pg 1 Hwk #9 Zachary Hightower

1. Alice needs to send Bob a number M using RSA encryption. She has to be careful of Eve, who is eavesdropping. Bob picks two primes $p=2$ and $q=11$, so that $n=pq=22$

(a.) What is $\phi(n)$?

$\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$

$\phi(n) = 10$

Or $\phi(n) = (p-1)(q-1) = (2-1)(11-1) = 10$

(b.) Bob picks the encryption key $e=7$
Is this a valid choice for an encryption key? Why or why not?

Yes, because 7 is within $Z^*_{\phi(n)} = Z^*_{10}$

and it has an inverse in $(Z^*_{10}, \otimes)$

$7 \cdot 3 = 1 \mod 10$

pg 2

(c.) Bob sends Alice $n = 22$ and $e = 7$, which she used to encrypt M. She gets the encrypted number $N = 15$, which she sends to Bob.

(d.) Decrypt N using the decryption key d. What was Alice's number M?

$d = 3$ because $e = 7$ and $d = 7^{-1} = 3$

We decrypt with the formula

$$
\begin{aligned}
N^d \pmod n &= 15^3 \pmod{22} \\
&= ((225) \cdot 15) \bmod 22 \\
&= ((225 \bmod 22) \cdot 15) \bmod 22 \\
&= (5 \cdot 15) \bmod 22 \\
&= 75 \bmod 22 \\
&= 9
\end{aligned}
$$

pg3

2. Using RSA encryption, we choose the primes $p = 11$; $q = 13$, and announce the public keys $n = 143$ and $e = 113$. Someone sends us the encrypted message $N = 81$. Find the original message.

$n = pq = 11 \cdot 13 = 143$ So, $\phi n = (p-1)(q-1) = 120$

113 is relatively prime to 120 and is an element of Z^*_{120}

$d = 113^{-1} = 37$ $\qquad 37 \otimes 113 = 1 \bmod 120$

To decrypt $N^d \pmod n = 81^{37} \pmod{143}$

$= (((81^2)^{18} \cdot 81) \bmod 143$

$= (((6561)^{18} \cdot 81) \bmod 143$

$= (((126)^{18} \cdot 81) \bmod 143$

$= (((126^2)^9 \cdot 81) \bmod 143$

$= (((15876)^9 \cdot 81) \bmod 143$

$= ((3^9) \cdot 81) \bmod 143$

$= ((19683) \cdot 81) \bmod 143$

$= ((92) \cdot 81) \bmod 143$

$= 7452 \bmod 143$

$= 16$

pg 4

3. Alice and Bob need to determine a secret key N using Diffie-Hellman key exchange. They agree on the prime $p = 11$ and the base $g = 7$

(a.) Alice chooses a secret integer $a = 3$. What number A does she send to Bob?

$A = g^a \bmod P$ so $A = 7^3 \bmod 11$

$A = 343 \bmod 11$

$A = 2$

(b.) Bob chooses a secret integer $b = 8$. What number B does he send to Alice?

$B = g^b \bmod P$

$= 7^8 \bmod 11$

$= 7^8 \bmod 11$

$= ((7^2)^4) \bmod 11$

$= ((49)^4 \bmod 11$

$= 5^4 \bmod 11$

$= 9$

pg 5

(c.) What is the secret key N, and how does Alice compute it?

$N = g^{ab} \bmod p \Rightarrow N = B^{a} \bmod p$

$= 9^{3} \bmod 11$

$= 729 \bmod 11$

$= 3$

(d.) What is the secret key N and how does Bob compute it?

$N = g^{ab} \bmod p \Rightarrow N = A^{b} \bmod p$

$= 2^{8} \bmod 11$

$= 256 \bmod 11$

$= 3$