Quiz-3
Cryptography and Network Security

[Total marks - 20]

[**Instructions**: Please upload your answers in Microsoft Teams by **19/10/2020**. Your **Roll No.** and **Name** must be mentioned. No marks will be awarded without detailed solution.]

1. [4 **mark**] Perform the modular exponentiation $17^{1236} \pmod{47}$ using

   (a) **Fast Modular Exponentiation**,

   (b) **Fermat's little theorem**.

   (Write your answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.)

2. [2 **mark**] Use **Euler's theorem** to compute the modular exponentiation $2^{22970} \pmod{25}$.
   (Write your answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.)

3. [3 **mark**] Compute each of the following orders, if they exist:

   (a) $\mathsf{ord}_{11}(3)$,

   (b) $\mathsf{ord}_{21}(6)$,

   (c) $\mathsf{ord}_{304}(21)$.

4. [5 **mark**] For $n = 81$, do the following:

   (a) Determine whether there are any primitive roots mod $n = 81$; if so, how many will there be?

   (b) If there are primitive roots mod $n = 81$, find the smallest one.

(c) If there are primitive roots, use the one you found in (b) to construct another.

5. [**2 mark**]

   (a) Use the **prime number theorem** to estimate the number of 1000-bit primes. This will be the number of primes between 2^{999} and 2^{1000}.

   (b) If we randomly pick a 1000-bit odd integer, estimate the probability that it will be prime.

6. [**4 mark**] Find all solutions for each of the following congruences (use **extended Euclidean algorithm**):

   (a) $6x \equiv 28 \pmod{776}$,

   (b) $15x \equiv 21 \pmod{1940}$.

——-The End———