First of all i used these modulo rules for further simplification of equation in these problem

Lets go to the problem two,

Problem two is about deffie-helman protocoal . We use this protocol to share a key . public knowleadge about this protocol is p and g ,which are given as 13 and 2 . and private knowleadge is secret component that each communicators chose which are 5 and 4 . It says that after shared the key , the key is used as numbers of letters to be shifted in ceirsar cyper encryption . Alice need to send message ENCRYPT .

In the first question it asked for eshared key and the encryption message

I started calculation shared key as bob since i thought it would be easier to calculate . as shown here alice send initial message A which is generated using her secret component . and bob used his secret component and modulo 13 operation to calculate shared key

After applying thefirst rule i mentioned previously i could get final answer as 9 . which means alice need to shift 9 letters to the right in order to get encrypted message . I generated the table to make it easier the encryption . and final encrypted message is like this.

Second question is about man in the middle attack . In the process ,man in the middle generate two seperate key for him and alice and him and bob . For that he uses secret component for himself which is given as 7 .

problem is to find the original message sent to the bob by eva if bob has recived this message.

First we need to find shared key between bob and eva . Eva has sent this initial message generated using her secret component . and bob used his secret component and modulo 13 operation in order to generate shared key . I have apply first rule that i mentioned earlier . and got final answer as 3 .

Then i generated table with cipher text and their relevant alphabet decryption process. Then i got the decrypted message as like this which is eva original message sent to bob.

Problem 3 about asyymetric encryption . In the question it uses RSA textbook for encryption and decryption . The question is to show all the major steps used in encryption and decryption prcoess .

First of all we need to choose two prime numbers , which have been given as 5 and 13 . Then i need to calculate N and pi . After that i need to chose coprime with pi .which also given as 7 .

Next i need to find d which is inverse value of e with mod pi . in this case d is 7

now we can derive public key tuple . N and e here 65 and 7 and private key tuple N and d in this case 65 and 7.

Now the key generation part is done and we have private key and public key. Assuming we distributed our public key to general public lets start with encryption process using public key . Since my index is 190070V . is chose my message as 5 . we can get encrypted message by m to the power e mod N operation. It gives much larger value to find mod N . I applied second rule for expnasion of 5 to the power of 7 . then i applied first rule to calculate 5 ti the power 6 by expanding 6 by 3 times six. after several steps i got 60 as the encrypted message.

Now private key holde should be able to decrypt this message and get original message . Let try that.

To decrypt i need to get mod N operation for encrypted message to the power d from private key tuple . as earlier i applied second rule and first rule in third step to simplyfy the euqation . then i again applied second rule again in step 6 to expand 25 to the power of 3 for further simplification . and finally i got the answer as 5 which is my original message .

This is the RSA textbook process works with its major steps.

|  |  |  |
| --- | --- | --- |
| fdsfdsdsfdsdsf | fdsfdsfd | sfddsf |
| sddsfds | sfds | dsfds |
| sdfdsffs | sdfds | dsfdsf |

