Cryptography and Network Security I
HW 2 Theory Part a.
Due October 9, 2018

1- Prove that
a) $a \equiv b \pmod n$ implies $b \equiv a \pmod n$
b) prove that $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$

2- Using extended Euclidean algorithm find the multiplicative inverse of
a) 1234 mod 4321
b) 24140 mod 40902
c) 550 mod 1769

3- Determine which of the following are reducible over GF(2)
a) $x^3 + 1$
b) $x^3 + x^2 + 1$
c) $x^4 + 1$

4- Determine the GCD of following pair of polynomials:
a) $x^3 - x + 1$ and $x^2 + 1$ over GF(2)
b) $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)

5- For a cryptosystem {P,K,C,E,D} where
P={a,b,c} with
PP(a)=1/4
PP(b)=1/4
PP(c)=1/2

K = (k1,k2,k3) with
P*K*(k1)=1/2
P*K*(k2)=1/4
P*K*(k3)=1/4

C = { 1,2,3,4}

Encryption table

Ek(P)	a	b	c
k1	1	2	1
k2	2	3	1
k3	3	2	4
k4	3	4	4

Calculate H(*K*|C)