ACME Corporation has a shopping website that makes a profit of $1000 per day. It's vulnerable to a particular DDOS attack that can bring the entire web server down for five days in a single incident. The engineers calculated each DDOS incident will cost the company $200 per day in security consulting fees along with the lost profit. The engineers also calculate that the chance of a DDOS attack is once in two years.

1a. [3pts] 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 a firewall that can prevent this particular DDOS attack that cost $10k to purchase with an annual licensing cost of $1000 per year be worth it? Explain.

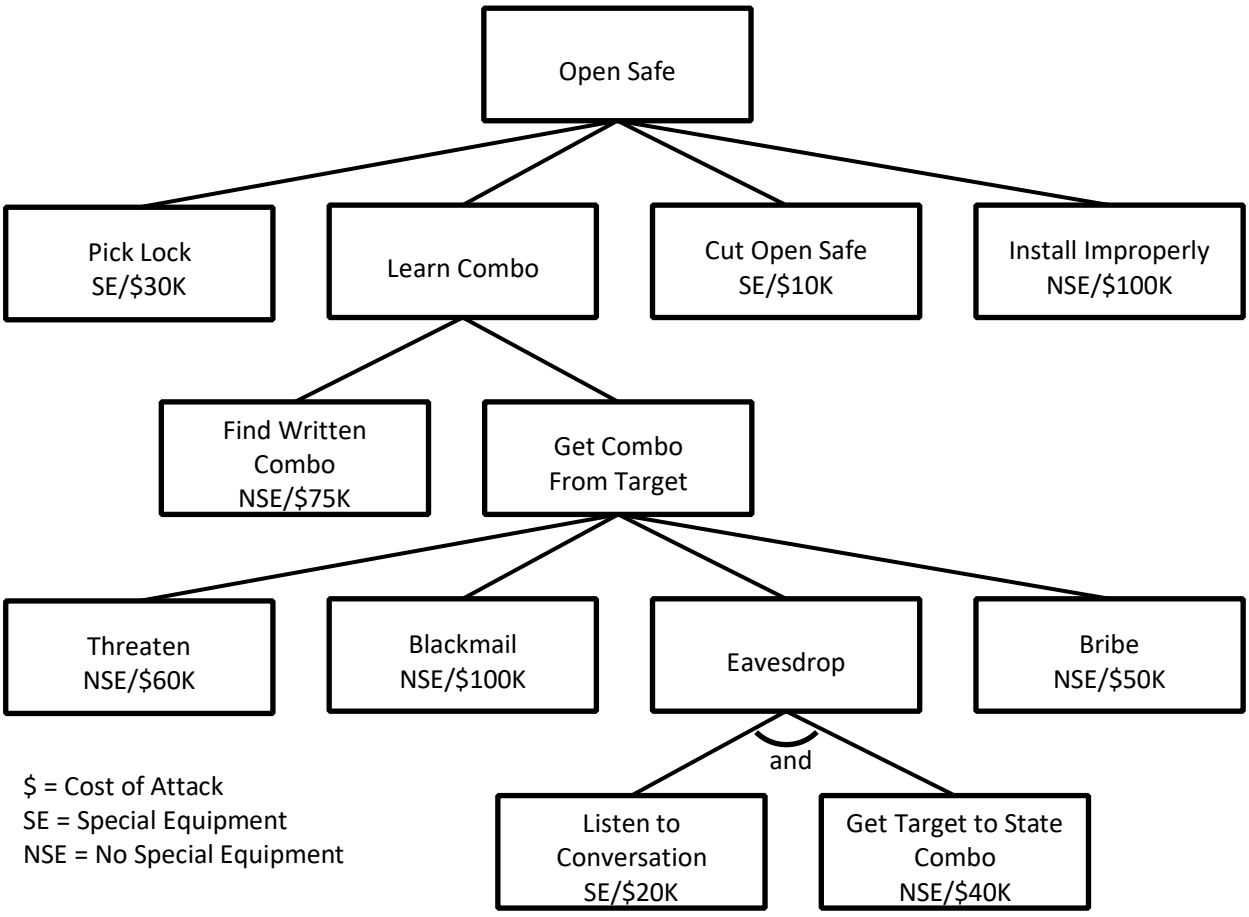
Risk Assessment: ACME Corporation has a MySQL database that contains credit card numbers. The company does not have a Cybersecurity specialist to keep the database continuously secure from the latest attacks. Suppose the MySQL database as a probability of being compromised once in four years, and each 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?

Risk Assessment: ACME Corporation has a corporate intranet where software for medical devices are being developed. ACME wants to secure the network by upgrading the firewall and installing an intrusion detection and monitoring program. The cost of the upgrade is a one-time fee of $300k with $100k a year of maintenance each year. Suppose the intranet has a probability of being compromised twice per year, and each time a compromise occurs, ACME will need to pay an outside consultant $100k to fix the compromise.

1a. [2 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. [2 pts] Would upgrading the security of the network be worth it? Why or why not?

