Information Systems and Network Security

Prof. Stefano Leucci

Question 1: Pseudorandom Functions

Provide a definition of pseudorandom function **(5 points)**.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a length preserving pseudorandom function. Show that none of the following two definitions of $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ is a pseudorandom function.

- $F'_k(x) = F_k(0\|x) \,\|\, F_k(0\|x)$ **(3 points)**
- $F'_k(x) = F_k(0\|x) \,\|\, F_k(x\|1)$ **(4 points)**

Question 2: Linear-Feedback Shift Registers

Describe the operation of a generic linear-feedback shift register (**5 points**).

Consider a linear-feedback shift register with a state of 4 bits that has been initialized to state s (via a call to `Init(`s`)`) and has subsequently been used to generate the sequence of bits `1,0,0,1,0,0,0,1` (via 8 successive calls to `Next()`).

- Recover the seed s. **(1 point)**
- Recover the linear function used to determine the leftmost bit of the register after each `Next()` operation. **(3 points)**

Question 3: Secret Sharing

Describe a 2-out-of-2 threshold secret sharing scheme (**2 points**), prove its security (**2 points**), and show how the scheme can be generalized to a n-out-of-n threshold secret sharing scheme for an arbitrary $n \geq 2$ (no proof of security is required) (**2 points**).

Alice, Bob, and Charlie shared a secret s using Shamir's 2-out-of-3 threshold secret sharing scheme with polynomials over $\mathbb{Z}_7$. Alice's share is $s_A = (1, 4)$ while Bob's share is $s_B = (2, 3)$.

- Recover the polynomial that has been used to generate the shares **(3 points)**
  Hint: The Lagrange basis polynomials (over $\mathbb{Z}_7$) for the set of x-coordinates $\{1, 2\}$ are $\ell_1(x) = 6x + 2$ and $\ell_2(x) = x + 6$.
- Recover the secret s. **(1 point)**
- Recover the share s_C of Charlie. **(1 point)**