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

First Semester of 2026 PhD Qualifying Exam

Subject: Cryptography | Full Points: 100 | Time: 3Hrs

Q1: (10 points)
Let (P, C, K, E, D) be a cryptosystem where P, C, and K are finite sets of possible plaintexts, ciphertexts, and keys, and E and D are respective the encryption and decryption rules. Does this equality $\boldsymbol{H(K|C) = H(K) + H(P) - H(C)}$ hold where H is an entropy function? Analyze your assertion formally.

Q2: (10 points)
Discuss the chosen ciphertext attack (CCA) in the textbook RSA version with a neat and clean diagram.

Q3: (10 points)
Define Chinese Remainder Theorem (CRT) and use it to find the unique solution $\boldsymbol{x}$ **(mod 105)** for a given set of equations:

$$x \equiv 5 \bmod 7$$
$$x \equiv 4 \bmod 5$$
$$x \equiv 1 \bmod 3$$

Q4: (6+4 points)
Define the security properties of a message authentication code (MAC). Compare and contrast MAC with a standard digital signature.

Q5: (7+3 points)
Let User A's private key be 7 and User B's private key be 11. Both parties have agreed to utilize the Diffie-Hellman key exchange method with a common prime of 29 and a generator of 3. What is the common secret key for A and B? Show that a Man-in-the-Middle Attack (MitMA) is possible during users A and B's communication.

Q6: (10 points)
What are the differences between a certificateless signature scheme and an identity-based signature scheme? Discuss it in detail with neat diagrams and their respective security models.

Q7: (10 points)
How does Existential Unforgeability under Chosen Message Attack (EUF-CMA) work? Discuss it in the context of an identity-based signature (IBS).

Q8: (8+7 points)
What does a "reduction" argument aim to achieve in a typical provable security analysis? Within a cryptographic proof that operates in the Random Oracle Model (ROM), describe the assumed behavior of the ideal hash function. How does an adversary interact with this "oracle"?

Q9: (5+10 points)
Provide a formal definition of attribute-based encryption (ABE) and demonstrate its IND-CCA security model in detail.