Crypto HW1.2

Todd Louison

September 2018

Q1.

a) Prove that a $\equiv$ b(mod n) implies b$\equiv$a(mod n)

$$\begin{aligned} a \equiv b(\text{mod n}) &\implies n \mid (b-a) \\ &\therefore n \mid (-1)(b-a) \\ &= n \mid (a-b) \\ &\therefore b \equiv a(\text{mod n}) \end{aligned}$$

b) Prove that a$\equiv$b(mod n) and b$\equiv$c(mod n) imply a$\equiv$c (mod n)

$$\begin{aligned} a \equiv b(\text{mod n}) &\implies n \mid (b-a) \\ b \equiv c(\text{mod n}) &\implies n \mid (c-b) \\ \text{Using linear combination} &= n \mid (b-a+c-b) \\ &= n \mid (a+c) \\ &\therefore a \equiv c(\text{mod n}) \end{aligned}$$

Q2.

Using extended Euclidean algorithm find the multiplicative inverse of
a) 1234 mod 4321

$$\begin{aligned}
4321 - 3(1234) &= 619 \\
1234 - 1(619) &= 615 \\
619 - 1(615) &= 4 \\
615 - 153(4) &= 3 \\
4 - 1(3) &= 1
\end{aligned}$$

$$\begin{aligned}
1 &= 4 - 1(3) \\
1 &= 4(615 - 4(153)) \\
1 &= 4(154) - 615 \\
1 &= (619 - 615)(154) - 615 \\
1 &= (619)(154) - 615(155) \\
1 &= (619)(154) - (1234 - 619)(155) \\
1 &= (619)(154) - (1234)(155) + 155(619) \\
1 &= (309)(619) - 155(1234) \\
1 &= (309)(4321 - 3(1234)) - 155(1234) \\
1 &= (309)(4321) - 927(1234) - 155(1234) \\
1 &= 309(4321) - 1082(1234)
\end{aligned}$$

$\therefore$ the multiplicative inverse is -1082

b) 24140 mod 40902

$$\begin{aligned}
40902 - 1(24140) &= 16762 \\
21410 - 1(16762) &= 7378 \\
16762 - 2(7378) &= 2006 \\
7378 - 3(2006) &= 1360 \\
2006 - 1(1306) &= 646 \\
1360 - 2(646) &= 68 \\
646 - 9(68) &= 34 \\
68 - 2(34) &= 0
\end{aligned}$$

Since the GCD is not 1, this has no multiplicative inverse.

c) 550 mod 1769

$$
\begin{aligned}
1769 - 3(550) &= 119 \\
550 - 4(119) &= 74 \\
119 - 1(74) &= 45 \\
74 - 1(45) &= 29 \\
45 - 1(29) &= 16 \\
29 - 1(16) &= 13 \\
16 - 1(13) &= 3 \\
13 - 4(3) &= 1 \\
1 &= 13 - 4(3) \\
1 &= 13 - 4(16 - 13) \\
1 &= 5(13) - 4(16) \\
1 &= 5(29 - 16) - 4(16) \\
1 &= 5(29) - 5(16) - 4(16) \\
1 &= 5(29) - 9(16) \\
1 &= 5(29) - 9(45 - 29) \\
1 &= 5(29) - 9(45) + 9(29) \\
1 &= 14(29) - 9(45) \\
1 &= 14(74 - 45) - 9(45) \\
1 &= 14(74) - 14(45) - 9(45) \\
1 &= 14(74) - 23(45) \\
1 &= 14(74) - 23(119 - 74) \\
1 &= 14(74) - 23(119) + 23(74) \\
1 &= 37(74) - 23(119) \\
1 &= 37(550 - 4(119)) - 23(119) \\
1 &= 37(550) - 148(119) - 23(119) \\
1 &= 37(550) - 171(119) \\
1 &= 37(550) - 171(1769 - 3(550)) \\
1 &= 37(550) - 171(1769) + 513(550) \\
1 &= 550(550) - 171(1769)
\end{aligned}
$$

$\therefore$ the multiplicative inverse is 550.

Q3.

