CSC591/495 Cryptography. Midterm Exam.

17 October 2018

Name: ______________________ Unity ID: ______________________

Problem 1. PRF [60 points] Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a Pseudorandom Function (PRF). Let z be a public string.

Problem 1a Let F^1 be the keyed function described below. Is F^1 a Pseudorandom Function? If yes, prove it by showing a reduction. If no, show a distinguisher and analyse its distinguishing advantage.

$F^1_k(x) = F_k(x) \oplus F_z(x)$.

Problem 1.b Let $F^2 : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^{2n}$ be the keyed function described below. Is F^2 a Pseudorandom Function? If yes, prove it by showing a reduction. If no, show a distinguisher and analyse its distinguishing advantage.

$F_k^2(x_1||x_2) = F_k(x_1)||F_k(x_2 \oplus k)$

Problem 2. Private-Key Encryption Scheme (CPA-security) [20 points]
Let F be a Pseudorandom Permutation (PRP). Recall that a PRP can be evaluated in both directions, that is $y = F_k(x)$ and $x = F_k^{-1}(y)$ by someone who knows the key k. Let $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme for messages of length n, and consider the encryption procedure Enc below:

$\underline{\Pi.\mathsf{Enc}(k, m)}$

1. $r \xleftarrow{\$} \{0,1\}^n$
2. $y \leftarrow F_k(m) \oplus r$
3. Output r, y.

1. Describe the correspondent decryption procedure
   $\underline{\Pi.\mathsf{Dec}(k, r, y)}$
   (a)
   (b)
   (c) Output
2. Is Π CPA-secure? If yes, write the formal proof. If not, describe an adversary and analyse its advantages in winning the CPA-security game.

Problem 3. Public-Key Encryption Scheme (CPA-security) [20 points] Let $\mathbb{Z}_N^*$ be a multiplicative group where the RSA assumptions holds. Let e, N be a RSA **public key** and let d be the correspondent secret key. We know that textbook RSA is not CPA-secure because is deterministic. Therefore we are considering a modified version of RSA that is instead probabilistic.

$\underline{\mathsf{Enc}(m, e, N)}$

1. Pick a random $r \leftarrow \mathbb{Z}_N^*$
2. $y = r^e \pmod N$
3. $c = r \cdot m \pmod N$.
4. Output ciphertext (y, c)

1. Describe the correspondent decryption procedure
   $\underline{\mathsf{Dec}(d, y, c)}$
   (a)
   (b)
   (c) Output
2. Is this modified RSA CPA-secure? If yes, write the formal proof. If not, describe an adversary and analyse its advantages in winning the CPA-security game. **Note.** You will **not** need to use any number theory to prove/disprove security.