CS 1050 Homework 12 Solutions

1a. $7x \equiv 1 \pmod{15} \Leftrightarrow 7x = 15k + 1$ for some k. This means that there should be a value of x in $\{0, 1, \ldots, 14\}$ such that $7x$ leaves a remainder of 1 when divided by 15. We see that $x = 13$ satisfies this condition since $7x \equiv 91 \equiv 1 \pmod{15}$. Therefore $x \equiv 13 \pmod{15}$. A more formal way to solve this is by seeing that gcd of 7 and 15 is 1. Therefore the inverse of 7 modulo 15 exists. Using extended euclid's algorithm we see that $7^{-1} \equiv 13 \pmod{15}$. Therefore $7^{-1}7x \equiv 13 \cdot 1 \pmod{15} \Rightarrow x \equiv 13 \pmod{15}$.

b. $10x + 20 \equiv 11 \pmod{23} \Rightarrow 10x \equiv -9 \equiv 14 \pmod{23}$. Now gcd(10,23) $= 1$. Therefore 10^{-1} modulo 23 exists. Using extended euclid's algoritm we get $10^{-1} \equiv 7 \pmod{23}$. Therefore $10^{-1}10x \equiv 7 \cdot 14 \pmod{23} \Rightarrow x \equiv 98 \equiv 6 \pmod{23}$.

c. $5x + 15 \equiv 4 \pmod{20} \Rightarrow 5x \equiv -11 \equiv 9 \pmod{20}$. However since gcd(5,20) $= 5$, then 9 should be divsible by gcd(5,20) $= 5$, which it is not. Therefore no integral solution to x exists for this equation.

d. We have $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$. Multiplying the second equation by 2 and subtracting the first from it, we get $x \equiv 8 \equiv 1 \pmod{7}$. Therefore $2x + y \equiv 2 + y \equiv 4 \pmod{7} \Rightarrow y \equiv 2 \pmod{7}$.

2. We are given that $ab = cd$, where a, and d are relatively prime. Now, $c = \frac{ab}{d}$. Since c is an integer ab must be divisible by d. However, since a and d are relatively prime, they share no common factors. Therefore, for ab to be divisible by d, all the factors of d must cancel out with b, in other words, b must be divisible by d.

3a. We are given $ax \equiv ay \pmod{n}$, which means that there is a k such that $ax - ay = kn$. Now if $gcd(a, n) = 1$, it means that a and n are relatively prime. Also we have that $a(x - y) = kn$. By the property proved in Problem 2, we get that $x - y$ must be divisible by n, therefore $x \equiv y \pmod{n}$.

b. Let $a = 4, n = 6, x = 3, y = 6$. Now, $ax = 12$, $ay = 24$ and $ax \equiv ay \pmod{n}$. However, $3 \not\equiv 6 \pmod{6}$.

4.a To encrypt 86, we need to calculate $86^e \pmod{n} = 86^3 \pmod{11 \cdot 17} = 86^3 \pmod{187} = 69$.

b. $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. Therefore $3d \equiv 1 \pmod{160}$. Therefore, using extended euclid's algorithm we get $d = 107$.

c. To decrypt we need to calculate the encrypted message raised to the power d modulo n. Therefore we need to calculate $69^{107} \pmod{187} = 86$.

5.a When we sign a message we essentially output $M^d \pmod{n}$, where M is the message to be signed and (d, n) is our private key. However, if M already something encrypted using our public key i.e. $M = N^e \pmod{n}$ for some message N, then when we sign it, we get $N^{ed} \pmod{n} = N$. Therefore we recover the original message.

b. When we sign the given message $y^e x'$, where $x' = x^e \pmod{n}$, we give to the adversary $(y^e x')^d \pmod{n} = y^{ed} x'^d \pmod{n} = yx^{ed} \pmod{n} = xy \pmod{n}$. If the value returned to the adversary is say $c \pmod{n}$, then he can get x by solving $xy \equiv c \pmod{n}$, since he knows the value of y. Infact if he chooses y such that $gcd(y, n) = 1$, he will get a unique value of x moudulo n (since then y^{-1} modulo n would exist).

6. The way to do this in a very simple manner would be fix a polynomial of degree 9 and to give Bush the value of the polynomial at 7 distinct points, and give the rest of his cabinet members the value of polynomial at distinct single points. Since the entire polynomial can be computed only if its value is known at atleast 10 distinct points (by Lagrangian interpolation, as done in the class), Bush and any three of his cabinet members can get the polynomial, and without Bush it would require atleast 10 of his cabinet members to get the polynomial. Once the polynomial say P, is known its value at a predetermined fixed point say $P(0)$ can be used to get the launch code.