Assignment 01

Instructor: Mehrdad Nojoumian
Course: Secret Sharing Protocols

Deadline: Feb 14

(1) Which one is a primitive root of 7?

a) 3

b) 5

c) 2

(2) Find an inverse of “23” modulo “120”. Also solve the following congruent equation 23x ≡ 3 (mod 120) for x. Use the Euclid’s Algorithm and the Extended Euclid’s Algorithm.

(3) Use the Fermat's little theorem to find: $3^{52} \left(mod \quad 11 \right)$.

(4) What are the prime factorizations of “48” and “60”? Also, find GCD(48, 60) and LCM(48, 60).

(5) What is the decimal expansion of $\left(1\mathrm{B}6\right)_{16}$? What is the Hexadecimal expansion of “485”?

(6) What sequences of pseudorandom numbers is generated using the linear congruential generator x_{n+1} = (4_{xn}+1) mod 7 with seed x_0 = 3?

(7) The validity of an ISBN can be evaluated as explained in the class.

- If the first 9 digits are “987654321”, what is the check digit x_{10}?
- Is “9753842601” (where x_1=9 & x_{10}=1) a valid ISBN number?

(8) Trace the Miller-Rabin probabilistic primality-test algorithm for a prime as well as a composite number. Provide details with respect to your tracing.