Glenn Smith
Crypto Hw 2.a

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 $a \equiv c \pmod{n}$

a.
Definition of $a \equiv b \bmod n$:
$a = xn + A$
$b = yn + B$
$A = B$
Since $(A = B) \rightarrow (B = A)$ then we could flip the two sides and say $b \equiv a \bmod n$

b.
$a \equiv b \bmod n$
$a = xn + A$
$b = yn + B$
$A = B$
$b \equiv c \bmod n$
$c = zn + C$
$B = C$
$A = B, B = C \rightarrow A = C$
$A = C \rightarrow a \equiv c \bmod n$

2- Using extended Euclidean algorithm find the multiplicative inverse of
a) 1234 mod 4321
$n = 4321$, $m = 1234$, $vn = (1, 0)$, $vm = (0, 1)$
$q = 3$, $n' = 619$, $vn' = (1, -3)$
$q = 1$, $m' = 615$, $vm' = (-1, 4)$
$q = 1$, $n' = 4$, $vn' = (2, -7)$
$q = 153$, $m' = 3$, $vm' = (-307, 1075)$
$q = 1$, $n' = 1$, $vn' = (309, -1082)$,
$q = 3$, $m' = 0$, $vm' = (1234, -4321)$
Inverse is $-1082 \equiv 3239 \bmod 4321$

b) 24140 mod 40902
These are not coprime, so they don't have a multiplicative inverse

c) 550 mod 1769
$n = 1769$, $m = 550$, $vn = (1, 0)$, $vm = (0, 1)$
$q = 3$, $n' = 113$, $vn' = (1, -3)$
$q = 4$, $m' = 98$, $vm' = (-4, 13)$

q = 1, n’ = 15, vn’ = (5, -16)
q = 6, m’ = 8, vm’ = (-34, 109)
q = 1, n’ = 7, vn’ = (39, -125)
q = 1, m’ = 1, vm’ = (-73, 234)
q = 7, n’ = 0, vn’ = (550, -1763)
550 is its own inverse

3- Determine which of the following are reducible over GF(2)
GF(2^1)
a) x^3 + 1
(x+1)(x^2 + x + 1) = x^3 + 2x^2 + 2x + 1 ≡ x^3 + 1
Reducible

b) x^3 + x^2 + 1
Irreducible

c) x^4 + 1
(x^2 + 1)(x^2 + 1) = x^4 + 2x^2 + 1 ≡ x^4 + 1 mod 2
Reducible

4- Determine the GCD of following pair of polynomials:
a) x^3 – x + 1 and x^2 +1 over GF(2)
 x^3 - x + 1
-(x^3 + x)
= -2x+1 ≡ 1 mod 2
So the GCD is 1
b) x^5 + x^4 +x^3 – x^2 – x +1 and x^3 + x^2 + x +1 over GF(3)
 x^5 + x^4 + x^3 - x^2 - x + 1
+2x^5 + 2x^4 + 2x^3 + 2x^2
3x^5 + 3x^4 + 3x^3 + x^2 - x +1 ≡ x^2 - x + 1 mod 3
x^3 + x^2 + x + 1 - x^3 + x^2 - x = 2x^2 + 1
2x^2 + 1 - 2x^2 + 2x - 2 = 2x - 1
x^2 - x + 1 - 4x^2 + 2x ≡ x + 1 mod 3
2x - 1 - 2x - 2 ≡ 0 mod 3
So the GCD is x + 1

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
PK(k1)=1/2
PK(k2)=1/4
PK(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

PrC(1) = 1/8+1/4+1/8 = 1/2
PrC(2) = 1/16+1/8+1/16 = 1/4
PrC(3) = 1/16+1/16+0 = 1/8
PrC(4) = 1/8+0+0 = 1/8

H(K|C) = -∑Pr(c) Pr(k|c) log2(Pr(k|c))
Pr(k|c) = Pr(c|k)Pr(k) / Pr(c)

