Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60088 Foundations of Cryptography **Spring 2026**

Short Test 1 **16-February-2026, 3 PM – 3:40 PM** **Marks = 10**

Here are all questions given in short test 1.

QUESTION 1: Let G be a PRG that stretches n-bit strings to $3n$-bit strings. For $s \in \{0,1\}^n$, write $G(s) = G_0(s)\|G_1(s)\|G_2(s)$, so that $G_0(s)$, $G_1(s)$ and $G_2(s)$ represent the first, second and third n-bit components of $G(s)$ respectively. Define a new PRG G' that stretches n-bit strings to $9n$-bit strings as:

$$G'(s) = G(G_0(s))\|G(G_1(s))\|G(G_2(s)).$$

Prove or Disprove: if G is a secure PRG, then so is G'.

QUESTION 2: Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Mac}_1, \mathsf{Vrfy}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Mac}_2, \mathsf{Vrfy}_2)$ be 2 MAC schemes. Construct a MAC scheme $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ as follows:

$\mathsf{Gen}(1^\lambda)$: return (k_1, k_2) where $k_1 \longleftarrow \mathsf{Gen}_1(1^\lambda)$ and $k_2 \longleftarrow \mathsf{Gen}_2(1^\lambda)$

$\mathsf{Mac}((k_1, k_2), m)$: return $t = (\mathsf{Mac}_1(k_1, m), \mathsf{Mac}_2(k_2, m))$

$\mathsf{Vrfy}((k_1, k_2), m, t = (t_1, t_2))$: return 1 if and only if $\mathsf{Vrfy}_1(k_1, m, t_1) = 1$ and $\mathsf{Vrfy}_2(k_2, m, t_2) = 1$

Prove or Disprove: Π is secure if either Π_1 is secure or Π_2 is secure.

QUESTION 3: Suppose that $h : \{0,1\}^{2n} \to \{0,1\}^n$ is a collision resistant hash function. Define a hash function $H : \{0,1\}^{4n} \to \{0,1\}^n$ as follows: write $x \in \{0,1\}^{4n}$ as $x = x_1||x_2$ with $x_1, x_2 \in \{0,1\}^{2n}$ and define

$$H(x) = h\left(h(x_1)||h(x_2)\right).$$

Prove or Disprove: H is collision-resistant.
