Do not begin until asked to do so

Name:

NYU ID:

Instructions:

- Be sure to read the questions carefully and answer all parts
- All questions require an explanation for full credit

1. **Risk Assessment**: ACME Corporation has a MySQL database that contains credit card numbers. The company does not have a Cybersecurity specialist to keep the database continuously secure from the latest attacks. Suppose the MySQL database as a probability of being compromised once in four years, and each time it's compromised it loses 1.5 million CC numbers which will cost the company $1 per CC number lost and $500k one-time marketing fee to repair ACME's reputation.

1a. [3 pts] What's the Single Loss Expectancy (SLE)?
1b. [2 pts] What's the Annualized Rate of Occurrence (ARO)?
1c. [2 pts] What's the Annualized Loss Expectancy (ALE)?
1d. [3 pts] Would hiring a team of Cybersecurity database specialists which costs $500k/year be worth it if the specialist can stop all database attacks? Why or why not?

2. **DNS Reconnaissance**: Suppose an attacker is performing reconnaissance on ACME Corporation using only the DNS protocol.
2a. [6pts] What are three methods using only the DNS protocol that an attacker can use to perform reconnaissance on ACME Corporation? Identify what type of information can be obtained.
2b. [4pts] What are two mitigation strategies to minimize what an attacker can obtain from using DNS?

3. **Covert Channels**: Suppose a client is communicating to a server using TCP. They have a covert channel set up by piggybacking on the TCP connections between the two hosts.
3a. [6 pts] Describe three ways that a covert channel can be established using only fields in the TCP header.
3b. [4 pts] Discuss two ways that this can be detected and potentially stopped.

4. **Scapy**: Explain what the following scapy commands do:
4a. [4 pts] send(Ether()/IP(src=RandIP(),dst="10.10.111.1")/TCP(dport=80))
4b. [4 pts] sr1(IP(dst="10.10.111.0/24")/TCP(dport=(1,100),flags="A"))

5. **Miscellaneous**

5a. [4 pts] Discuss how is DNS amplification attack similar to NTP amplification attack?

5b. [4 pts] What are the differences between the nmap Connect scan and SYN Scan?

5c. [4 pts] Using the Julius Caesar's Cipher, the plaintext message "HELLO" is encrypted to the ciphertext "XUBBE". What is the key used?

6. Perform RSA key generation with p=7 and q=11. Note: you must show work for any modular mathematics.

6a. [2 pts] Compute n and φ

6b. [2 pts] Choose the smallest possible public (encryption) exponent e

6c. [4 pts] Choose a private (decryption) exponent d

6d. [4 pts] Encrypt the plaintext message m=18 with the public key

6d: [2 pts] Explain if it's possible to encrypt using the decryption key d and decrypt using the encryption key e.

7. Perform Diffie-Hellman shared key generation with g=5, n=19, Alice selects a=6 as her secret, Bob selects b=7 as his secret.

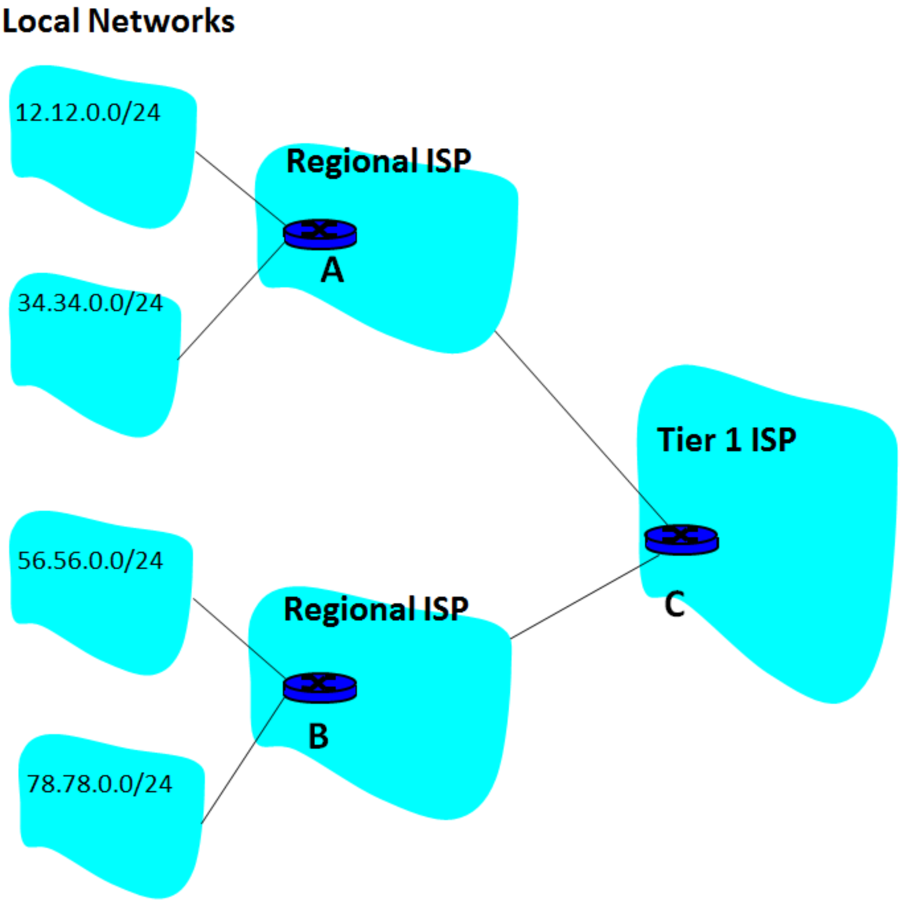
7a. [3pts] calculate Alice's public key A

7b. [2pts] calculate Bob's public key B

7c. [4pts] calculate the shared key K

7d. [3pts] Based on the size of a, b, g, and n, would this key exchange be difficult to break if Trudy intercepted the publically exchanged values? Why or why not?

