

# Quiz of CS549 Cryptography and Network Security

ASSIGNED: JAN. 18TH, 2006 SPRING 2006, CS DEPARTMENT, IIT

YOUR NAME \_\_\_\_\_

1. What is the time complexity needed to sort  $n$  numbers by using only *comparisons*? Here we assume that we can decide in one time-unit which number is larger among two numbers.

2. Order the following functions according to their order of growth from the lowest to the highest. If you think that two functions are of the same order (i.e  $f(n) = \Omega(g(n))$ ). Then put them in the same group.

$$n^3 - n^2, \log(n^2), \log n, 2^n, n!, 1000n^2, 100^n,$$

3. What are the values of following formulas?  $(-3) \cdot 7 \pmod{8}$ ; and  $3^{2005} \pmod{2006}$ .

4. What is the best method known by you to test whether a number  $p$  is a prime number or not?

5. Circle the following terminologies you knew previously? Out of these 20 terminologies, how many do you know? \_\_\_\_\_.

private-key, public-key, DES, RSA, SHA1, MD5, digital signature, zero-knowledge proof, bit-commitment, one-time password, digital cash, AES, ElGamal, pseudo-prime-number, pseudo-random-number, Euler Theorem, Little Fermat Theorem, Chinese Remainder Theorem, birthday paradox, entropy.

6. How to compute the number  $12345^{23456789} \pmod{101}$  efficiently?