11120IIS/500400 Applied Cryptography, Spring 2023 **19-Apr-2023**

Midterm

Instructor: Prof. Amir Rezapour

1. Discuss the advantages and disadvantages of public-key and symmetric-key cryptosystems. (10 points)

2. Describe the polynomial-time reduction $A \preceq_{ploy} B$. (10 points)

3. What is the Kerckhoff's principle in cryptanalysis? (10 points)

4. We use DES in cipher feedback mode (CFB) to encrypt a plaintext $m = m_1 m_2 \ldots m_{100}$ into a ciphertext $c_1 c_2 \ldots c_{100}$, where each m_i is 16-bit long. The ciphertext is sent to Bob. If c_{16} and c_{26} are missing and c_9 and c_{89} are received as c'_9 and c'_{89} wrongly, what m_i's can B compute correctly from the received ciphertext? (10 points)

5. Assume that a plaintext bit M is given with $Pr[M = b] = p_b$, where $b \in \{0, 1\}$. Assume that random key K of the one-time pad encryption is chosen by $Pr[K = 0] = 0.42$ and $Pr[K = 1] = 0.58$. Consider the one-time pad encryption $C = M \oplus K$.

   (a) Assume that an adversary A_1 guesses M randomly without even examining the ciphertext C. Show that the success probability of A_1 is exactly 0.5. (10 points)

   (b) Suggest a good strategy A_2 of guessing M if p_0 and p_1 are known. (15 points)

6. Use the Chinese Remainder Theorem to compute $0 \leq x < 1785$ for $x \bmod 7 = 1, x \bmod 15 = 3$, and $x \bmod 17 = 12$. (15 points)

7. In the SubBytes of AES, $f(x) = x^{-1} \bmod X^8 + X^4 + X^3 + X + 1$. Compute $f(01100011)$. (20 points)