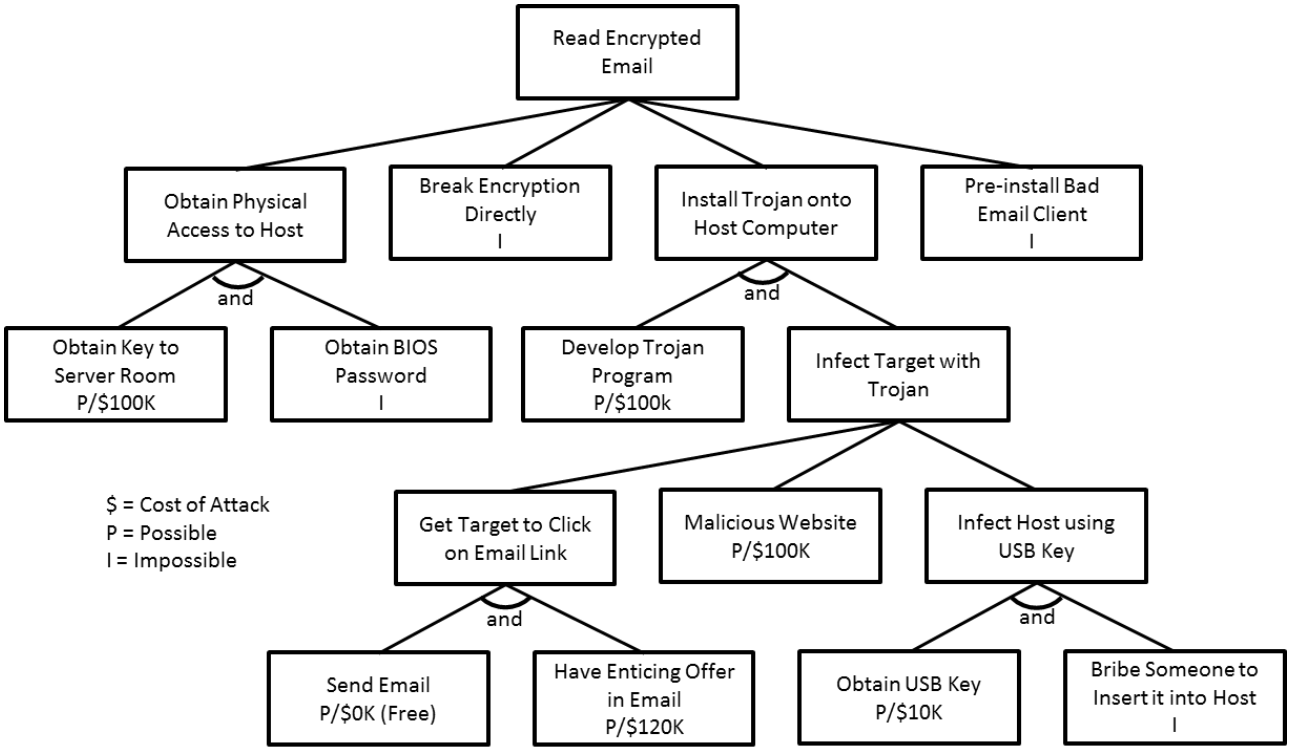
Attack Trees



$ = Cost of Attack
SE = Special Equipment
NSE = No Special Equipment

2a. [3pts] What's the cheapest attack (name and amount) that requires no special equipment?
2b. [4pts] What's the cheapest and most expensive methods and amounts to **Get Combo From Target**?
2c. [3pts] What's the most expensive attack (name and amount) that requires special equipment?

Attack Trees

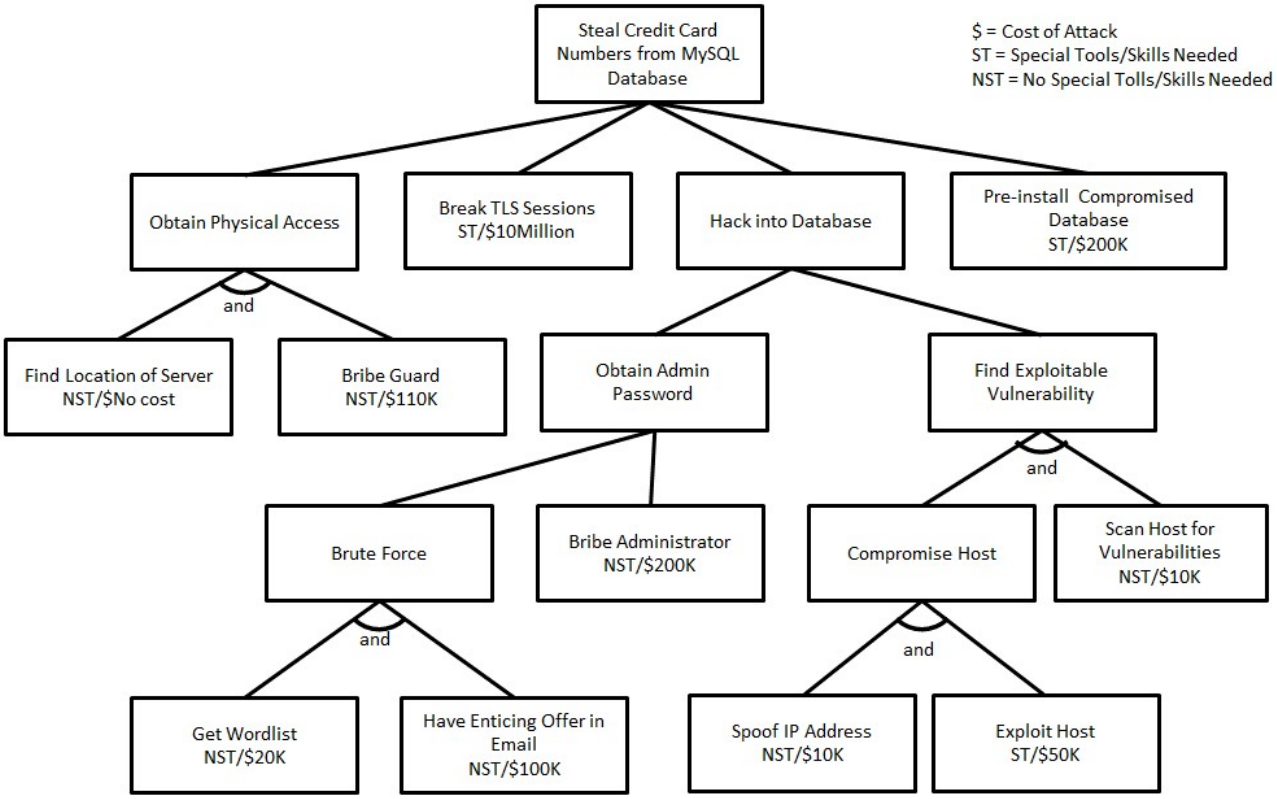


1a. [3 pts] What's the cheapest attack (name and amount) that's Possible?

1b. [4 pts] What's the cheapest and most expensive methods (name and amount) that's Possible to Infect Target with Trojan?

