

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

Second Semester of 2025 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (10 points) Please prove an encryption scheme is of perfect secrecy by information theory.

Problem 2: (10 points) Please describe the definition of $H(X)$, $H(X, Y)$, and $H(X|Y)$ in detail.

Problem 3: (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 4: (10 points) Please define formally the security of pseudorandom function.

Problem 5: (10 points) Please describe Chinese Remainder Theory (CRT) formally.

Problem 6: (15 points) Please prove the security of RSA-based full-domain hash signature scheme formally.

Problem 7: (15 points) Please define formally the ciphertext-only, chosen plaintext, and chosen ciphertext attacks, respectively.

Problem 8: (10 points) Please define formally the existential unforgeability against chosen message attacks for the security of digital signatures.

Problem 9: (10 points) Please define an identity-based encryption scheme and its security for semantic security.