (b) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ with the primes $p_1$, $p_2$, $\cdots, p_r$ and $k_i \geq 0$, compute $\phi(n)$. Using this, compute $\phi(9000)$.

   (c) Decrypt the ciphertext

   1037 0431 0629 0690 0204 2267 0595

   that was encrypted using the RSA algorithm with the public key $(e, n) = (211, 2419)$. Note that the private key is $(d, n) = (11, 2419)$. Use the standard encoding procedure:
   A = 01, B = 02, . . ., Z = 26,

, = 27, . = 28, ? = 29,

0 = 30, 1 = 31, . . ., 9 = 39, ! = 40.

[10 + 10 + 20 = 40]

4. Users $A$ and $B$ use the Diffie-Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.
   (a) If user $A$ has private key $X_A = 39$, what is the $A$'s public key $Y_A$?
   (b) If user $B$ has private key $X_B = 42$, what is the $B$'s public key $Y_B$?
   (c) What is the secret shared key?

[5 + 5 + 10 = 20]

5. Consider an ElGamal encryption scheme with a common prime $q = 71$ and a primitive root $\alpha = 7$. If the user $B$ (the receiver) has a public key $Y_B = 11$ and the user $A$ (the sender) chooses a private key $X_A = 7$, determine the ciphertext of the plaintext message $M = 40$.

[10]

***Submission Instructions***

Copying in assignments leads to award ZERO marks in assignment marks. Also, the source from which you have copied, that source student will be treated under the same rule.

Please submit the assignment in hard copy stating the following at the top:

Introduction to Information Security

Assignment Set 2

submitted by

Name: XYZ, Roll No: abc