1c. [3 pts] Suppose it's Possible to "Obtain BIOS Password", and the Cost of Attack for it is $50K. Now, what is the cheapest attack (name and amount) that's Possible now?

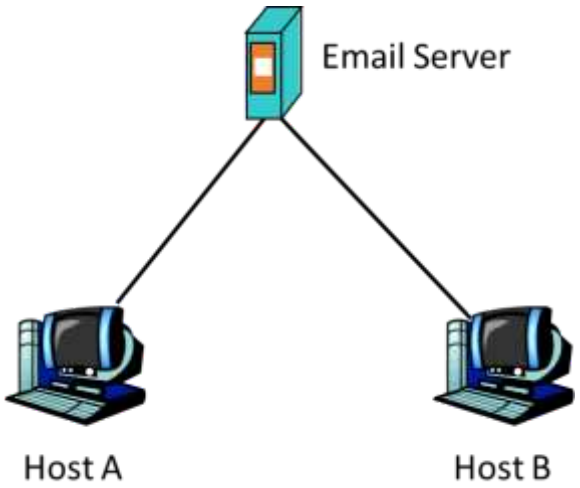
Attack Trees



1a. [3 pts] What's the cheapest attack (name and amount) that requires no special tools or skills?

1b. [3 pts] What's the cheapest and most expensive methods (name and amount) to Hack into Database?

1c. [4 pts] Suppose "Find Location of Server" now requires $50k rather than "no cost." Does this change any of the other two answers? If so, how.



The above diagram depicts a network inside ACME Corporation. Hosts A and B can communicate with the Email Server. Note: For these two problems, there are no other hosts available.

4a. [8 pts] Suppose Trudy has root access to Host A, and she wants to perform a port scan of Host B with sending as few as possible packets between Host A and B. Explain how Trudy can do this with the minimal possibility of being detected by ACME.
4b. [2 pts] What conditions are required in order to make this attack possible?

Session hijacking: Suppose Alice, Bob, and Trudy are connected to the same local switch. Alice has opened a telnet connection to Bob. Trudy knows that there's a telnet connection and wants to hijack the telnet connection.

2a. [4 pts] if Trudy **cannot** see the traffic, explain in detail (protocol level details) how Trudy can inject traffic into Bob and how difficult it is do that.
2b. [2 pts] Explain if two-way communication is possible between Trudy and Bob if Trudy **cannot** see the traffic.
2c. [6 pts] Answer 2a and 2b supposing that Trudy **can** see the traffic between Alice and Bob.

---

nmap:
3a. [10 pts] Using the standard nmap UDP scan, how does nmap decide if a port is open, closed, or filtered?
3b. [2 pts] Where does nmap fit in the network attack methodology?

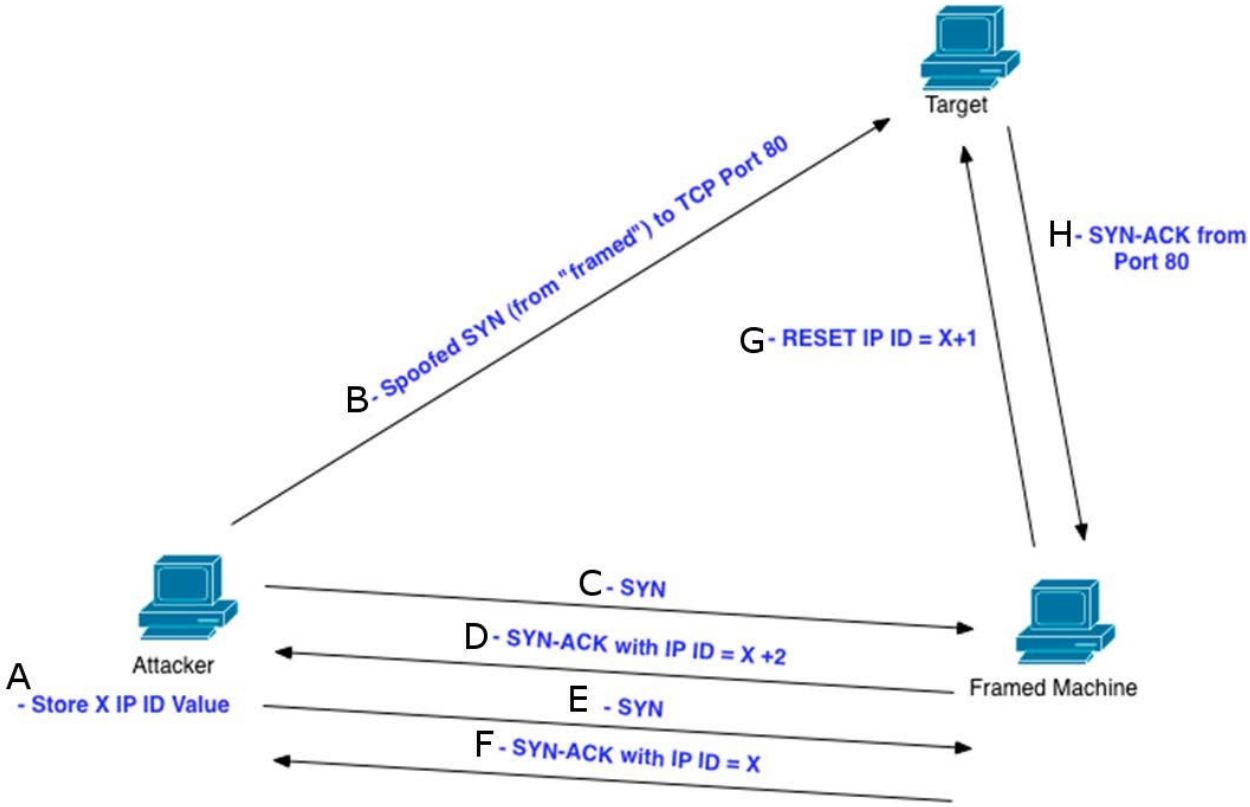
Attacks
2a. [3 pts] What is a technical way in which Trudy would obtain the email server's address (i.e., mail.acmecorporation.com) using DNS without being detected by ACME in any way? Explain.
2b. [3 pts] What kind of attack does Split DNS mitigate, and how does it do it?
2c. [3 pts] When using the nmap TCP ACK Scan, what is the meaning if a **RST** is returned for a port? 2d. [3 pts] What is the meaning if the response is **nothing**?

