Midterm Solutions:

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)?

Answer: SLE = 5 * ($1000 + $200) = $6000

1b. [2 pts] What's the Annualized Rate of Occurrence (ARO)?

Answer: ARO = 0.5

1c. [2 pts] What's the Annualized Loss Expectancy (ALE)?

Answer: ALE = SLE * ARO = $6000 * 0.5 = $3000

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.

Two possible answers: YES, because it's worth it because ACME will save money in five years **OR** NO, because in five years there'll be more and difference vulnerabilities.

Year	Cost w/ FW	Cost w/o FW
1	$11k	$3k
2	$12k	$6k
3	$13k	$9k
4	$14k	$12k
5	$15k	$15k

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)?

Answer: SLE = $1,500K + $500K = $2,000K

1b. [2 pts] What's the Annualized Rate of Occurrence (ARO)?

Answer: ARO = 0.25

1c. [2 pts] What's the Annualized Loss Expectancy (ALE)?

Answer: ALE = SLE * ARO = $2,000K * 0.25 = $500K

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?

Two possible answers:

1. No, it's not worth it because the cost is the same, so it does not make any business sense.
2. Yes, it would be worth it because it reduces the overall risk of the system.

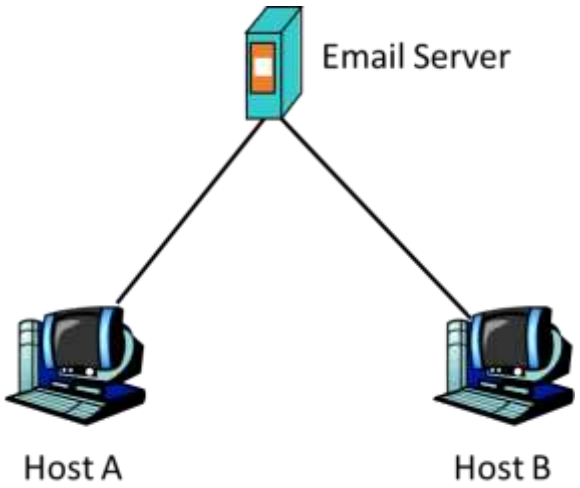
Risk Assessment: ACME Corporation has a corporate intranet where software for medical devices are being developed. ACME wants to secure the network by upgrading the firewall and installing an intrusion detection and monitoring program. The cost of the upgrade is a one-time fee of $300k with

$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)?
Answer: SLE = $100K
1b. [2 pts] What's the Annualized Rate of Occurrence (ARO)?
Answer: ARO = 2
1c. [2 pts] What's the Annualized Loss Expectancy (ALE)?
Answer: ALE = SLE*SRO = $200K
1d. [2 pts] Would upgrading the security of the network be worth it? Why or why not?
Two possible answers: • Yes: For an investment in the new security system, it would start saving the company money in three years. • No: The investment will only be worth it after three years, and there's no guarantee that the new firewall will thwart future threats

---

Lecture 2 – Network Reconnaissance



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.
Answer: If Trudy is unable to see the traffic, then she would be extremely difficult to inject traffic into the telnet connection as she would be to properly guess the sequence numbers. Trudy would need to inject blind packets into the network with a very small chance of success.

2b. [2 pts] Explain if two-way communication is possible between Trudy and Bob if Trudy **cannot** see the traffic.
Answer: If Trudy cannot see the packets, then two way communications is near impossible. Theoretically, it is possible to establish a reverse shell if you can't see the traffic if Trudy can successfully inject a reverse shell code into the hijacking packet. But it's certainly very difficult, to near impossible.
2c. [6 pts] Answer 2a and 2b supposing that Trudy **can** see the traffic between Alice and Bob.
Answer: For 2a: If Trudy can see the traffic, then she can see the sequence numbers and thus it'll be very easy for her to inject traffic. For 2b: Two-way communications is usually very easy if Trudy can see the traffic.

---

nmap:

3a. [10 pts] Using the standard nmap UDP scan, how does nmap decide if a port is open, closed, or filtered?

Answer:

- OPEN: If a host reply with any data in the packet than it is clear that the port is open.
- CLOSED: If a packet is sent to a particular port and it replies with port unreachable then it is clear that the port is closed.
- OPEN or FILTERED: But if there is no reply from the host than the port might be open or it might be filtered.

