CSS 322 – QUIZ 6 ANSWERS

First name: _____ Last name: _____

ID: _____ Total Marks: _____

out of 10 (+2 bonus)

Question 1 [4 marks]

Using RSA, encrypt the message M = 3, assuming the two primes chosen to generate the keys are p = 13 and q = 7. You should choose a value e < 10. Show your calculations and assumptions.

With RSA we perform the following calculations:

$n = pq = 13.7 = 91$

$\phi(n) = (p-1)(q-1) = 12.6 = 72$

e and $\phi(n)$ should be relatively prime, which means their greatest common divisors should be 1. That means *e* cannot be a divisor of 72 including 2, 3, 4, 6, 8, 9, 12, 18, 24 or 36. Since e must be less than 10, it can be either 5 or 7.

If e = 5:

$C = M^e \bmod n$

$= 3^5 \bmod 91$

$= 243 \bmod 91$

$= 61$

If *e* = 7:

$C = 3^7 \bmod 91$

$= 2187 \bmod 91$

$= 3$

Question 2 [4 marks]

If Alice used the RSA algorithm in Question 1 to send the message M = 3 to Bob so that Charlie could not read the message, then:

a) Do you know Alice's public key? If yes, what is it?

Answer: No. The public and private key needed to encrypt both belong to Bob. Nothing is known about Alice's public (or private) key.

b) Do you know Bob's public key? If yes, what is it?

Answer: Yes. Bob's public key is a combination of *n* and *e*: {91, 5}.

c) Assuming a brute force attack is not possible, explain the steps that Charlie could take to break the encrypted message. (You do not need to perform the calculations, you just need to say what Charlie needs to calculate and why).

Answer: Charlie needs to calculate *d*. He can do so from knowing that d.e = 1 mod($\phi(n)$), and hence needs to calculate $\phi(n)$. That is, count all the numbers less than 91 that are relatively prime with 91.

d) Although breaking RSA in this example with the steps from part (c) is possible, in general, why is RSA hard to break?

Answer: It is hard (practically impossible for large numbers) to factor $\phi(n)$, which involves finding the prime factors of *n*.

Question 3 [2 marks]

In the above questions, if a central Certificate Authority is used, then what is its purpose? (That is, what does the Certificate Authority do).

Answer: The CA certifies that the Public key of Bob actually belongs to Bob.

Bonus Question [Bonus 2 marks]

Show the calculations to break the cipher from Question 2(c).

As an attacker we know the public key values, that is, n = 91 and e = 5. We also know the ciphertext C = 61. To determine the plaintext M, we need to find d, which means we need to find $\phi(n)$ since:

$de \equiv 1 \bmod(\phi(n))$

Using trial and error, we factor 91 into its two prime factors: 13 and 7. This gives us $\phi(n)$ = (p-1)(q-1) = 72.

So now we determine which what values of d does 5d mod 72 = 1 hold:

73 / 5 is not an integer

145 / 5 is an integer (29).

So d = 29, and now we can calculate the plaintext:

$M = C^d \bmod n$

$= 61^{29} \bmod 91$

$= 3$