[6 pts] Using the standard nmap TCP SYN scan, how does nmap decide if a port is open, closed, or filtered?

Exploits: In the nmap scan option called FTP bounce scan:

3a. [4 pts] What vulnerability in FTP is being used by nmap for port scanning?
3b. [6 pts] Explain how this feature works and describe the possible outcomes.

Figure: nmap IDLE Scan



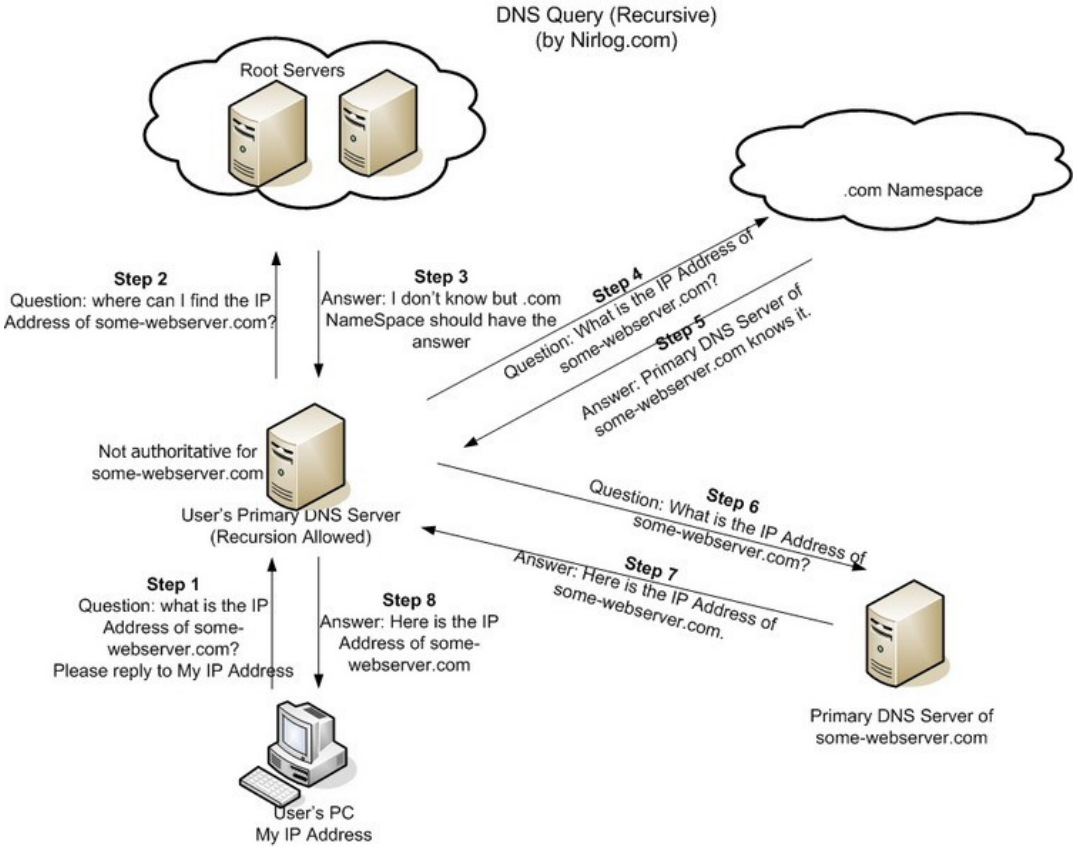
[8 pts] In the above illustration, place A-H in the correct sequence order.

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?

DNS Exploits: Remember that DNS queries are usually recursive, as shown in this diagram:



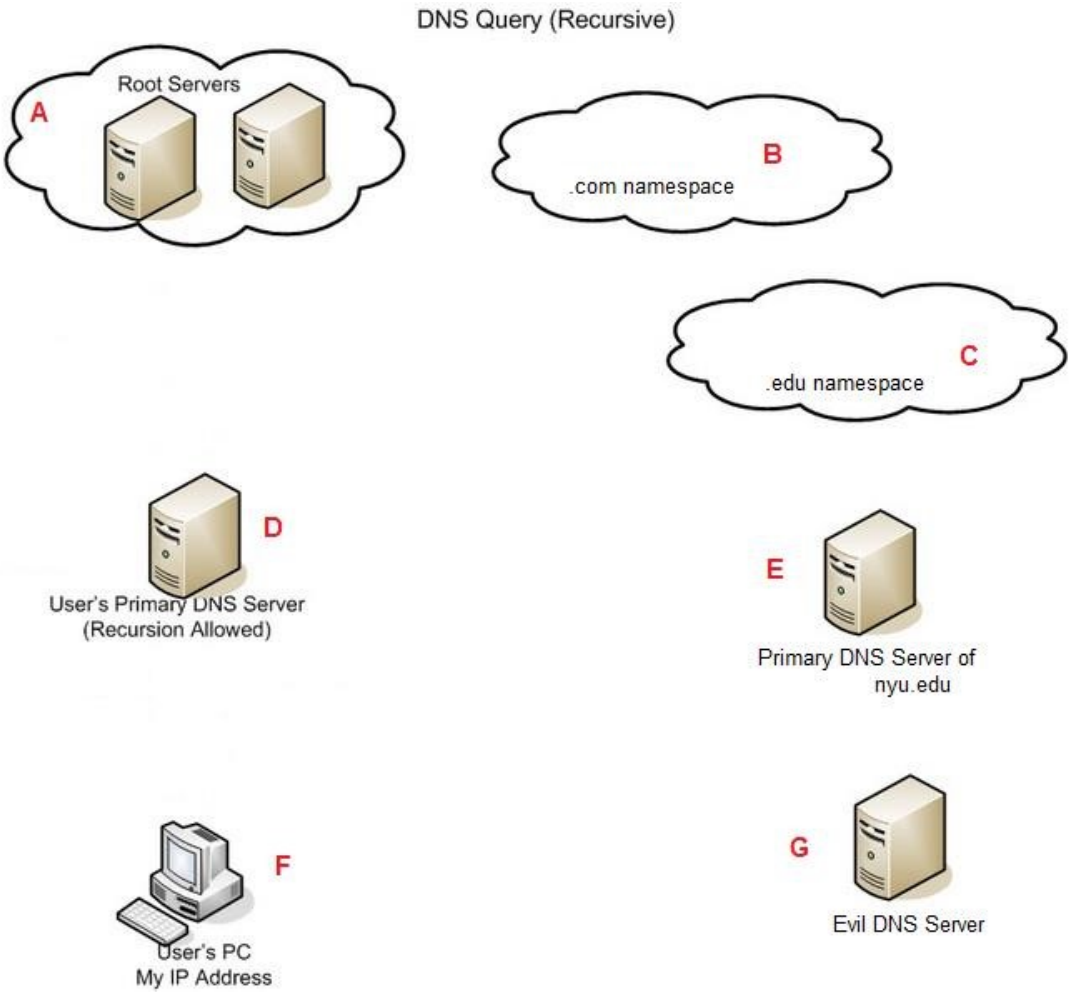
Suppose an attacker wants to perform DNS cache poisoning so the domain name acmecorporation.com is diverted it to a malicious website.

