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

First Semester of 2024 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (10 points) Please define formally a secure public-key encryption with indistinguishability under chosen ciphertext attacks (IND-CCA) .

Problem 2: (10 points) Please describe how to prevent the man-in-the-middle attack against the Diffie-Hellman key exchange protocol.

Problem 3: (10 points) Please describe the definition of $H(X)$, $H(X,Y)$, and $H(X|Y)$ in detail.

Problem 4: (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 5: (10 points) Please describe Chinese Remainder Theory (CRT) formally.

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

Problem 7: (10 points) Please define formally the existential unforgeability against chosen message attacks for the security of digital signatures.

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

Problem 9: (15 points) Please define formally the ciphertext-only, chosen plaintext, and chosen ciphertext attacks, respectively.