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.

Answer: Use DNS to lookup the MX Record.

2b. [3 pts] What kind of attack does Split DNS mitigate, and how does it do it?

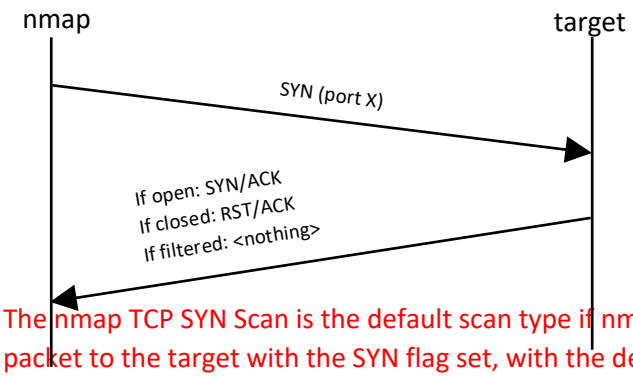
Answer: Split DNS mitigates the DNS Brute Force Forward Attack which allows an attacker to bruteforce subdomain names via a wordlist. Split DNS mitigates this by having an Internal DNS server which stores subdomains only used internally, and having an External DNS server for external users only for front facing subdomains.

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**?

Answer: The port is not filtered by a firewall. Any hosts will respond with a RST to an unsolicited TCP ACK whether the port is open or not.

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

Answer: TCP SYN Scan



The nmap TCP SYN Scan is the default scan type if nmap as root/admin rights. nmap will send a TCP packet to the target with the SYN flag set, with the destination port set to X. nmap will repeat this for each port.

Open: If the port is open, the target will respond with a SYN/ACK, meaning that host is trying to establish a connection

Closed: If the port is closed, the target will respond with a RST/ACK

Filtered: If the port is filtered, then the target will respond with nothing or with an ICMP unreachable

---

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?

Answer: nmap is exploiting a feature in FTP that allows the FTP server to send a file to a remote host. This allows for nmap to scan a target without the target knowing who scanned it.

3b. [6 pts] Explain how this feature works and describe the possible outcomes.
Answer: nmap would connect to a FTP server that's vulnerable (that is, has this feature enabled), and use the "port" command to try to list directory. If target is listening on the port it will respond with a 150 or 226 response. If the port is not listening or closed it will respond with "425 Can't build data connection: Connection refused." Port numbers and command name not required for full points.

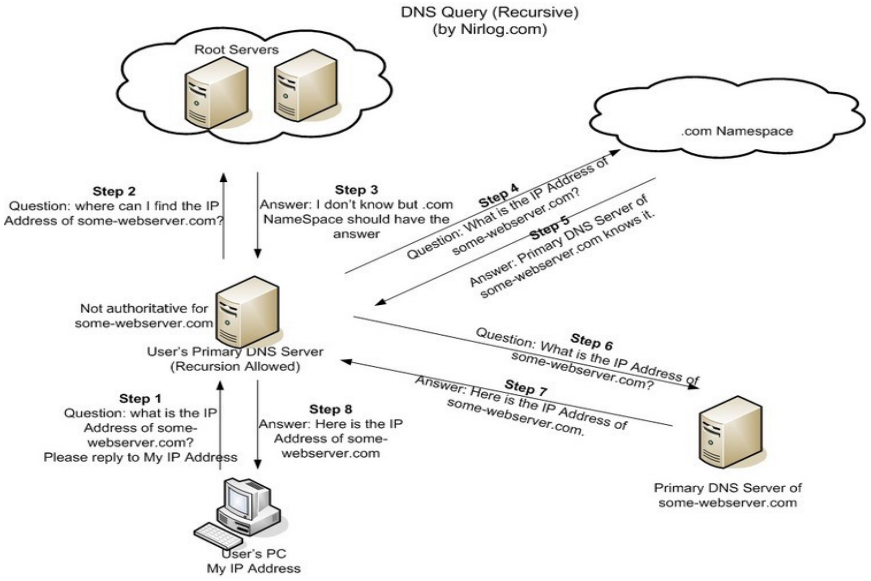
DNS Reconnaissance: Suppose an attacker is performing reconnaissance on ACME Corporation using only the DNS protocol.

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.

