VIT-AP
UNIVERSITY

Programme: MTSE Semester: Winter 2020-21

Subject: Information and System Security Subject Code: SWE3003

ASSIGNMENT-2

Points (Weightage): 20 (8%) **Submission Due Date: 15-May-2021**

[**Note**: You may use computer programs to solve. But show detailed steps of the solutions.]

1) Use the Fermat’s method to find the factors of 127.

2) The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

3) Show that if n is an odd composite integer, then the Miller-Rabin test will return inconclusive for a = 1 and a = (n-1).

4) If ***n*** is composite and passes the Miller-Rabin test for the base ***a***, then ***n*** is called a strong pseudoprime to the base ***a***. Show that 2047 is a strong pseudoprime to the base 2.

5) Using Fermat's theorem,

   a) Find 3^{201} mod 11.

   b) Find a number ***n*** between 0 and 72 with ***n*** congruent to 9^{794} modulo 73.

   c) Find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29. (You should not need to use any brute force searching.)

6) Using Euler's Theorem

   a) Find a number ***n*** between 0 and 9 such that ***n*** is congruent to 7^{1000} modulo 10.

b) Find a number x between 0 and 28 with x^{85} congruent to 6 modulo 35. (You should not need to use any brute force searching.)

7) Determine the following:

a) $\phi(41)$ b) ϕ (27)   c) ϕ (231)   d) ϕ (440)

8) A box contains gold coins. If the coins are equally divided among six friends, four coins are left over. If the coins are equally divided among five friends, three coins are left over. If the box holds the smallest number of coins that meets these two conditions, how many coins are left when equally divided among seven friends?

9) Find the smallest positive integer that is one more than a multiple of 5, 2 more than a multiple of 11 and 3 more than a multiple of 7.

10) How many primitive roots does 25 have? Find them all.

11) Perform encryption and decryption using the RSA algorithm, if p = 397; q = 401, e = 343; Plaintext M = “NO”. [Coding: A=0, B=1, …, Z=25]

12) Perform Rabin Cryptosystem (The example from the slide) and solve the problem showing the detailed steps.

13) Perform RSA-based digital signature scheme (key generation, signing, and verifying) where p = 167, q=113, e=201, and the message M=”hi”. [Coding: A=0, B=1, …, Z=25]

14) Perform ElGamal-based digital signature scheme (key generation, signing, and verifying) where p = 3119, e_1=2, d=127, r=307, and the message M=320.

15) Alice and Bob use Diffie-Hellman Key Agreement protocol to agree upon a secret key. They select p=331, g=97, x=53 and y=67. Find the secret key.

---$---