Pr(k4) = 0 so just ignore it

Pr(1|k1) = Pr(a) + Pr(c) = 3/4
Pr(2|k1) = Pr(b) = 1/4
Pr(3|k1) = 0
Pr(4|k1) = 0
Pr(1|k2) = Pr(c) = 1/2
Pr(2|k2) = Pr(a) = 1/4
Pr(3|k2) = Pr(b) = 1/4
Pr(4|k2) = 0
Pr(1|k3) = 0
Pr(2|k3) = Pr(b) = 1/4
Pr(3|k3) = Pr(a) = 1/4
Pr(4|k3) = Pr(c) = 1/2

Pr(k1|1) = Pr(1|k1) Pr(k1) / Pr(1) = (3/4) (1/2) / (1/2) = 3/4
Pr(k1|2) = Pr(2|k1) Pr(k1) / Pr(2) = (1/4) (1/2) / (1/4) = 1/2

$Pr(k1|3) = Pr(3|k1)\ Pr(k1) / Pr(3) = (0)\ (1/2) / (1/8) = 0$
$Pr(k1|4) = Pr(4|k1)\ Pr(k1) / Pr(4) = (0)\ (1/2) / (1/8) = 0$
$Pr(k2|1) = Pr(1|k2)\ Pr(k2) / Pr(1) = (1/2)\ (1/4) / (1/2) = 1/4$
$Pr(k2|2) = Pr(2|k2)\ Pr(k2) / Pr(2) = (1/4)\ (1/4) / (1/4) = 1/4$
$Pr(k2|3) = Pr(3|k2)\ Pr(k2) / Pr(3) = (1/4)\ (1/4) / (1/8) = 1/2$
$Pr(k2|4) = Pr(4|k2)\ Pr(k2) / Pr(4) = (0)\ (1/4) / (1/8) = 0$
$Pr(k3|1) = Pr(1|k3)\ Pr(k3) / Pr(1) = (0)\ (1/4) / (1/2) = 0$
$Pr(k3|2) = Pr(2|k3)\ Pr(k3) / Pr(2) = (1/4)\ (1/4) / (1/4) = 1/4$
$Pr(k3|3) = Pr(3|k3)\ Pr(k3) / Pr(3) = (1/4)\ (1/4) / (1/8) = 1/2$
$Pr(k3|4) = Pr(4|k3)\ Pr(k3) / Pr(4) = (1/2)\ (1/4) / (1/8) = 1$

$H(K|C) = -\sum Pr(c)\ Pr(k|c)\ \log 2(Pr(k|c))$
$-(Pr(1)(Pr(k1|1)\log 2\ Pr(k1|1)+Pr(k2|1)\log 2\ Pr(k2|1)+Pr(k3|1)\log 2\ Pr(k3|1))$
$+Pr(2)(Pr(k1|2)\log 2\ Pr(k1|2)+Pr(k2|2)\log 2\ Pr(k2|2)+Pr(k3|2)\log 2\ Pr(k3|2))$
$+Pr(3)(Pr(k1|3)\log 2\ Pr(k1|3)+Pr(k2|3)\log 2\ Pr(k2|3)+Pr(k3|3)\log 2\ Pr(k3|3))$
$+Pr(4)(Pr(k1|4)\log 2\ Pr(k1|4)+Pr(k2|4)\log 2\ Pr(k2|4)+Pr(k3|4)\log 2\ Pr(k3|4)))$

$-((1/2)((3/4)\log 2\ (3/4)+(1/4)\log 2\ (1/4))$
$+(1/4)((1/2)\log 2\ (1/2)+(1/4)\log 2\ (1/4)+(1/4)\log 2\ (1/4))$
$+(1/8)((1/2)\log 2\ (1/2)+(1/2)\log 2\ (1/2))$
$+(1/8)((1)\log 2\ (1)))$

$= 0.906$