DNS Recon	Possible types of information obtained
Standard DNS Request	Examples: A (IPv4 Address), AAAA (IPv6 Address), MX (mail server), NS (name server), et al. Full credit entails understanding that information like this can be obtained from DNS
Brute-force Forward DNS	Trying DNS requests on different URLs, such as ftp.nyu.edu and see if it works. This can obtain information about other hosts on the network
DNS Zone Transfer	If successful, will obtain all the records on DNS server

2b. [4pts] What are two mitigation strategies to minimize what an attacker can obtain from using DNS?
No answer provided.

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.

Answer: Steps 3, 5, 7, and 8. The attacker can potentially insert or modify any response to a DNS request.

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

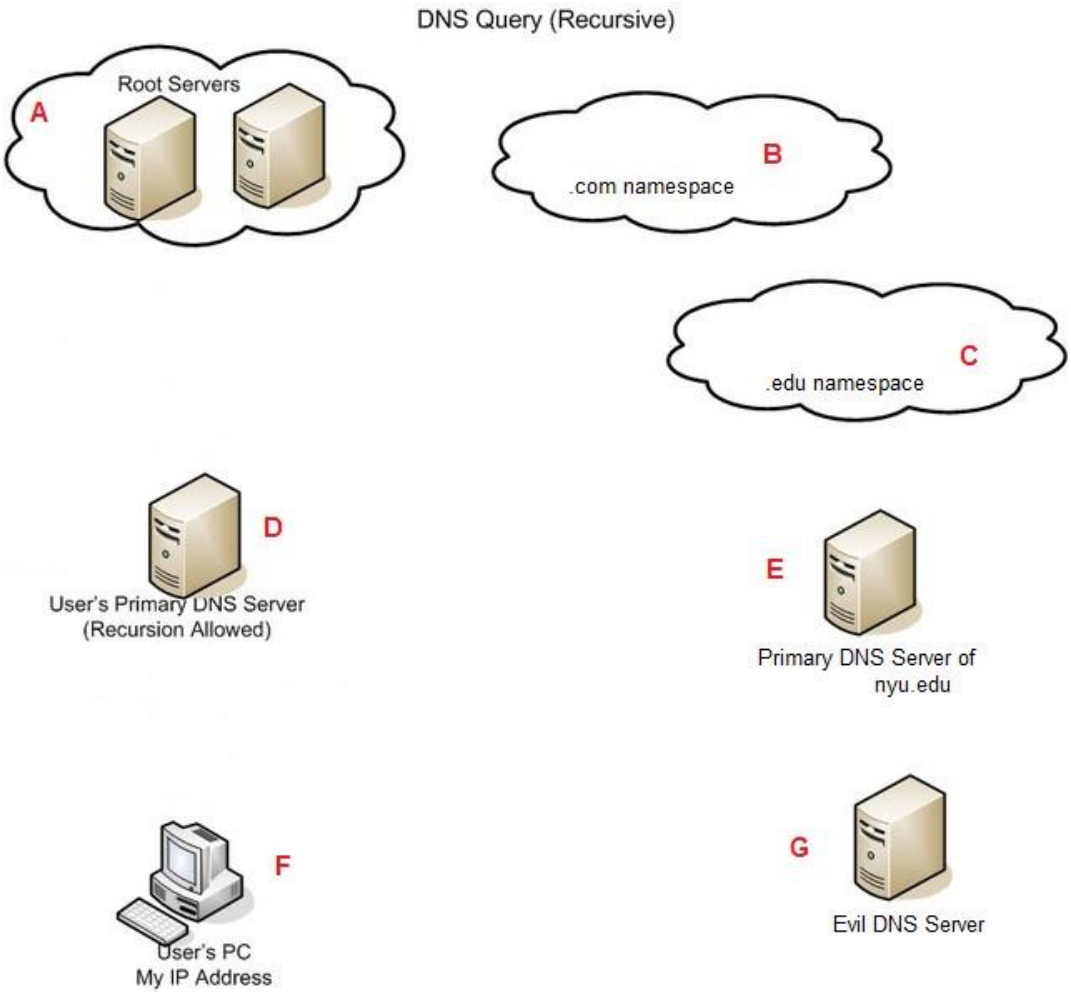
Answer:

1. Timing: the DNS response must be before the actual server responds.
2. Transaction ID (sequence number): the DNS transaction ID must match with the one in the request
3. Spoof IP Address of Server: the source IP address must be from the DNS server

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.

