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

First Semester of 2023 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (10 points) Please define formally the security of pseudorandom permutation.

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

Problem 3: (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 4: (10 points) Please define unforgeability for digital signatures formally.

Problem 5: (10 points) Please describe the calculation of an inverse by the extended Euclidean algorithm formally.

Problem 6: (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 7: (10 points) What are the difference between ID-based signature and PKI-based signature schemes in security.

Problem 8: (15 points) Please prove the security of RSA-based full-domain hash signature scheme formally.

Problem 9: (15 points) Suppose there are three entities A, B, and C, and they are untrusted to each other. Moreover, A and C, and B and C, share common secret keys, K_{AC} and K_{BC}, respectively. Please design a three-party authenticated key exchange protocol to achieve mutual authentication and session key exchange between A and C.