Isaac Llewellyn
661582062

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

A:
b mod n ≡ A implies that A is congruent to (N-B)
implies that nl(a-b); that is, if b is congruent to a mod N, then their difference is a multiple of N.
We can then see that -1*

1- Prove that

a) a ≡ b(mod n) implies b ≡ a(mod n)

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

B:
a ≡ b mod n and b ≡ c mod n imply: nl(a-b), nl(b-a), nl(b-c), nl(c-b)
From this we can combine nl(a-b) and nl(b-c) to nl(a-b+b-c)
In this, the b's cancel yielding nl(a-c) which implies a ≡ c mod n

2- Using extended Euclidean algorithm find the multiplicative inverse of

a) 1234 mod 4321

b) 24140 mod 40902

c) 550 mod 1769

A;
First find the GCF of the two numbers 1234 and 4321
4321 = 1234 * 3 + 619
1234 = 619 * 1 + 615
619 = 615 * 1 + 4.
615 = 4 * 153 + 3
4 = 3 * 1 + 1
1 = 4 - 3
GCF = 1. Therefore an inverse exists.
We recursively calculate to find the inverse
p0 = 0, p1 = 1
0 - 1*3 mod 4321 = 4318
1 - 1* 4318 mod 4321 = 4
4318 - 1* 4 mod 4321 = 3414
4 - 1*4314*153 mod 4321 = 1075
4314 - 1075*1 mod 4321 = 3239
The multiplicative inverse is 3239

B:
First find the GCF of the two numbers 24140 and 40902

40902 = 24140 * 1 + 16762
24140 = 16762 * 1 + 7378
16762 = 7378 * 2 + 2006
7378 = 2006 * 3 + 1360
2006 = 1360 * 1 + 646
1360 = 646 * 2 + 68
646 = 68 * 9 + 34
68 = 34 * 2 + 0 — As no 1 exists, no inverse exists.

C:
First find the GCF of the two numbers 550 and 1769

1769 = 550 * 3 + 119
550 = 119 * 4 + 74
119 = 74 * 1 + 45
74.= 45 * 1 + 29
45 = 29 * 1 + 16
29 = 16 * 1 + 13
16 = 13 * 1 + 3
13 = 3 * 4 + 1
3 = 3 + 0
Therefore an inverse exists.

We recursively calculate to solve for the inverse

p0 = 0, p1 = 1
0 - 1*3 mod 1769 = 1766
1 - 1*1776*4 mod 1769 = 13
1766 - 13*1 mod 1769 = 1753
13 - 1753*1 mod 1769 = 29
1753 - 29*1 mod 1769 = 1224
29 - 1224*1 mod 1769 = 74
1224 - 74*1 mod 1769 = 1650
74 - 1650*4 mod 1769 = 550

The multiplicative inverse is 550

3- Determine which of the following are reducible over GF(2)

a) $x^3 + 1$

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

c) $x^4 + 1$

GF(2) = max 'x' power of 2
A: (x+1)(x^2-x+1)
b:no
c:(x+1)^4

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)

A:
x2 + 1 / (x3 - x + 1 )
1*x= x3 + x, (x3 - x + 1) - (x3 + x ) = -2x - 10

-2x - 10 / (x2 + 1)
-2mod2 = 0, As they can not be multiplied into each other fully, the GCD is 1

B:
x3 + x2 + x + 1 / x5 + x4 + x3 - x2 - x + 1
1*x2 = x5 + x4 + x3 + x2, (x5 + x4 + x3 - x2 - x + 1) - (x5 + x4 + x3 + x2) = - x + 1
(-x + 1) / ( x3 + x2 + x + 1 )
1*-x2 = x3 - x2, ( x3 + x2 + x + 1 ) - ( x3 - x2 ) = 2x2 + x + 1
1*-2x = 2x2 - x, (2x2 + x + 1 ) - (2x2 - 2x ) = -x + 1
1*1 = -x + 1, (-x +1) - (-x + 1) = 0. GCD = -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
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)

**H(KIC) = H(K) + H(P) - H(C)**

**H(K) = -( 1/2 * log2(1/2) + 1/4 * log2*(1/4) + 1/4 * log2*(1/4) ) = 1.5**
**H(P) = -( 1/4 * log2*(1/4) + 1/4 * log2*(1/4)+ 1/2 * log2(1/2) ) = 1.5**
**H(C) =**
**Probability that 1 comes: 1/2*1/4+1/2*1/2 + 1/4*1/2 = 1/2**
**Probability that 2 comes: 1/2*1/4 + 1/4*1/4 + 1/4*1/2 = 1/4**
**Probability that 3 comes: 1/4*1/4 + 1/4*1/4 = 1/8**
**Probability that 4 comes: 1/4*1/2 = 1/8**
**H(C) = -( 1/2log2(1/2) + 1/4log2(1/4) + 1/8log2(1/8)+1/8log2(1/8) ) = 1.75**
**H(KIC) = H(K) + H(P) - H(C) = 1.5 + 1.5 - 1.75 = 1.25**