Answer: The difficulty is that ingress filtering must be implemented at all levels of the network as IP spoofing can always occur at a sub-network.

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: …
Answer:
• Step 1: F -> D: User makes a request her local DNS server • Step 2: D -> A • Step 3: A -> D • Step 4: D -> C • Step 5: C -> D • Step 6: D -> E • Step 7: E -> D • Step 8: D -> F

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.
Answer: Trudy can successfully poison the cache of the user's primary DNS server by replying back to any queries by the server in steps 3, 5, or 7. Trudy will need to (1) reply faster; (2) match the Transaction ID; and (3) spoof the source IP.

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.

Answer:

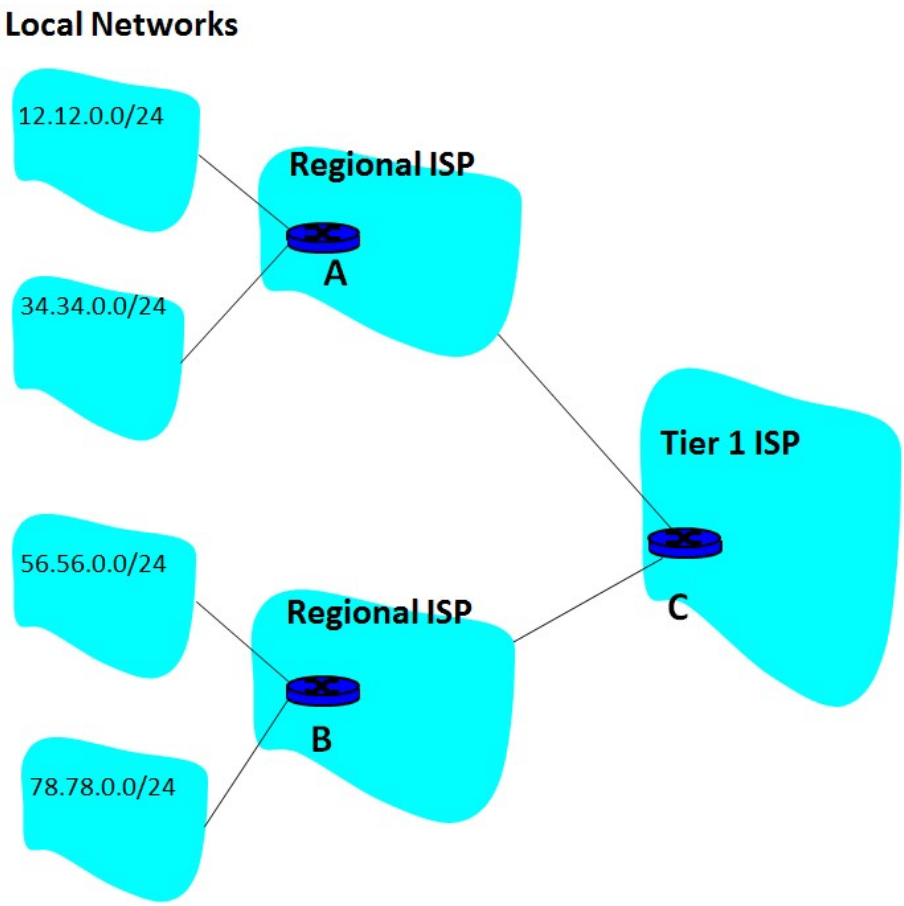
Abuse	Difficulty
1. Recon: Obtain a list of the last 600 IP/hostnames	Easy. No explanation needed.
2. Perform a DDOS attack by using 'monlist' feature. Spoof source IPs using the target as destination IP. Request size: 48-234 bytes; Response size: ~48kb	Spoofing IPs is easy. Need to deal with ingress filters.
3. Intercept a request and reply with the incorrect time to mess up server time syncs. Will mess up logging.	Easy: If on the same LAN Very Hard: Not on same LAN
4. Covert channel: encoding information into the Reference ID, or source IP or hostname. Either the NTP server or another client will retrieve the information.	Not terribly difficult. Attacker will need to control a DNS server to encode hostname

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

Answer:

1. Disable 'monlist', or filter it out using a Firewall
2. Use authentication for the request/response

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.

