Ryan Stillings

Cryptography and Network Security I

HW2 Theory Part a

1. Prove that:

a) a ≡ b(mod n) implies b ≡ a(mod n)

If a ≡ b mod n then n|(b - a). n|(b - a) implies n|(-1)(b - a) which is equivalent to n|(a - b). Therefore, b ≡ a mod n.

b) a ≡ b(mod n) and b ≡ c(mod n) imply a ≡ c (mod n)

If a ≡ b mod n and b ≡ c mod n then n|(b - a) and n|(c - b). Because the sum of two numbers with a common divisor will share that divisor, we can write n|(b - a + c - b) which is equivalent to n|(c - a). Therefore, a ≡ c mod n.

2. Find multiplicative inverse of:

a) 1234 mod 4321

t	r
0	4321
1	1234
-3	619
4	615
-7	4
1075	3
-1082	1
-1082 + 4321 = **3239**	0

b) 24140 mod 40902

t	r
0	40902
1	24140
-1	16762
2	7378
-5	2006
17	1360
-22	646
61	68
-571	34
no inverse found	0

c) 550 mod 1769

t	r
0	1769
1	550
-3	119

13	74
-16	45
29	29
-45	16
74	13
-119	3
550	1
550	0

3. Determine which are reducible over GF(2):
   a) $x^3+1 = (x+1)(x^2+x+1)$
   b) $x^3 + x^2 + 1$ = not reducible
   c) $x^4+1 = (x+1)^4$

4. determine GCD:
   a) $x^3 - x + 1$ and $x^2 + 1$ over GF(2) = 1 mod 2
   b) $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3) = $x + 1$ (mod 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
   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

Calculate H(K|C):

$\Pr(1) = \frac{1}{2}$

$\Pr(2) = \frac{1}{4}$

$\Pr(3) = \frac{1}{8}$

$\Pr(4) = \frac{1}{8}$

Pr(k|C)	=
Pr(k1|1)	¾
Pr(k1|2)	½
Pr(k1|3)	0
Pr(k1|4)	0
Pr(k2|1)	¼
Pr(k2|2)	¼
Pr(k2|3)	¼
Pr(k2|4)	0
Pr(k3|1)	0
Pr(k3|2)	¼
Pr(k3|3)	¼
Pr(k3|4)	¼
Pr(k4|1)	0
Pr(k4|2)	0
Pr(k4|3)	½
Pr(k4|4)	¾

$-(\frac{1}{2}(\frac{3}{4}\log_2\frac{3}{4}+\frac{1}{4}\log_2\frac{1}{4}+0\log_2 0)+\frac{1}{4}(\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{4}\log_2\frac{1}{4})+\frac{1}{8}(0\log_2 0+\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{2}\log_2\frac{1}{2}))=\frac{3log3}{8log2}-\frac{3}{2}=0.9056$