CS250:	Hw5 Answers	Fall 2016

1. Your two primes are 11 and 13. You publish your public modulus $n = 143$ and your public encrypting key $e = 7$. But you keep the factorizaton of n secret.

1a. $\varphi(11 \cdot 13) \;=\; 10 * 12 = 120$

1b. Use Euclid's algorithm to compute your secret decryption key, d, the multiplicative inverse of e mod $\varphi(n)$.

$1 = 120 \cdot 1 + 7 \cdot (-17)$. $\quad d = 7^{-1}$ (mod 120) $= (-17)\%120 \;=\; 103$.

1c. Showing your work, compute the encryption of 98 using your public key. (Note you should use the algorithm in Epp, Example 8.4.5.) Call this encrypted message a.

$a = 98^7\,\%143 = 32$. Note that 7 = 111 base 2. The powers of 98 (mod 143) are as follows: $98^2\,\%143 = 23$, $98^4\,\%143 = 100$.

Thus, $98^7\,\%143 \;=\; (98^4 \cdot 98^2 \cdot 98^1)\,\%143 \;=\; (98 \cdot 23 \cdot 100)\,\%143 \;=\; 32$.

1d. $32^{103}\,\%143 = 98$. To see this note that 103 = 1100111 base 2.

The powers of 32 mod 143 are: 32, 23, 100, 133, 100, 133, 100.

$32^{103}\,\%143 \;=\; (32^{64} \cdot 32^{32} \cdot 32^4 \cdot 32^2 \cdot 32^1)\,\%143 \;=\; (100 \cdot 133 \cdot 100 \cdot 23 \cdot 32)\,\%143 \;=\; 98$.

1e. To sign the message, "25", raise 25 to the power d mod n. Call the answer c, your signed contract.

$25^{103}\,\%143 = 38$

The powers of 25 mod 143 are: 25, 53, 92, 27, 14, 53, 92.

$25^{103}\,\%143 \;=\; (25^{64} \cdot 25^{32} \cdot 25^4 \cdot 25^2 \cdot 25^1)\,\%143 \;=\; (92 \cdot 53 \cdot 92 \cdot 53 \cdot 25)\,\%143 \;=\; 38$.

1f. The powers of 38 mod 143 are; 38, 14, 53.

$38^7\,\%143 \;=\; (38^4 \cdot 38^2 \cdot 38^1)\,\%143 \;=\; (53 \cdot 14 \cdot 38)\,\%143 \;=\; 25$.

2. We will prove the CRT. Please make sure that you understand what this says:

$$\forall a, b > 1\, (\gcd(a, b) = 1 \ \rightarrow\ \forall x \in \mathbf{Z}/a\mathbf{Z}\ \forall y \in \mathbf{Z}/b\mathbf{Z}\ \exists! z \in \mathbf{Z}/ab\mathbf{Z}\ (z \equiv x \pmod a \ \wedge\ z \equiv y \pmod b)))$$

2a. In order to prove the CRT, let $a > 1, b > 1$ with $\gcd(a, b) = 1$. Define the function, $f : \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \rightarrow \mathbf{Z}/ab\mathbf{Z}$ as follows: $\quad f(x, y) \stackrel{\text{def}}{=} \big(x \cdot b \cdot (b^{-1}\text{mod } a) \ +\ y \cdot a \cdot (a^{-1}\text{mod } b)\big)\ \%\ (a \cdot b)$

Show that $f(x, y) \equiv x \pmod a$ and $f(x, y) \equiv y \pmod b$. First note that $(n\%ab)\%a \ = \ n\%a$. Thus, we have to show that $(x \cdot b \cdot (b^{-1}\text{mod } a) \ +\ y \cdot a \cdot (a^{-1}\text{mod } b))\ \%\ a \ = \ x$. This is an easy calculation: the first term is x since $b \cdot (b^{-1}\text{mod } a) \equiv 1 \pmod a$ and the second term is 0 (mod a). A similar argument shows that $f(x, y)\ \%\ b \ = \ y$.

2b. Argue that it follows that f is 1:1. From 2a, we know that $f(x, y)\ \%\ a = x$ and $f(x, y)\ \%\ b = y$. Thus, from $f(x, y)$ we can uniquely determine x and y. Thus f is 1:1.

2c. $|\mathbf{Z}/n\mathbf{Z}| = n$. Thus both the domain and co-domain of the function f have cardinality ab.

2d. f is a 1:1 function from a set of size ab to a set of size ab. Since every element of the co-domain is hit at most once, and ab elements of the co-domain are hit, all the elements of the co-domain must be hit. Thus f is onto. (Any function from a finite set of size n to a set of the same size, n, is 1:1 if and only if it is onto. Note this is not true in general, just with these finite and same size conditions.) **Thus, we have proved the CRT.**

2e. Now let $f' = f \cap (\mathbf{Z}_a^* \times \mathbf{Z}_b^*)$ be the restriction of f to $\mathbf{Z}_a^* \times \mathbf{Z}_b^*$. Argue that $f' : f \cap (\mathbf{Z}_a^* \times \mathbf{Z}_b^*) \rightarrow \mathbf{Z}_{ab}^*$ and that f' is $1:1$ and onto.

f' is 1:1 because any restriction of a 1:1 function is still 1:1. (Since f never hits the same item in the co-domain twice, neither can f'.) Let $n \in \mathbf{Z}_{ab}^*$ be arbitrary. By the CRT, we know that $n = f(x, y)$ for some $x \in \mathbf{Z}/a\mathbf{Z}$ and $y \in \mathbf{Z}/b\mathbf{Z}$. Observe that $\gcd(x, a) = 1$ because from the definition of f, if x had a divsor in common with a, then $f(x, y)$ would have that same divisor in common with ab. For the same reason, $\gcd(y, b) = 1$. It follows that f' is onto.

2f. Since f' is a 1:1 and onto function, it's domain and co-domain have the same size. It thus follows that $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.