Answer: Ingress filtering is an IP address filtering technique that ensures that source IP addresses are coming from networks that they are supposed to be coming from. It is attempting to prevent IP source address spoofing.

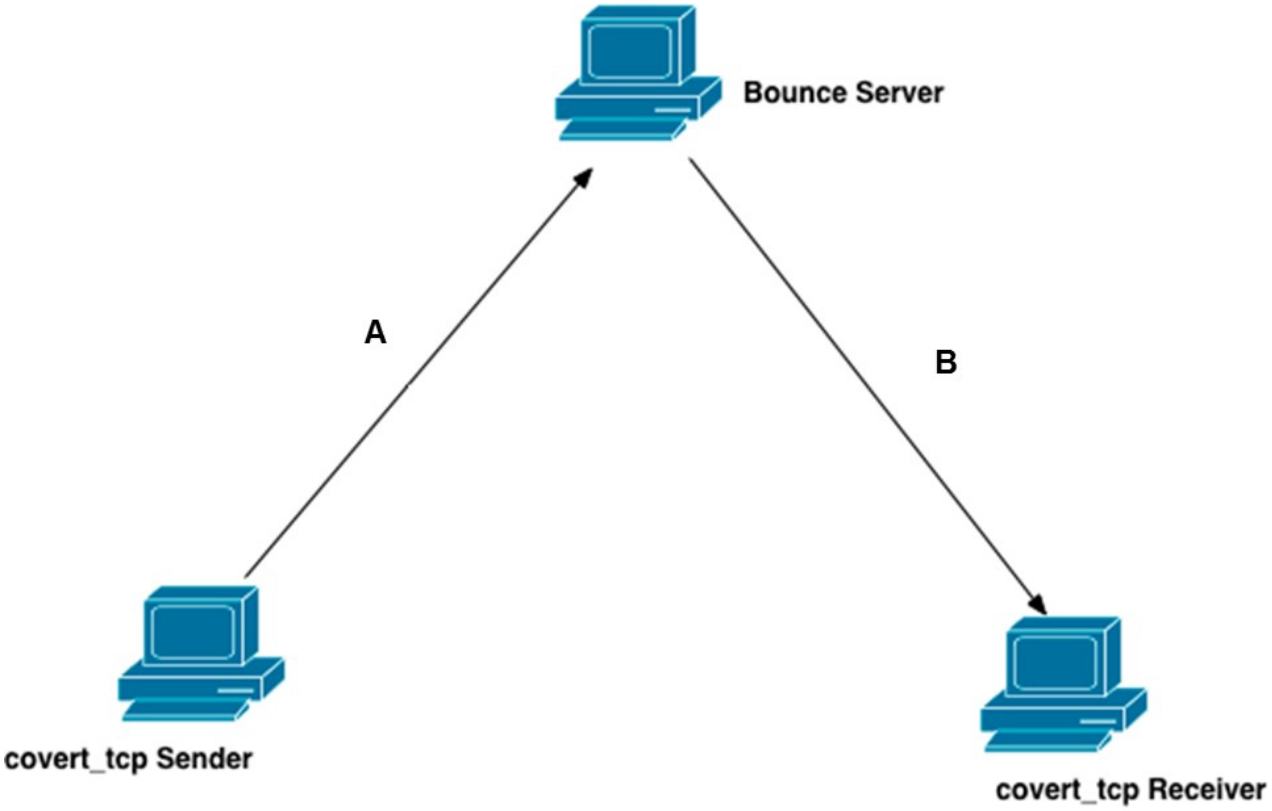
8b. [4 pts] If ingress filtering is implemented for Router C, what addresses what it filter or not filter? What address can still bypass the filtering?

Answer: If ingress filtering is on Router C, then it should filter all address except for 12.12.0.0/24, 34.34.0.0/24, 56.56.0.0/24, and 78.78.0.0/24. Any other IP source packet not from those networks would be filtered, however, spoofed address can still bypass the filter because the downstream networks (i.e., the network where Router A and B are in) are not perform ingress filtering and thus there can be spoofing performed within the downstream networks. For example, a host in the 12.12.0.0/24 network can spoof a source address 34.34.1.1.

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?

Answer: Router A would filter everything except 12.12.0.0/24 and 34.34.0.0/24, while Router B would filter everything except 56.56.0.0/24 and 78.78.0.0/24. There can still be spoofed addresses inside the local networks. For example, a host inside the 12.12.0.0/24 network can still spoof another address in the 12.12.0.0/24 network.

