CSS322 – Quiz 4 Answers

Name: ____

ID: ______________________________ Mark: __________ (out of 10)

Question 1 [5 marks]

There are 4 users in a network: *Napat, Jira, Apiwat, Funtida*. Each user has their own pair of public/private keys: PU_{user} and PR_{user} (e.g. PU_{Napat} and PR_{Napat}). Using a public key algorithm, the encrypt and decrypt operations performed with a particular *key* can be written as:

$$C = E_{key}(P) \qquad P = D_{key}(C)$$

Answer the following questions assuming all appropriate keys have been generated and distributed. Use the notation for keys and encrypt/decrypt as given above.

a) List all the keys known (or that can be easily obtained) by Napat/Jira/Apiwat/Funtida. [2 marks]

Answer

Each user knows their own key pair, as well as the public keys of other users. For example, Napat would know:

PU_{Napat}, PR_{Napat}, PU_{Jira}, PU_{Apiwat}, $PU_{Funtida}$

b) If Napat/Funtida/Napat/Funtida wants to send a confidential/authenticated message *M* to Jira/Apiwat/Funtida/Jira, then write the operation the sender performs on *M*. [2 marks]

Answer

To send a confidential message, the message must be encrypted with the recipients public key. For example, for Napat to send to Jira:

$E_{PUJira}(M)$

To send an authenticated message, the message must be encrypted with the senders private key. For example, for Napat to send to Jira:

$E_{PRNapat}(M)$

c) What key is used by the recipient to decrypt the received message? [1 mark]

Answer

For confidentiality, the recipient decrypts using their private key, e.g. Jira would decrypt with PR_{Jira}.

For authentication, the recipient decrypts using the senders public key, e.g. Funtida would decrypt using PU_{Napat}.

Question 2 [5 marks]

Using RSA, encrypt the message M = 4/3/6/3, assuming the two primes chosen to generate the keys are p = 13/11/17/13 and q = 7/7/5/11. You should choose the smallest possible $e > 1$. Show your calculations and assumptions.

Answer

First calculate the value of n from p and q:

$$n = p*q$$

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

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

Now we need to choose a value of e which is relatively prime to $\Phi(n)$. Consider the factors of $\Phi(n)$ and then choose an e which does not have a common factor.

Finally the encryption is:

$$C = M^e \bmod n$$

p	q	n	$\Phi(n)$	Factors of $\Phi(n)$	Possible e	M	C
13	7	91	72	2,3,4,6,8,9,...	5,7	4	23
11	7	77	60	2,3,4,5,6,...	7	3	31
17	5	85	64	2,4,...	3,5,7,9	6	46
13	11	143	120	2,3,4,5,6,8,...	7	3	42