Dept. of Computer Science and Engineering, National Sun Yat-sen Univ.

First Semester of 2022 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (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 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: (20 points) Please provide the security definitions of existential unforgeability against chosen message attacks and semantic security against chosen chiphertext attacks for a security scheme that achieves the confidentiality and non-repudiation protection simultaneously for an arbitrary message.

Problem 4: (20 points) Please design a user anonymous authenticated key exchange protocol for two entities, where both entities have to authenticate each other mutually and public-key cryptosystem is allowed to be utilized. (Notes: please also specify clearly what kind of security has to be achieved for the used cryptosystem in the proposed protocol.)

Problem 5: (10 points) Please describe what are ciphertext-only, known plaintext, chosen plaintext, and chosen ciphertext attacks.

Problem 6: (10 points) Please define the security of existential unforgeability for a generic digital signature scheme.

Problem 7: (20 points) Suppose there are three entities A, B, and C, where B and C are fully trusted, and the communication channel between them is secure. Moreover, A and C share a secret key, K. Please design a three-party authenticated key exchange protocol with forward secrecy with asymmetric and symmetric cryptographic algorithms. (Note: The security feature of mutual authentication, session key exchange, and forward secrecy should be achieved among A and B).