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. The Sender sends a packet with the IP source spoofed as the Receiver, and Destination to be the Bounce Server. The TCP SYN flag is set, with a ISN set to (ASCII# - 1).

5b. [6pts] Details of communications for label B.
The Bounce Server will receive the packet, and will reply to the Receiver because the source address was spoofed. There are two possible responses:
1. SYN/ACK(ASCII# - 1 + 1)
2. RST/ACK(ASCII# - 1 + 1)
In either case, the ASCII# is successfully transmitted to the Receiver.

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. **Any three of the following is full points:**

1. Use the data field in the ping which allows arbitrary data.
2. Changing the fields such as identifier and sequence number to a secret message. For example, "A" can be encoded to ASCII number 65 and inserted into the field.
3. A ICMP echo-reply is supposed to put the echo-request packet into the reply. If the source IP is spoofed, then the ping can be bounced off a bounce server.
4. Using frequency or timing. For example, one ping could mean an "A" while two pings could mean a "B".

4b. [4 pts] Describe two ways that this can be detected and stopped.

1. Check the data field and drop packets with ping payload data. This is hard because it will likely break ping.
2. Check the fields in the icmp header to make sure the sequence number begins at 0 and increments as it's supposed to.

---

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. Flags (Urgent, push), ISN, covert_tcp ACK # method, strange freqnency or timing

3b. [4 pts] Discuss two ways that this can be detected and potentially stopped. Look for patherns in the flags, non-random ISN.

---

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. Trudy can spoof the address to be looked up, i.e., DNS lookup A record "this_is_my_secret_message.evil.com"

6b. [4 pts] Explain how Trudy would be able to receive information from her DNS server to ACME. Trudy can receive information from any DNS records such as A (123.123.123.123) or TXT ("secret message").

6c. [4 pts] How would ACME Corporation be able to stop Trudy from sending data? Receiving data? ACME can look for DNS queries/responses when the user did not actually visit the page.

Perform RSA key generation with $p=5$ and $q=13$.

6a. [2 pts] Compute n and φ

Answer:

$n = pq = 5 * 13 = 65$

$\varphi = (p-1)(q-1) = (5-1)(13-1) = (4)(12) = 48$

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

Answer:

Find e such that:

$1 < e < \varphi$;

GCD(e, φ)=1

Not possible e: 1, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 19, …

Possible e: 5, 7, 11, 13, 17, 19, …

Choose e=5

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

Answer:

$ed \bmod \varphi = 1$ or $(ed - 1) \bmod \varphi = 0$

$e = 5$; $\varphi = 48$

$5d \bmod 48 = 1$

Try k = (5d-1)/48; d = (48k+1)/5, for k = 1, 2, 3, ...

k=1; d=49/5 ... **NO**

k=2; d=(48(2)+1)/5 = 97/5 ... **NO**

k=3; d= (48(3)+1)/5 = 145/5 = 29 ... **YES**

Choose d = 29

6d. [4 pts] Encrypt the plaintext message $m=5$ with the public key

Answer:

$c = m^e \bmod n = (5)^5 \bmod 65 = 5$

Check your work: $m = c^d \bmod n = 5^{29} \bmod 65 = 5$

(*required if you made a math mistake*)

$5 \bmod 65 = 5$

$5^2 \bmod 65$

$= ((5^1 \bmod 65)(5^1 \bmod 65)) \bmod 65$

$= ((5)(5)) \bmod 65 = 25 \bmod 65$

$= 25$

$5^4 \bmod 65$

$= ((5^2 \bmod 65)(5^2 \bmod 65)) \bmod 65$

$= ((25)(25)) \bmod 65 = 625 \bmod 65$

$= 40$

$5^5 \bmod 65$

$= ((5^1 \bmod 65)(5^4 \bmod 65)) \bmod 65$

$= ((5)(40)) \bmod 65 = 200 \bmod 65$

$= 5$

6e: [2 pts] Are the values of the exponent e and exponent d a good choice? Why or why not?

Answer: No, because these values of e, d make the ciphertext the same as the plaintext. Also, they're small.