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

a) $x^3 + 1$
In GF(2) we try to substitute in 0 and 1:
f(0) $= 0^3 + 1 = 1$ **X**
f(1) $= 1^3 + 1 = 2$ which in GF(2) $= 0$ ✓

GF(2) = (x+1)$(x^2 + x + 1)$, so this is **reducible**.

b) $x^3 + x^2 + 1$
Attempt the same substitution:
f(0) $= 0^3 + 0^2 + 1 = 1$ **X**
f(1) $= 1^3 + 1^2 + 1 = 3 = 1$ **X**

Since neither are 0, this is **not reducible.**

c) $x^4 + 1$
Attempt the same substitution:
f(0) $= 0^4 + 1 = 1$ **X**
f(1) $= 1^4 + 1 = 2 = 0$ ✓

GF(2) $= (x + 1)^4$. This means this is **reducible**.

Q4.

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

$$
\begin{aligned}
x^3 + x + 1 - (x + 1)(x^2 + x + 1) &= x^2 + x \\
x^2 + x + 1 - (1)(x^2 + x) &= 1 \\
x^2 + x - (x^2 + x)(1) &= 0 \\
gcd &= 1
\end{aligned}
$$

b) $x^5 + x^4 + x^3 – x^2 – x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)

$$
\begin{aligned}
x^5 + x^4 + x^3 - x^2 - x + 1/x^3 + x^2 + x + 1 &= x^2 \text{ with a remainder of } x^2 - x + 1 \\
x^3 - +x^2 + x + 1/x^2 - x + 1 &= x + 2 \\
x + 2/x + 2 &= 1 \\
\therefore gcd &= x + 2
\end{aligned}
$$

Q5.

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($K|C$)

We begin by calculating Pr(c), where c is the ciphertext:

$$\begin{aligned}
Pr(1) &= \frac{1}{2}(\frac{1}{4}+\frac{1}{2}) + \frac{1}{4}(\frac{1}{2}) + \frac{1}{4}(0) + 0 = \frac{3}{8} + \frac{1}{8} &= \frac{1}{2} \\
Pr(2) &= \frac{1}{2}(\frac{1}{4}) + \frac{1}{4}(\frac{1}{4}) + \frac{1}{4}(\frac{1}{4}) + 0 = \frac{1}{8} + \frac{1}{16} + \frac{1}{16} &= \frac{1}{4} \\
Pr(3) &= \frac{1}{2}(0) + \frac{1}{4}(\frac{1}{4}) + \frac{1}{4}(\frac{1}{4}) + 0 = \frac{1}{16} + \frac{1}{16} &= \frac{1}{8} \\
Pr(4) &= \frac{1}{2}(0) + \frac{1}{4}(0) + \frac{1}{4}(\frac{1}{2}) + 0 = \frac{1}{8} &= \frac{1}{8}
\end{aligned}$$

Along with this, we need to calculate the probability of each ciphertext given a key:

	1	2	3	4
k1	3/4	1/4	0	0
k2	1/2	1/4	1/4	0
k3	0	1/4	1/4	1/2
k4	0	0	1/4	3/4

Each of these probabilities are found by Pr(Col | Row), so the probability of the ciphertext given the key.

Now that we know both Pr(C | K) and Pr(C), we can use Bayes' theorem to calculate Pr(K | C):

	k1	k2	k3	k4
1	3/4	1/4	0	0
2	1/2	1/4	1/4	0
3	0	1/2	1/2	0
4	0	0	1	0

Finally, we will plug everything into the conditional entropy formula:

$$
\begin{aligned}
H(K \mid C) = &-\Sigma_{(\text{k in K, c in C})} Pr(c)Pr(k \mid c)\log_2(Pr(k \mid c)) \\
&= -\ (1/2(3/4\log_2(3/4) + 1/4\log_2(1/4) + 0\log_2(0) + 0\log_2(0)) \\
&\quad + 1/4(1/2\log_2(1/2) + 1/4\log_2(1/4) + 1/4\log_2(1/4) + 0\log_2(0)) \\
&\quad + 1/8(0\log_2(0) + 1/2\log_2(1/2) + 1/2\log_2(1/2) + 0\log_2(0)) \\
&\quad + 1/8(0\log_2(0) + 0\log_2(0) + 1\log_2(1) + 0\log_2(0))
\end{aligned}
$$

Simplified it becomes:

$$
\begin{aligned}
H(K \mid C) = -(&1/2(3/4\log_2(3/4) + 1/4\log_2(1/4)) \\
&+ 1/4(1/2\log_2(1/2) + 1/2\log_2(1/4)) \\
&+ 1/8(\log_2(1/2)) \\
&+ 1/8(\log_2(1))
\end{aligned}
$$

Which, when calculated, becomes ≈ -0.09436.