Department of CIS

Subject: Network Security
Summer 2020

Theory Part (Marks – 35)

Question

Bob and Mary are two people who want to have a secure, encrypted communication; however, an eavesdropper named Eve wants to listen into their conversation.

Bob opts for an asymmetric cryptosystem where he will have a private key and Mary will be sent a public key with which she could encrypt her texts. So, they both looked into RSA cryptosystems and used that for their communication. Bob wants to use small prime numbers like 19 and 23 at first but using these small prime numbers, he figured out a problem in the RSA cryptosystem while trying to encrypt a text like "Hie". He changed his initial prime numbers to something that falls within the range of 235 to 245 so that the prime numbers are larger. Bob also wanted his encryption key, e to be in the range of 70 to 80.

They also explored other cryptosystems such as 3DES and AES and even looked at classical ciphers such as Ceaser's Cipher to see which better suited their needs.

(Note that Bob and Mary chose A = 1 while they converted the alphabetical term to numerical for encryption)

Task 1 (Design): 15 marks

What would the public key and private key be for Bob after he changed his prime number range to 235-245? Show the whole process in which he finds this out.

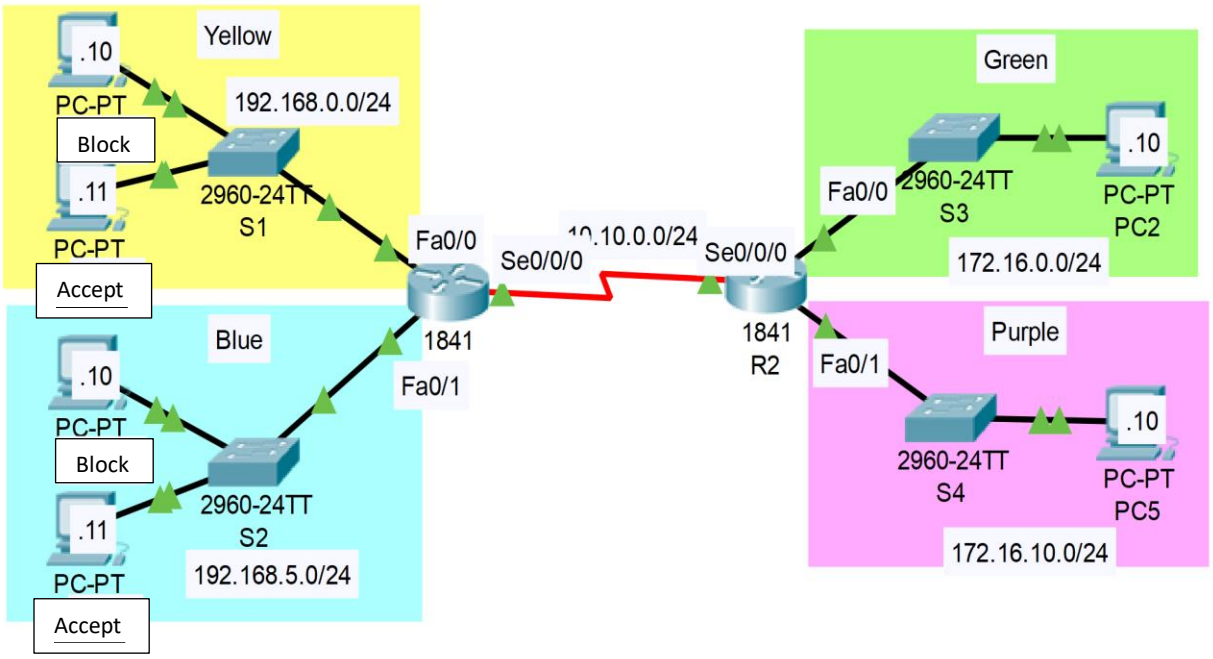
Task 2 (Simulation): 10 marks

Why would Bob not be able to encode “Hie” using the keys derived from 19 and 23. Show the simulation by trying to encrypt and decrypt the message and give your reason.

Task 3 (Critical Evaluation): 10 marks

Other than RSA, Bob tried for other ciphers as well. One of them was Ceaser’s Cipher with a shift of 17. What would the changed text message be? Would this be more or less secure than RSA? Give proper reasoning behind that.

Lab Part (Marks – 25)



Link to PKA file –

https://drive.google.com/file/d/14FRDMWhZKWEA9SVGgah3H3r0Eu3jIdc8/view?usp=sharing

Task 1 (15 Marks):

In the topology above, the network devices and hosts have already been configured with IP addresses and static routes. You have to design a **standard, named ACL** that **permits** *one host from the yellow* and *one host from the blue networks* to reach the *green network*. **All other yellow and blue hosts must not be able to reach the green network.** The ACL should not affect the purple network in any way. Place the ACL in the correct interface of the correc

Task 2 (5 Marks):

Place the ACL in the correct interface of the correct router. Remember that you're using a named standard ACL.

Task 3 (5 Marks):

If you were to block both the hosts from the yellow network into the green network, how should you change your named ACL? Show it.

Submission Guidelines:

- Your submission should be in the form of a single word-processed document **(.doc or .docx)** that includes any necessary diagrams.
- Naming of the file as **example:** 183-16-315.docx
- **Marks will be deduced accordingly if any plagiarism of work is provided.**

DEADLINE:15th August 2020