3a. [3 pts] Identify the step number(s) in the diagram in which the attacker can insert traffic to poison the DNS cache. Explain your answer.

3b. [6 pts] What are three issues that the attacker needs to overcome in order to successfully poison the DNS cache?

3c. [3 pts] Explain the main difficulty with using ingress filtering to prevent IP spoofing. Ingress filtering is only allowing subnets at the router that are supposed to be connected to the router.

DNS Cache Poisoning: The following diagram consist of the DNS architecture.



A is the Root Server
B is the DNS server for the .com Namespace
C is the DNS server for the .edu Namespace
D is the user's local DNS server (i.e., Comcast DNS Server)
E is the NYU DNS server
F is the user's PC
G is Trudy's Evil DNS Server

5a. [6 pts] Assume all caches are empty. Describe the communications required for the user (F) to find the IP address of engineering.nyu.edu using the DNS recursive method. *Hint: Your answer should look something like this:*
Step 1: F -> D: User makes a request her local DNS server Step 2: …

5b. [4 pts] Suppose Trudy was able to successfully poison the DNS cache of the user's primary DNS Server (D) to that it believes that the Primary DNS Server of nyu.edu is the Evil DNS Server (G). Describe how Trudy might have been able to achieve this.

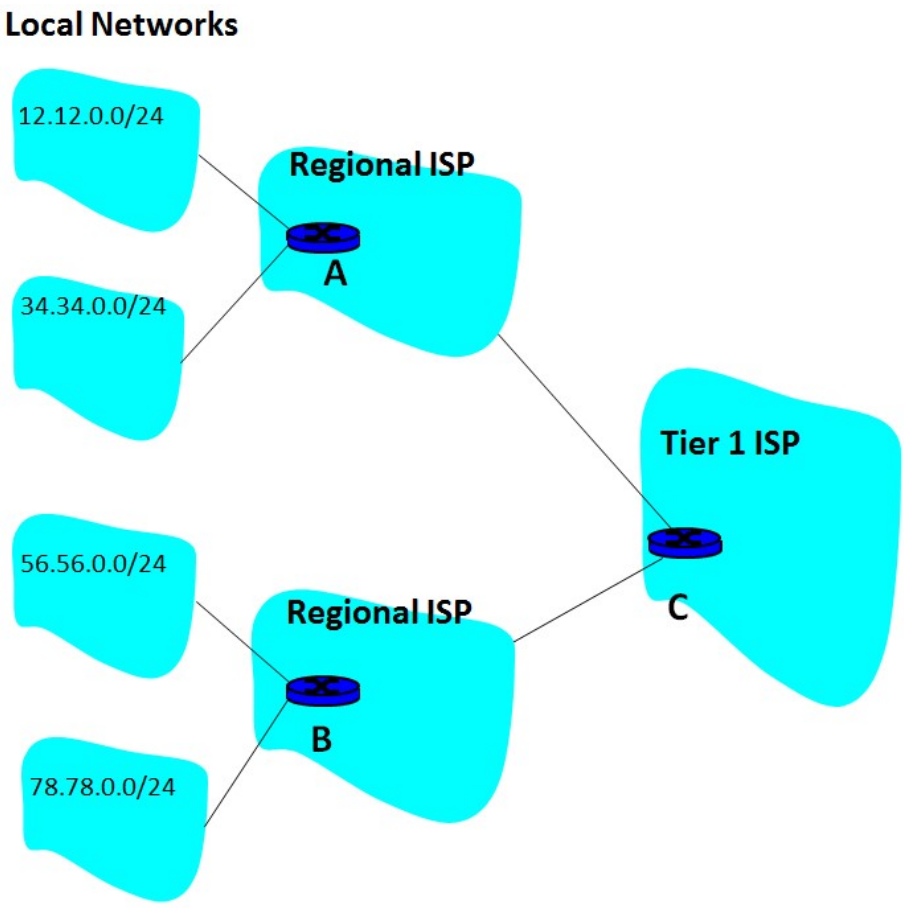
Network Time Protocol (NTP) is a common protocol used to sync the time between client and server. Windows PCs are set by default to sync the clock from a Microsoft NTP server. NTP operates on UDP

port 123. In normal usage, a client sends a request (packet size about 48bytes) to an NTP server for the time, and then the client listens for a response from the server. NTP also has a feature called “monlist” in which a client can request (packet size about 48bytes) a list that contains the last 600 hostnames with IP addresses of clients that have connected to that server. The NTP request also contains a 32-bit Reference ID that the server response must contain for the client to accept the response.

