Amanda Lewis

Dr. Shebaro

COSC 3325-02

HW #3

Problem #1:

Alice's public key: (21, 5)

Alice's private key: (21, 5)

Part 1:

For my private and public keys, I will pick p=5 and q=7 so N=35. I will pick e=5 so d=29 because 145 % (4)(6) = 1

My public key: (35, 5)

My private key: (35, 29)

Part 2:

My name is "Amanda Lewis" and transforming it into ASCII would give 34-65-77-65-78-68-65-32-76-69-87-73-83-84. Since most of these numbers are greater than the N's, I will go digit by digit and convert using Alice's public key. I know $2^5\%21 = 11$, $3^5\%21 = 12$, $4^5\%21 = 16$, $5^5\%21 = 17$, $6^5\%21 = 6$, $7^5\%21 = 7$, $8^5\%21 = 11$, and $9^5\%21 = 18$. so I will get 12-16-6-17-7-7-6-17-7-8-6-8-6-17-12-11-7-6-6-18-8-7-7-12-8-12-8-16 as my string representing each of the digits from the original message.

Part 3:

Given the string of digits 34-65-77-65-78-68-65-32-76-69-87-73-83-84 which represent my name, I will use my private key so anyone who intercepts the message can use my public key to decode and verify that I am the sender of the message. I know $2^{29}\%35 = 32$, $3^{29}\%35 = 33$,

$4^{29}\%35 = 9$, $5^{29}\%35 = 10$, $6^{29}\%35 = 6$, $7^{29}\%35 = 7$, $8^{29}\%35 = 8$, and $9^{29}\%35 = 4$. This will give 33-9-6-10-7-7-6-10-7-8-6-8-6-10-33-32-7-6-6-4-8-7-7-33-8-33-8-9 as my digital signature.

Part 4:

I will encrypt my message with Alice's public key, and then sign it with my private key so anyone can decrypt and verify I am the sender, but only Alice can read the message. The encrypted message is 12-16-6-17-7-7-6-17-7-8-6-8-6-17-12-11-7-6-6-18-8-7-7-12-8-12-8-16 from part 2 and $11^{29}\%35 = 16$, $12^{29}\%35 = 17$, $16^{29}\%35 = 11$, and $17^{29}\%35 = 12$, $18^{29}\%35 = 23$. The message encrypted with my digital signature will be 17-11-6-12-7-7-6-12-7-8-6-7-6-12-17-16-7-6-6-23-8-7-7-17-8-17-8-11.

Part 5:

I will encrypt my digital signature, which has been encrypted with my private key, with Alice's public key so only she can decrypt and read the message by using her private key and then my public key to decrypt my signature. My digital signature was 33-9-6-10-7-7-6-10-7-8-6-8-6-10-33-32-7-6-6-4-8-7-7-33-8-33-8-9 from part 3 and $10^5\%21 = 19$, $32^5\%21 = 2$, and $33^5\%21 = 3$. My encrypted message becomes 3-18-6-19-7-7-6-19-7-8-6-8-6-19-3-2-7-6-6-16-8-7-7-3-8-3-8-18.

Problem #2:

Their common shared key is $10^{11*13}\%541 = 511$. Alice will send $10^{11}\%541 = 297$ to Bob and Bob will send $10^{13}\%541 = 486$ to Alice. Alice will compute $486^{11}\%541 = 511$ and Bob will compute $287^{13}\%541 = 511$.