

Cryptography and Network Security I

HW 2 Theory Part a.

Due October 9, 2018

A:

$b \bmod n = a$ implies that b is congruent to $a \bmod n$

First we see that $b \bmod n$ implies that $n|(a-b)$; that is, if b is congruent to $a \bmod N$, then their difference is a multiple of N .

We can then see that $-1*n(a-b) = n(b-a)$, showing that $a \bmod n$ would also be congruent to $b \bmod n$.

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 $a \equiv c \pmod{n}$

B:

$a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply: $n|(a-b)$, $n|(b-a)$, $n|(b-c)$, $n|(c-b)$

From this we can combine $n|(a-b)$ and $n|(b-c)$ to $n|(a-b+b-c)$

In this, the b 's cancel yielding $n|(a-c)$ which implies $a \equiv c \pmod{n}$

2- Using extended Euclidean algorithm find the multiplicative inverse of

a) $1234 \bmod 4321 \equiv 1$

b) $24140 \bmod 40902$

c) $550 \bmod 1769$. Therefore an inverse exists^{D:}

We recursively calculate to find the inverse

$p_0 = 0, p_1 = 1$

$0 - 1 * 3 \bmod 4321 = 4318$

$1 - 1 * 4318 \bmod 4321 = 4$

$4318 - 1 * 4 \bmod 4321 = 3414$

$4 - 1 * 4314 * 153 \bmod 4321 = 1075$

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

a) $x^3 + 1$ The multiplicative inverse is 3239

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:

$x^2 + 1 / (x^3 - x + 1)$

$1*x = x^3 + x, (x^3 - x + 1) - (x^3 + x) = -2x - 10$

$-2x - 10 / (x^2 + 1)$

$-2\text{mod}2 = 0$, As they can not be multiplied into each other fully, the GCD is 1

B:

$x^3 + x^2 + x + 1 / x^5 + x^4 + x^3 - x^2 - x + 1$

$1*x^2 = x^5 + x^4 + x^3 + x^2, (x^5 + x^4 + x^3 - x^2 - x + 1) - (x^5 + x^4 + x^3 + x^2) = -x + 1$

$(-x + 1) / (x^3 + x^2 + x + 1)$

$1*x^2 = x^3 - x^2, (x^3 + x^2 + x + 1) - (x^3 - x^2) = 2x^2 + x + 1$

$1*x^2 = 2x^2 - x, (2x^2 + x + 1) - (2x^2 - x) = -x + 1$

$1*x^1 = -x + 1, (-x + 1) - (-x + 1) = 0$. GCD = $-x + 1$

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

$p_0 = 0, p_1 = 1$

$0 - 1 * 3 \bmod 1769 = 1766$

$1 - 1 * 1766 * 4 \bmod 1769 = 13$

$1766 - 13 * 1 \bmod 1769 = 1753$

$13 - 1753 * 1 \bmod 1769 = 29$

$1753 - 29 * 1 \bmod 1769 = 1224$

$29 - 1224 * 1 \bmod 1769 = 74$

$1224 - 74 * 1 \bmod 1769 = 1650$

$74 - 1650 * 4 \bmod 1769 = 550$

The multiplicative inverse is 550

5- For a cryptosystem $\{P, K, C, E, D\}$ where

$P = \{a, b, c\}$ with

$$PP(a) = 1/4$$

$$PP(b) = 1/4$$

$$PP(c) = 1/2$$

$K = (k_1, k_2, k_3)$ with

$$PK(k_1) = 1/2$$

$$PK(k_2) = 1/4$$

$$PK(k_3) = 1/4$$

$$C = \{1, 2, 3, 4\}$$

Encryption table

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

Calculate $H(K|C)$