**Initial Test**

**Instructor: Mehrdad Nojoumian**

**CIS 5371: Practical Aspects of Modern Cryptography**

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

Definition: a primitive root modulo a prime **p** is an integer **r** in Zp such that every nonzero element of Zp is a power of **r**.

a) 3

b) 5

c) 2

**(2)** Find an inverse of “23” modulo “120”. Subsequently, Solve the congruent equation 23x ≡ 3 (mod 120) for “x”. (Hint: Use Euclid’s Algorithm & Extended Euclid’s Algorithm)

Definition: an integer **ā** such that āa ≡ 1 (mod m) is said to be an inverse of **a** modulo **m**.

**(3)** Use the Fermat's little theorem to find: .

Theorem: ap-1 ≡ 1 (mod p)

**(4)** What are the prime factorizations of “48” and “60”?

**(5)** Find GCD(48, 60) and LCM(48, 60).

**(6)** What is the decimal expansion of ? What is the Hexadecimal expansion of “485”?

**(7)** What sequences of pseudorandom numbers is generated using the linear congruential generator xn+1 = (4xn+1) mod 7 with seed x0 = 3?