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

Second Semester of 2021 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (10 points) Please describe full domain hash formally.

Problem 2: (10 points) Please describe how a man-in-the-middle attack in Diffie-Hellman key agreement protocol is practiced and how to prevent from such attack. (Note: Need to describe the design of a protocol by using an existing cryptosystem 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 prove formally the extended Euclidean algorithm.

Problem 5: (10 points) Please define semantic security formally.

Problem 6: (10 points) Please define an identity-based encryption (IBE) formally. (Note: Please also state how the variables are selected when defining IBE.)

Problem 7: (15 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 8: (10 points) Please define the security of existential unforgeability for a generic digital signature scheme.

Problem 9: (15 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 using only symmetry-based encryption, cryptographic hash function, and Diffie-Hellman key agreement. (Note: The security feature of mutual authentication, session key exchange, and forward secrecy should be achieved among A and B).