Information Systems and Network Security

Prof. Stefano Leucci

Question 1: Definitions of Perfect Secrecy

Provide any two equivalent definitions of perfect secrecy among the ones discussed in the course **(2 points)** and prove that one of the two (of your choice) implies the other **(2 points)**.

Question 2: Security of an Encryption Scheme

Consider the encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where:

- the message space $\mathcal{M}$, the key space $\mathcal{K}$, and the ciphertext space $\mathcal{C}$ are all equal to $\{\mathtt{0},\mathtt{1}\}^n$.
- $\mathsf{Gen}(\mathtt{1}^n)$ samples two binary string x, y independently and uniformly at random from $\{\mathtt{0},\mathtt{1}\}^n$. If $x \neq \mathtt{0}^n$, it returns the key $k = x$. Otherwise it returns the key $k = y$.
- $\mathsf{Enc}_k(m)$ returns $m \oplus k$.
- $\mathsf{Dec}_k(c)$ returns $c \oplus k$.

Formally prove or disprove each of the following:

(a) Π is perfectly secret **(2 points)**

(b) Π is EAV-secure **(4 points)**

(c) Π is CPA-secure **(2 points)**

Question 3: Pseudorandom Number Generators

Define the concept of *secure pseudorandom number generator (PRG)* **(1 point)**.

Consider the function $G : \{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^{n+1}$ defined as $G(s) = (1\|s) \wedge (s\|1)$, where $\|$ denotes concatenation and $\wedge$ denotes the "bitwise and" operation. Prove that G is not a secure PRG by designing a polynomial-time distinguisher and analyzing its advantage (**3 points**).