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*

Answer: $A = g^a \bmod n = 5^5 \bmod 19 = 9$

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

Answer: $B = g^b \bmod n = 5^6 \bmod 19 = 7$

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

Answer:

$K_A = B^a \bmod n = 7^5 \bmod 19 = 11$

$K_B = A^b \bmod n = 9^6 \bmod 19 = 11$

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?

Answer: Values are too small. Trudy will see that and attempt to brute force. DH has a complexity of $\sqrt{2} * \log(n)$

---

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?

Answer: There are probably repeating blocks, namely the 1st and 3rd block.

8b. [3 pts] Decrypt 001110110011 without CBC

Answer:

dec(0011) = 1100

dec(1011) = 0100

dec(0011) = 1100

8c. [6 pts] Decrypt 001110110011 using CBC and IV=1010

Answer:

CBC Mode Decryption

Plaintext 1 = dec(Ciphertext 1) ⊕ IV = dec(0011) ⊕ 1010 = 1100 ⊕ 1010 = 0110

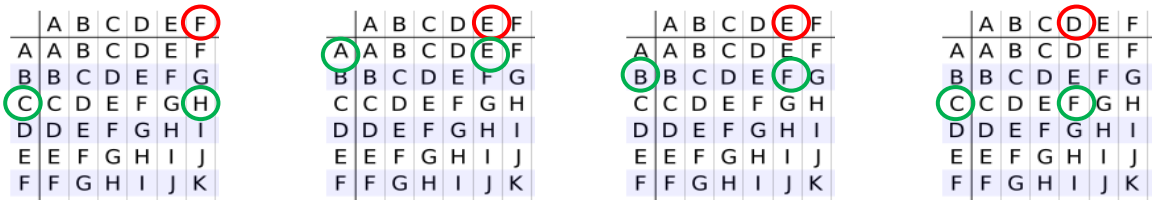
Plaintext 2 = dec(Ciphertext 2) ⊕ Ciphertext 1 = dec(1011) ⊕ 1011 = 0100 X 0011 = 0111

Plaintext 3 = dec(Ciphertext 3) ⊕ Ciphertext 2 = dec(0011) ⊕ 1011 = 1100 X 1011 = 0111

Vignere

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

Answer:



The table was not given, but it's trivial to recreate the table yourself.
Decrypt H: Lookup Row C / Cell H => Column F
Decrypt E: Lookup Row A / Cell E => Column E
Decrypt F: Lookup Row B / Cell F => Column E
Decrypt F: Lookup Row C / Cell F => Column D
Answer: FEED

7b. [2] Does the table in Vignere need to be kept secret for this cryptographic scheme to work?
Two possible answers, depending on explanation: Either the "key" (CAB) or the "table" must be kept secret. Typically, it's the "key" (CAB) that is kept secret.
No. The table in this case is the encryption engine. As long as the key "CAB" is kept secret, then the table does not need to be kept secret.

- or -

Yes. The table is the "key" used to decrypt the message. If the table is kept secret, then the encryption engine "CAB" does not need to be secret.

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
Answer:
$n = pq = 3 * 11 = 33$
$\varphi = (p-1)(q-1) = (3-1)(11-1) = (2)(10) = 20$
8b. [2 pts] Choose the smallest possible public (encryption) exponent e
Answer:
Find e such that:

$1 < e < \varphi$;
GCD(e, φ)=1

Not possible *e*: 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18
Possible *e*: 3, 7, 9, 11, 13, 17, 19
Choose *e*=3
8c. [4 pts] Choose a private (decryption) exponent d
Answer:
$ed \bmod \varphi = 1$ or $(ed - 1) \bmod \varphi = 0$

$e = 3$; $\varphi = 20$
$3d \bmod 20 = 1$
Try d=1 => 3(1) mod 20 ?= 1 ... **NO**
d=2 => 3(2) mod 20 ?= 1 ... **NO**
d=3 => 3(3) mod 20 ?= 1 ... **NO**
d=4 => 3(4) mod 20 ?= 1 ... **NO**
d=5 => 3(5) mod 20 ?= 1 ... **NO**
d=6 => 3(6) mod 20 ?= 1 ... **NO**
d=7 => 3(7) mod 20 ?= 1 ... **YES**

Choose d=7

8d. [4 pts] Encrypt the plaintext message m=6 with the public key
Answer: $c = m^e \bmod n = (6)^3 \bmod 33 = 18$
Check your work: $m = c^d \bmod n = 18^7 \bmod 33 = 6$ (*required if you made a math mistake*)
8e: [2 pts] Is RSA the preferred or non-preferred choice for encrypting large messages? Explain why.
Answer: RSA is not preferred for encrypting large messages using RSA to encrypt messages is excruciatingly slow. Generating RSA key pairs is also very slow (~5 seconds).