5a. [6 pts] Describe in detail three ways an attacker can abuse this protocol. Describe how difficult it would be to perform the attack.

5b. [4 pts] Describe in detail methods to stop an attacker from abusing this protocol.

Ingress Filtering



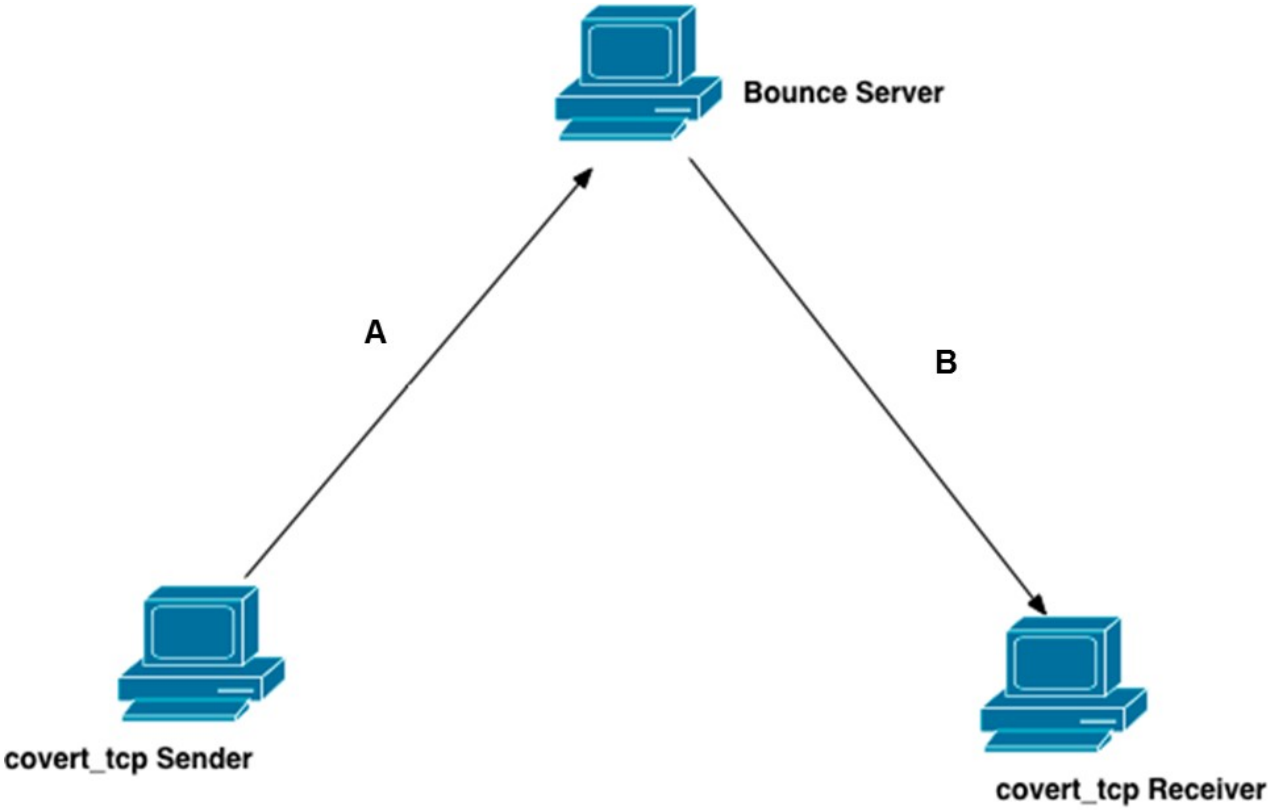
The networks depicted in the above diagram are implementing ingress filtering. The four networks on the left are the local networks (e.g., NYU), the middle two networks are regional ISPs, and the rightmost network is a Tier-1 ISP. The labels A, B, and C donate Routers in the respected networks that are 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?

5. [10 pts] This diagram represents the covert_tcp (TCP ACK Method) of transferring data fromone host to another.



Describe the method by which the "covert_tcp Sender" can send a message to "covert_tcp Receiver" using the Bounce Server. Include necessary details on the IP or TCP headers in order to explain your answer.

5a. [4 pts] Details of communications for label A.

5b. [6pts] Details of communications for label B.

---

3. **Covert Channels**: Suppose two hosts are communicating to each other using only pings. They have a covert channel set up by piggybacking on the ping echo requests and replies between the two hosts. There is no other communications between the two hosts.

4a. [6 pts] Describe three ways that a covert channel can be established using only fields in the ping header.
4b. [4 pts] Describe two ways that this can be detected and stopped.

1. **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.

---

6. Covert Channels: Trudy is an employee of ACME Corporation and wants to exfiltrate data out of the ACME to her server. Trudy has set up a DNS server ns.evil.com. ACME Corporation has a proxy/filtering server that ensures only legitimate DNS queries can be sent and received from the Internet.

6a. [4 pts] Explain how Trudy would be able to send information out of ACME to her DNS server using only the DNS protocol.

6b. [4 pts] Explain how Trudy would be able to receive information from her DNS server to ACME.

6c. [4 pts] How would ACME Corporation be able to stop Trudy from sending data? Receiving data?

Perform RSA key generation with *p=5* and *q=13*.
6a. [2 pts] Compute *n* and *φ*
6b. [2pts] 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=5* with the public key
6e: [2 pts] Are the values of the exponent *e* and exponent *d* a good choice? Why or why not?

Perform Diffie-Hellman shared key generation with *g=5*, *n=19*, Alice selects *a=5* as her secret, Bob selects *b=6* 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. Cipher Block Chaining (CBC)

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

8a. [3 pts] If Trudy intercepted Ciphertext 001110110011 from Alice to Bob and she knows that Cipher Block Chaining (CBC) is not used, what can she figure out about the message?
8b. [3 pts] Decrypt 001110110011 without CBC
8c. [6 pts] Decrypt 001110110011 using CBC and IV=1010

Vignere

7a. [4] Using the standard Vignere (Vigenere) (Poly-alphabetic Encryption) table, decrypt the message HEFF using the key CAB.

