

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

**Second Semester of 2024 PhD Qualifying Exam**

**Subject: Cryptography**

**Full Points: 100**

**Time: 3Hrs**

---

**Q1: (3+7 points)**

Define random (R) and uniform random (UR) variables formally with suitable examples. Let  $Y$  be a random variable over  $\{0,1\}^n$  and  $X$  be an independent uniform variable on  $\{0,1\}^n$ . Show that  $Z = X \oplus Y$  is a uniform variable over  $\{0,1\}^n$ .

**Q2: (2.5x4 points)**

List and demonstrate four elementary attacks on textbook-RSA.

**Q3: (7+3 points)**

Define the security properties of a message authentication code (MAC). Compare and contrast MAC with standard digital signature.

**Q4: (6+4 points)**

Discuss formally the terms perfect forward secrecy (FS) and backward secrecy (BS) in Diffie-Hellman-like key exchange protocol. What are the fundamental requirements of a protocol to support these traits?

**Q5: (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 encryption decryption rules. Does this equality  $H(K|C) = H(K) + H(P) - H(C)$  hold where  $H$  is an entropy function? Analyze your assertion formally.

**Q6: (9+6 points)**

Appropriately define the notion of the group signature. Does the group signature provide the same functionalities as the ring signature? Justify your claim.

**Q7: (15 points)**

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

**Q8: (10 points)**

Provide a formal definition of attribute-based encryption (ABE) that clarifies how the security parameters are chosen.

**Q9: (10 points)**

How can cryptography be employed to guarantee user privacy in end-to-end communication? Provide an appropriate illustration.