UConn, CSE Dept.
Spring 2023
CSE 3400/CSE 5080: Introduction to Computer and Network Security
(or Introduction to Cybersecurity)

Assignment 2

Instructor: Prof. Ghada Almashaqbeh
Posted: 2/10/2023
Submission deadline: 2/18/2023, 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).
Note: This homework will have a **shorter late days allowance** than usual. It will be only 4 days (instead of the usual 5), after which no late submissions will be accepted. And as usual, if you still have free late days, you can up to 4 days from them, and if not, there will be a deduction for late days.

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

1. $F'_k(x) = (x \oplus k) \parallel F_k(x) \parallel F_k(x+1)$, where each of k and x is of length n bits.
2. $F''_k(x) = F_{k_1}(x) \oplus F_{k_2}(x)$, where $k = k_1 \parallel k_2$, and each of k_1, k_2, x is of length n bits.
3. $F'''_k(x) = k_1 \parallel F_{k_2}(x)$, where $k = k_1 \parallel k_2$ and each of k_1, k_2, x is of length n bits.

Note: if the scheme is not a PRF then provide an attack against it and informally 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 PRG, and $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a 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, they are not stream ciphers). (In all parts k is a long random secret key)

1. Given message $m \in \{0,1\}^n$, choose random string $r \in \{0,1\}^{n/2}$, and form an encryption as: let $y = G(r)$, $E_k(m) = (y, F_k(y) \oplus m)$.
2. Given message $m \in \{0,1\}^n$, choose a random string $r \in \{0,1\}^n$ and encrypt m as $E_k(m) = (r, lsb(F_k(r)) \parallel (F_k(r) \oplus m))$ where lsb is the least significant bit.
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 $r \in \{0,1\}^{n/2}$ and $r' \in \{0,1\}^n$ and encrypt m as: $E_k(m) = (r, r', G(r) \oplus m_1, F_k(r') \oplus m_2, F_k(r'+1) \oplus m_3)$.

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

Problem 3 [15 points]

- We know that a deterministic encryption scheme is not secure against a CPA attacker. Is it secure against a CTO attacker? why?
- For the basic PRF-based encryption scheme we took in class (which is provably secure against CPA attacker), we use a PRF (call it F), for each message a random string r is generated and then encryption is $E_k(m) = (r, F_k(r) \oplus m)$. Is this scheme still secure against a CPA attacker if the length of the message m (and so the output of the PRF) is 1 bit? why?

Note: this problem has 5 points extra.