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

First Semester of 2025 PhD Qualifying Exam

Subject: Cryptography

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

Problem 2: (10 points) Please describe how to calculate the redundancy rate of English language.

Problem 3: (10 points) Please describe Chinese Remainder Theory (CRT) formally.

Problem 4: (10 points) Please define formally the existential unforgeability against chosen message attacks for the security of digital signatures.

Problem 5: (10 points) Please define a group signature scheme with traceability formally.

Problem 6: (10 points) Please describe the definition of $H(X)$, $H(X,Y)$, and $H(X|Y)$ in detail.

Problem 7: (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 8: (15 points) Please define a certificateless signature scheme and its security formally.

Problem 9: (15 points) What are the differences between a certificateless signature scheme and an identity-based signature scheme?