11120IIS/500400 Applied Cryptography, Spring 2023 **Due: 26-Apr-2023**

Homework 1

Instructor: Prof. Amir Rezapour

1. 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 $Pr[K = 0] = 0.6$ and $Pr[K = 1] = 0.4$. 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. (20 points)

   (b) Suggest a good strategy A_2 of guessing M if p_0 and p_1 are known. (20 points)

2. The Euclidean algorithm computes $gcd(a, b)$.

   (a) Give the algorithm and show that its computation time is polynomial in the total length m of a and b, where $m = len(a) + len(b)$. (10 points)

   (b) Solve the equation $r \times 128 + s \times 54 = 2$. (10 points)

3. In the SubBytes of AES, $f(x) = x^{-1}\ mod\ X8 + X4 + X3 + X + 1$. Compute $f(11101001)$. (20 points)

4. Use the Chinese Remainder Theorem to compute $0 \leq x < 352$ for $x\ mod\ 3 = 1$, $x\ mod\ 11 = 3$, and $x\ mod\ 16 = 13$. (20 points)