Assignment III

Cryptography and Network Security (CSE324)

1a. What are the applications of random numbers?

b. State and prove Fermat's theorem. Using Fermat's theorem find 3^{201} mod 11.

2a. What are the requirements for a sequence of numbers to be pseudorandom?

b. Give an example and explain the working of Blum Blum Shub Generator.

3a. State and prove Euler's theorem. Find ø(35), ø(256) using Euler's totient function.

b. Explain pseudorandom number generation using triple DES.

4a. Draw neat diagrams of random and pseudorandom number generators and explain.

b. Explain Linear Congruential Generator. What is its limitation and how can it be overcome?

5a. Describe RC4 algorithm.

b. Given x≡ 2(mod 3) , x≡ 3(mod 5) , x ≡ 2(mod 7) solve for x using Chinese remainder theorem.

6a. Find any one primitive root of 9.
b. Write the Miller- Rabin algorithm and explain with an example.