7b. [2] Does the table in Vignere need to be kept secret for this cryptographic scheme to work?

Perform RSA key generation with p=3 and q=11. Note: you must show work for any modular mathematics.

8a. [2 pts] Compute n and ϕ

8b. [2 pts] Choose the smallest possible public (encryption) exponent e

8c. [4 pts] Choose a private (decryption) exponent d

8d. [4 pts] Encrypt the plaintext message m=6 with the public key

8e: [2 pts] Is RSA the preferred or non-preferred choice for encrypting large messages? Explain why.

Perform Diffie-Hellman shared key generation with g=2, n=11, Alice selects a=9 as her secret, Bob selects b=4 as his secret. Note: you must show work for any modular mathematics.

9a. [3 pts] Calculate Alice's public key A

9b. [2 pts] Calculate Bob's public key B

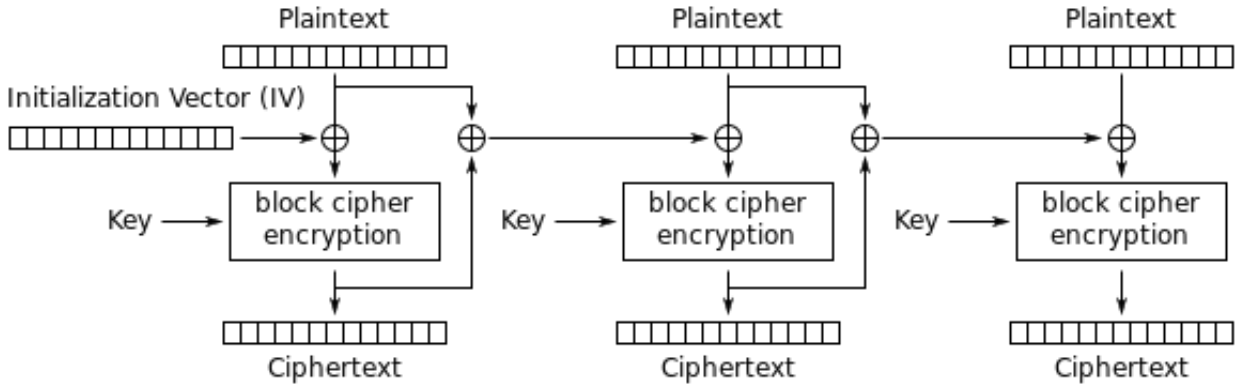
9c. [4 pts] Calculate the shared key K

9d. [3 pts] What values are publically shared between Alice and Bob?

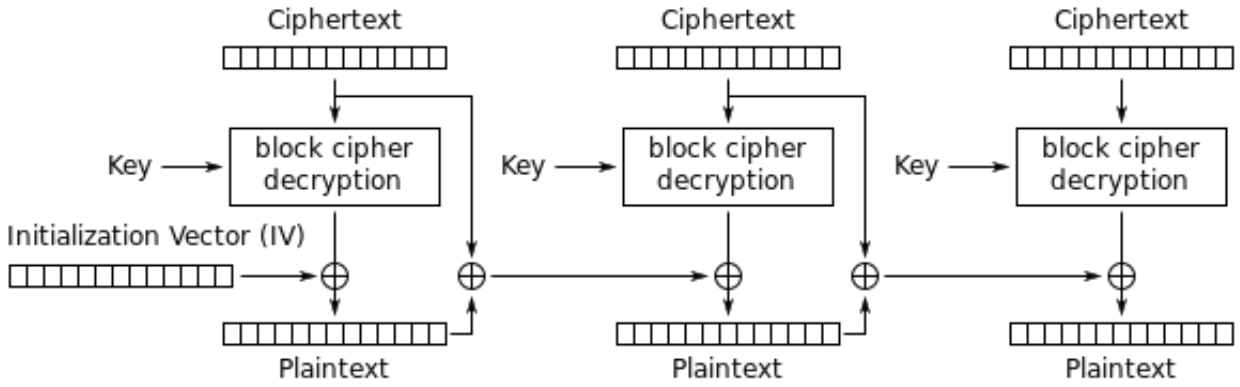
Block Cipher Mode of Operations

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 Propagating cipher-block chaining (PCBC), a similar mode of operation to CBC.



Propagating Cipher Block Chaining (PCBC) mode encryption



Propagating Cipher Block Chaining (PCBC) mode decryption

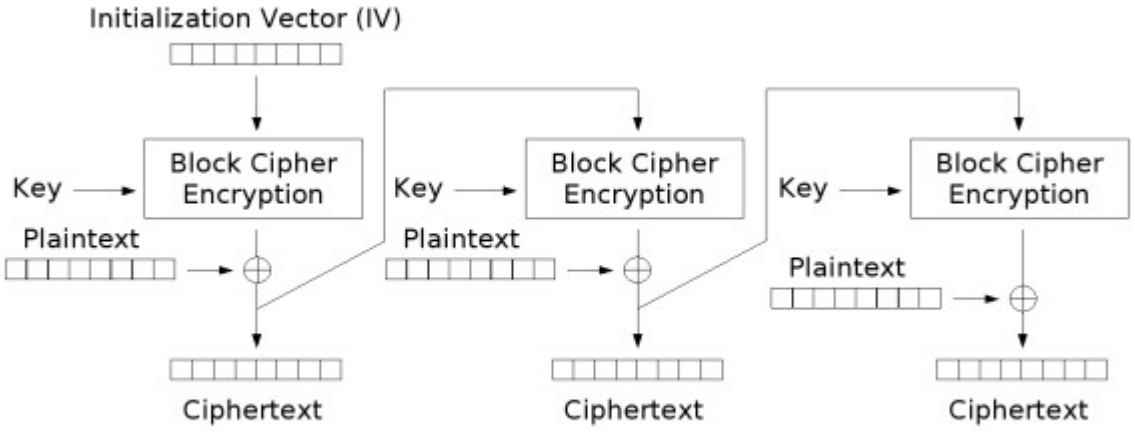
10a. [3 pts] If Trudy intercepted Ciphertext 001110110011 from Alice to Bob and knows that CBC is used, can she easily figure out that blocks are repeating?

