Indian Institute of Technology, Kharagpur

Date...................... Time: 60 mins Full Marks: 25
Second Class Test (Autumn) Semester 2020-21 No. of Students: 56
Sub. No. MA 61027 Subject Name: Cryptography and Network Security

Instruction: The test is in open-book, open-notes mode. Answer all questions. No marks will be awarded without proper justification. Notations used are as explained in the class.

1. [**4 mark**] We consider the RSA encryption. Write each answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.

   (i) To illustrate the RSA system, we use primes $p = 23$ and $q = 17$. As public encryption key we use $e = 3$. Compute the decryption key d. Show your computation.

   (ii) Describe in detail how the ciphertext $C = 165$ is decrypted. You must show that you understand how the algorithm for efficient modular exponentiation works.

2. [**4 mark**] Let p be an odd prime. Describe briefly with justification how to compute the following using the square and multiply algorithm to compute modular exponentiations:

   (i) The multiplicative inverse of an element in Z_p^*.

   (ii) The square root of a quadratic residue in Z_p^*, where $p \equiv 3 \pmod 4$.

3. [**2 mark**] Find all square roots (if they exist) of $\sqrt{100} \pmod{209}$.

4. [**2 mark**] Let $k \geq 1$ be such that $p = 6k+1$, $q = 12k+1$, and $r = 18k+1$ are primes. Show that $n = pqr$ is a Carmichael number.

5. [**2 mark**] If p is an odd prime, show that

$$\sum_{a=1}^{p-2} \left(\frac{a(a+1)}{p} \right) = -1.$$

6. [**2 mark**] Compute the following order, if exists: $\mathsf{ord}_{n^2}(g)$ where $g = (n+1)^t$ and t is a positive integer.

7. [**2 mark**] Compute $\left(\frac{1801}{8191}\right)$ without factoring any odd integer.

8. [**2 mark**] Alice wants to securely send m to Bob. She selects p, a prime $> m$ and integer a relatively prime to $p-1$. She sends $c = m^a \bmod p$ and p to Bob over an insecure channel. Bob selects an integer b that is relatively prime to $p-1$, computes $d = c^b \bmod p$ and sends d to Alice. Alice finds g such that $ag = 1 \bmod p-1$. She then computes $e = d^g \bmod p$ and sends e to Bob. Explain what Bob must do to obtain m.

9. [**5 mark**]

   (a) How many primitive roots does $n = 334$ have?

   (b) What is the smallest primitive root mod 334?

   (c) How many integers mod 334 have order equal to 2? If such elements exist, find one.

——-The End———