Cryptology: Problem Sheet 5

Topic: Hash Functions

1. A keyed hash function $\mathsf{H}_k : \{0,1\}^* \to \{0,1\}^n$ is said to be t-wise regular, if for any distinct $x_1, \ldots, x_t \in \{0,1\}^*$ and for any non-zero $y \in \{0,1\}^n$,

$$\Pr[\mathsf{H}_k(x_1) \oplus \ldots \oplus \mathsf{H}_k(x_t) = y] \leq \epsilon.$$

   Prove that the 3-wise regular advantage of Polyhash is at most $\ell/2^n$, where ℓ is the maximum number of message blocks.

2. Given an Almost XOR Universal (AXU) keyed hash function H and a PRF F, show that the construction

$$\mathsf{mWC}_{K_1,K_2}(M) := (F_{K_1}(N), H_{K_2}(M) \oplus N)$$

   is not a secure MAC, even if N is used as a nonce.

3. You are using the Wegman-Carter MAC in a protocol to authenticate messages of even number of blocks. Which of the following hash functions can you use in your MAC?

   (a) $H(k, m = (m_1 \| \cdots \| m_{2i})) := m_1 \cdot k^{2i} \oplus m_2 \cdot k^{2i-1} \oplus \cdots \oplus m_{2i} \cdot k.$

   (b) $H(k, m = (m_1 \| \cdots \| m_{2i})) := k^{2i+1} \oplus m_1 \cdot k^{2i} \oplus m_2 \cdot k^{2i-1} \oplus \cdots \oplus m_{2i} \cdot k.$

   (c) $H(k, m = (m_1 \| \cdots \| m_{2i})) := k^{i+1} \oplus (m_1 \oplus m_2) \cdot k^i \oplus \cdots \oplus (m_{2i-1} \oplus m_{2i}) \cdot k.$

4. Let $\mathsf{H1}$ and $\mathsf{H2}$ be two family of hash functions from $\{0,1\}^k \times \{0,1\}^*$ to $\{0,1\}^n$. Let k_1, k_2 be two hash keys sampled independently and uniformly from $\{0,1\}^k$. Then, we define a $2n$-bit hash function

$$\mathsf{H}_{(k_1,k_2)}(m) := \mathsf{H1}_{k_1}(m) \parallel \mathsf{H2}_{k_2}(m),$$

   where $m \in \{0,1\}^*$.

   (a) Show that if at least one of $\mathsf{H1}$ or $\mathsf{H2}$ is collision resistant, then H is collision resistant.

   (b) Determine whether an analogous claim holds for second preimage resistance and preimage resistance, respectively.

   (c) Let $\mathsf{F} : \{0,1\}^s \times \{0,1\}^{2n} \to \{0,1\}^n$ be a PRF that maps $2n$-bit string to an n-bit string. Derive an upper bound on the PRF advantage of the construction

$$F_S \circ \mathsf{H}_{(k_1,k_2)}(m),$$

   where K is sampled uniformly from $\{0,1\}^s$. Assume that both $\mathsf{H1}$ and $\mathsf{H2}$ are ϵ universal.