**UConn, School of Computing**
**Fall 2024**
**CSE 3400/CSE 5850: Introduction to Computer and Network Security / Introduction to Cybersecurity**

# Assignment 2

Instructor: Prof. Ghada Almashaqbeh
Posted: 9/18/2024
Submission deadline: 9/26/2024, 11:59 pm

**Note:** Solutions **must be typed** (using latex or any other text editor) and must be submitted as a pdf (not word or source latex files).

**Problem 1 [45 points]**
Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF, state whether the following constructions are secure PRFs (in all parts $k$ is a long random secret key).

1. $F'_k(x) = F_k(\bar{x}) \parallel F_k(x)$, where each of $k$ and $x$ is of length $n$ bits, and $\bar{x}$ is the bitwise negation of $x$.
2. $F''_k(x) = \big(F_{k_1}(x) \oplus F_{k_2}(x)\big) \parallel x$, where $k = k_1 \parallel k_2$, and each of $k_1, k_2, x$ is of length $n$ bits.
3. $F'''_k(x) = lsb(F_{k_1}(x)) \parallel F_{k_2}(x)$, where $k = k_1 \parallel k_2$, each of $k_1, k_2, x$ is of length $n$ bits, and $lsb$ is the least significant bit.

**Note:** if the scheme is not a PRF then provide an attack against it and analyze/justify its success probability. If the scheme is a PRF, just provide a convincing argument (formal proofs are not required) and state why the attacker advantage is negligible.

**Problem 2 [45 points]**
Let $G : \{0,1\}^{n/2} \rightarrow \{0,1\}^n$ be a secure PRG, and $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF. For each of the following encryption constructions, state the decryption algorithm, and then state whether it is a secure encryption scheme against a CPA attacker. (All the following are block ciphers; we encrypt $m$ all at once, and in all parts $k$ is a long random secret key.)

1. Given message $m \in \{0,1\}^n$, choose random string $r \in \{0,1\}^n$, and form an encryption as: let $y = F_k(r)$, $E_k(m) = (RH(y), G(RH(y)) \oplus m)$, where $RH$ is the right half of the string.
2. Given message $m \in \{0,1\}^n$, choose a random string $r \in \{0,1\}^n$ and encrypt $m$ as $E_k(m) = (r, F_k(F_k(r)) \oplus m)$.
3. Given message $m \in \{0,1\}^{3n}$, parse $m$ as $m = m_1 \parallel m_2 \parallel m_2$ where $|m_1| = |m_2| = |m_3| = n$, then choose a random $r \in \{0,1\}^n$ and a random $r' \in \{0,1\}^n$ and encrypt $m$ as: $E_k(m) = (r, r', F_k(1^n) \oplus m_1, F_k(r) \oplus m_2, F_k(r') \oplus m_3)$.

**Note:** If the scheme is insecure then provide an attack against it and analyze its success probability. If the scheme is secure, just provide a convincing argument (formal security proofs are not required) and state why the attacker advantage is negligible.

**Problem 3 [15 points]**

- Alice claims that OTP is a deterministic encryption scheme (so it cannot be secure against a CPA attacker) since there is no randomness generation in OTP. Is her claim true? Justify your answer.
- Show how to decrypt (or basically invert) using the Feistel network shown in Slide 10, Lecture 4. So given an input $g_k(m)$ that is described in that slide, can you get $m$ back using the same network structure? If yes, how?

**Note:** This problem has 5 points bonus.