CSS322 – Quiz 4 Answers

Name: ____

ID: ____________________________ Mark: __________ (out of 10)

Question 1 [2 marks]

Calculate the following:

a) $\Phi(24)$

b) $\Phi(19)$

c) $\Phi(323)$

Answers

$\Phi(24)$: factors of 24 are 2, 3, 4, 6, 8, 12. Numbers relatively prime to 24 are: 1, 5, 7, 11, 13, 17, 19, 23. Therefore $\Phi(24) = 8$.

$\Phi(19)$: 19 is prime therefore the answer is 18.

$\Phi(323)$: 323 = 19*17, and since both 19 and 17 are prime, $\Phi(323) = \Phi(19) * \Phi(17) = 18*16 = 288$.

Question 2 [2 marks]

Derive (or manually calculate) the answer to: $19^8 (mod\ 24)$

Answer

Euler's theorem states: $a^{\Phi}(n) \equiv 1\,(mod\ n)$ if *a* and *n* are relatively prime.

We know $\Phi(24) = 8$ and we know 19 and 24 are relatively prime (see question 1). Therefore the expression is in the form of Euler's theorem, and hence the answer is 1 (mod 24).

Question 3 [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.

Answer

First calculate the value of *n* from *p* and *q*:

$$n = p * q = 13 * 7 = 91$$

The totient of *n* is easily calculated since we know *n*'s prime factors, *p* and *q*:

$\Phi(n)=\Phi(p*q)=\Phi(p)*\Phi(q)=(p-1)*(q-1)=12*6=72$

Now we need to choose a value of *e* which is relatively prime to $\Phi(n)$. Note the factors of 72 are: 2, 3, 4, 6, 8, 9 ,12, 18, 24 and 36. *e* must not have a factor in common with these, and since the question limits *e* to less than 10, the possible value are: 5 or 7.

The encryption with *e* = 5:

$C=M^e \bmod n=3^5 \bmod 91=243 \bmod 91=61$

If *e* = 7:

$C=M^e \bmod n=3^7 \bmod 91=2187 \bmod 91=3$

Question 4 [2 marks]

If Alice used the RSA algorithm in Question 3 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? [1 mark]

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? [1 mark]

Answer

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

Bonus Question [Bonus 2 marks]

Assuming brute force is not possible, show the calculations that Charlie would need to perform to to break the cipher from Questions 3 and 4.

Answer

The attacker knows *n* = 91, *e* = 5 and *C* = 61. To determine the plaintext *M* the attacker can try to find *d* (part of the private key).

Since $ed \equiv 1 \bmod (\Phi(n))$ we first need to find $\Phi(n)$. You could manually count the values less than 91 and relatively prime to 91 or factor 91 into its prime factors (which is easy for such a small number): 13 and 7. Now we have *p* and *q* we can calculate $\Phi(n)$ to be 72.

Now we must find a value of *d* which is a multiplicative inverse of *e*. In other words, a number that satisfies one of the following:

5d = 73 or 5d = 145 or 5d = 217 or …, since if we mod by 72 the answer will be 1.

From the above you notice that if d = 29 it is a multiplicative inverse of e. You we have d we can find the plaintext by decrypting:

$$M = C^d \bmod n = 61^{29} \bmod 91 = 3$$