

**Department of Computer Science and Engineering,
National Sun Yat-sen University**

Second Semester of 2023 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (10 points) Please define formally the security of a message authentication code algorithm.

Problem 2: (10 points) Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem. Then $H(\mathbb{K}|\mathbb{C}) = H(\mathbb{K}) + H(\mathbb{P}) - H(\mathbb{C})$.

Problem 3: (10 points) Please describe how to prevent the man-in-the-middle attack against the Diffie-Hellman key exchange protocol.

Problem 4: (10 points) Please describe the definition of $H(X)$, $H(X, Y)$, and $H(X|Y)$ in detail.

Problem 5: (10 points) Prove that $H(X, Y) = H(Y) + H(X|Y)$. Then show as a corollary that $H(X|Y) \leq H(X)$, with equality if and only if X and Y are independent.

Problem 6: (15 points) Please define an identity-based signature scheme and its security formally.

Problem 7: (10 points) Please prove the security of RSA-based full-domain hash signature scheme formally.

Problem 8: (10 points) Please define anonymity (unlinkability) for mutual authentication formally.

Problem 9: (15 points) Please define an identity-based encryption scheme and its security for semantic security.