10b. [3 pts] Decrypt Ciphertext 001110110011 without using any mode

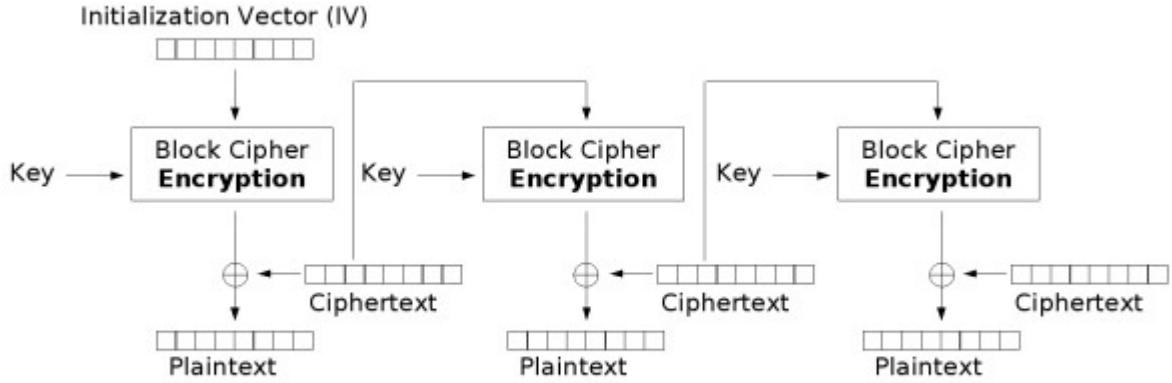
10c. [6 pts] Decrypt Ciphertext 001110110011 using PCBC and IV=1010

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

Perform RSA key generation with p=5 and q=11. Note: you must show work for any modular mathematics.

5a. [2 pts] Compute n and φ
5b. [2 pts] Choose the smallest possible public (encryption) exponent e
5c. [3 pts] Choose a private (decryption) exponent d
5d. [2 pts] Encrypt the plaintext message m=25 with the public key
5e. [3 pts] Decrypt your solution in part d to obtain the original message m=25
5f: [2 pts] What mathematical property provides the security of RSA encryption?

Perform Diffie--Hellman shared key generation with g=6, n=17, Alice selects a=5 as her secret, Bob selects b=11 as his secret. Note: you must show work for any modular mathematics.

6a. [3 pts] calculate Alice's public key A
6b. [2 pts] calculate Bob's public key B
6c. [4 pts] calculate the shared key K
6d. [3 pts] In the Diffie--Hellman exchange, what values can Trudy see, and what values she cannot?

Block Cipher Mode of Operations: Suppose you have an encryption function as follows, with block size of five bits:

Encryption: c(m) = m XOR *11000*

Decryption: m(c) = c XOR *11000* For example, for plaintext message m=10101, the ciphertext c would be 01101.

7a. [3 pts] Does the IV in Cipher Block Chaining (CBC) need to be kept a secret? Explain why or why not.
7b. [3 pts] Decrypt Ciphertext 000110001100011 without using any mode
7c. [6 pts] Decrypt Ciphertext 000110001100011 using CBC and IV=10110

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.

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?

RSA: Perform RSA key generation with p=3 and q=19. Note: you must show work for any modular mathematics.

7a. [2 pts] Compute n and φ

7b. [2 pts] Find the five smallest possible values for public (encryption) exponent e

7c. [4 pts] Using the smallest e from 7b, choose a private (decryption) exponent d

7d. [4 pts] Encrypt the plaintext message m=20 with the public key

7d: [2 pts] What's the recommended size of the modulus, n, be in today's standards?

DH: Perform Diffie-Hellman shared key generation with g=7, n=13, Alice selects a=4 as her secret, Bob selects b=5 as his secret.

8a. [3pts] calculate Alice's public key A

8b. [2pts] calculate Bob's public key B

8c. [4pts] calculate the shared key K

8d. [3pts] Why is Diffie-Hellman preferred over RSA for generation of bulk encryption keys?

Cipher Block Chaining (CBC)

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

9a. [3 pts] If Trudy intercepted Ciphertext 100110011001 from Alice to Bob and she knows that Cipher Block Chaining (CBC) is used, what can she figure out about the message?
9b. [3 pts] Decrypt 100110011001 without CBC
9c. [6 pts] Decrypt 100110011001 using CBC and IV=0101

Scapy: Explain what the following scapy command do:
[4 pts] send(IP(dst="10.10.111.1",ttl=10)/ICMP()) 8b. [4 pts] sr(IP(dst="10.10.111.0/24")/TCP(dport=(80,81))) See attached file below for a reference on scapy.

[4 pts] send(Ether()/IP(src=RandIP(),dst="10.10.111.1")/TCP(dport=80))
[4 pts] sr1(IP(dst="10.10.111.0/24")/TCP(dport=(1,100),flags="A"))
[4 pts] ans,unans = sr(IP(dst="10.10.111.0/24", ttl=5)/TCP(dport=139), timeout=1)
ans.nsummary()
unans.nsummary()

Miscellaneous
[2 pts] Encrypt "HELLO WORLD" with Julius Ceasar's Cipher of key 5 (positive 5). 9b. [4 pts] Define what a chosen-plaintext attacks is.
[4 pts] What attack does SYN Cookies mitigate? How does it do that?
[4 pts] What is Split DNS and what attack is and what it's intended to mitigate?
[4 pts] Describe the main reason that an attacker might want install a Reverse WWW Shell onto a target's computer.
[4 pts] Using the standard Vigenere (Poly--alphabetic Encryption) table, decrypt the message LLMN using the key CDB. Show work or explain.
[4 pts] Discuss how is DNS amplification attack similar to NTP amplification attack?
[4 pts] What are the differences between the nmap Connect scan and SYN Scan?
[4 pts] Using the Julius Caesar's Cipher, the plaintext message "HELLO" is encrypted to the ciphertext "XUBBE". What is the key used?