8. Ingress Filtering



The networks depicted in the above diagram are implementing ingress filtering. The four networks on the left are the local networks (e.g., NYU), the middle two networks are regional ISPs, and the rightmost network is a Tier-1 ISP. The labels A, B, and C donate Routers in the respected networks that are implementing ingress filtering. For example, Router A is the router performing ingress filtering for traffic from the networks from the networks 12.12.0.0/24 and 34.34.0.0/24.

8a. [4 pts] Explain what ingress filtering is and what type of attack it is attempting to prevent.

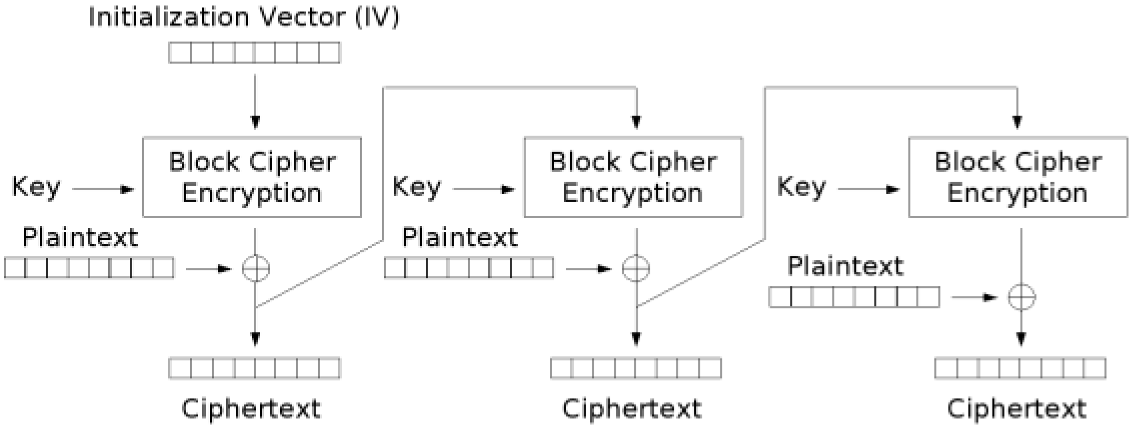
8b. [4 pts] If ingress filtering is implemented for Router C, what addresses what it filter or not filter? What address can still bypass the filtering?

8c. [4 pts] If ingress filtering is implemented for Router A and B, what addresses would each router filter or not filter? What address can still bypass the filtering?

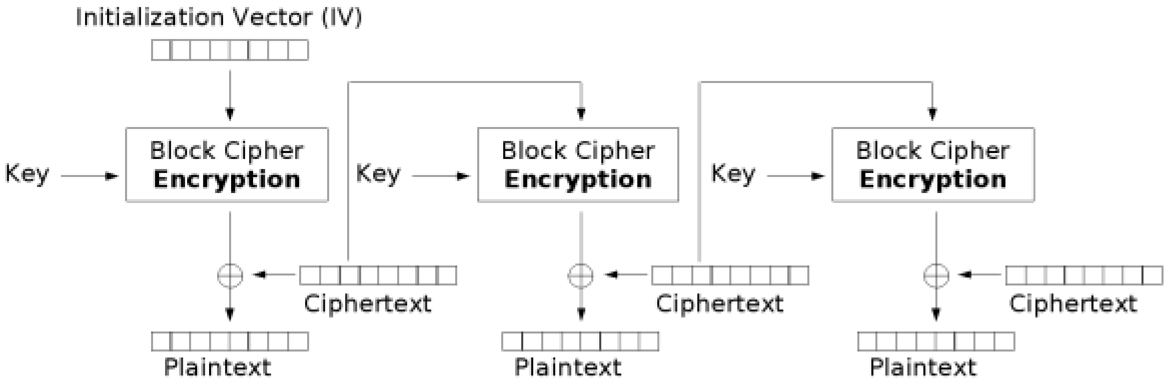
9. Block Cipher Mode of Operations

Input	**Output**	**Input**	**Output**
0000	0111	1000	1111
0001	0110	1001	1110
0010	0101	1010	1101
0011	0100	1011	1100
0100	0011	1100	1011
0101	0010	1101	1010
0110	0001	1110	1001
0111	0000	1111	1000

The following diagram shows Cipher Feedback (CFB), a similar mode of operation to CBC. Note that for CFB, the decryption mode actually uses the encryption.



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption

9a. [3 pts] What benefit does "mode of operations" add to block ciphers?

9b. [3 pts] Decrypt Ciphertext 110000111011 without using any mode

9c. [6 pts] Decrypt Ciphertext 110000111011 using CFB and IV=0101