$6 \bmod 33 = 6$
$6^2 \bmod 33 = ((6 \bmod 33)(6 \bmod 33)) \bmod 33 = ((6)(6)) \bmod 33 = 36 \bmod 33 = 3$

$6^3 \bmod 33 = ((6 \bmod 33)(6^2 \bmod 33)) \bmod 33 = ((6)(3)) \bmod 33 = 18 \bmod 33 = 18$
$5 \bmod 11 = 5$

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
Answer: $A = g^a \bmod n = 2^9 \bmod 11 = 6$
9b. [2 pts] Calculate Bob's public key B
Answer: $B = g^b \bmod n = 2^4 \bmod 11 = 5$
9c. [4 pts] Calculate the shared key K
Answer:
$K_A = B^a \bmod n = 5^9 \bmod 11 = 9$
$K_B = A^b \bmod n = 6^4 \bmod 11 = 9$
9d. [3 pts] What values are publicly shared between Alice and Bob?
Answer: A, g, n, B (everything except for a, b)

$2 \bmod 11 = 2$
$2^2 \bmod 11 = ((2 \bmod 11)(2 \bmod 11)) \bmod 11 = ((2)(2)) \bmod 11 = 4 \bmod 11 = 4$
$2^4 \bmod 11 = ((2^2 \bmod 11)(2^2 \bmod 11)) \bmod 11 = ((4)(4)) \bmod 11 = 16 \bmod 11 = 5$
$2^8 \bmod 11 = ((2^4 \bmod 11)(2^4 \bmod 11)) \bmod 11 = ((5)(5)) \bmod 11 = 25 \bmod 11 = 3$
$2^9 \bmod 11 = ((2^8 \bmod 11)(2 \bmod 11)) \bmod 11 = ((3)(2)) \bmod 11 = 12 \bmod 11 = 6$

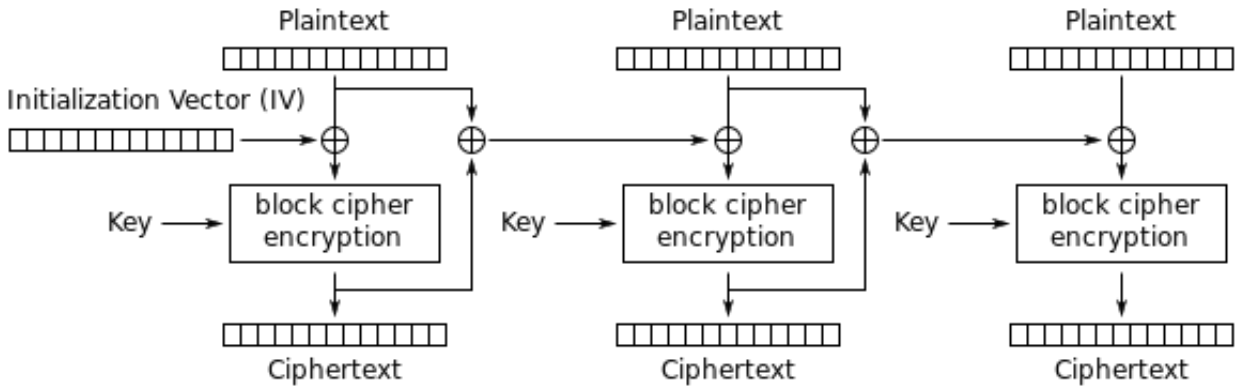
$5^2 \bmod 11 = 5*5 \bmod 11 = 25-22=3$
$5^4 \bmod 11 = 3*3 \bmod 11 = 9$
$5^8 \bmod 11 = 81 \bmod 11 = 81-77 = 4$
$5^9 \bmod 11 = 4*5 \bmod 11 = 20-11 = 9$

$6 \bmod 11 = 6$
$6^2 \bmod 11 = 36 \bmod 11 = 36-33 = 3$
$6^4 \bmod 11 = 9 \bmod 11 = 9$

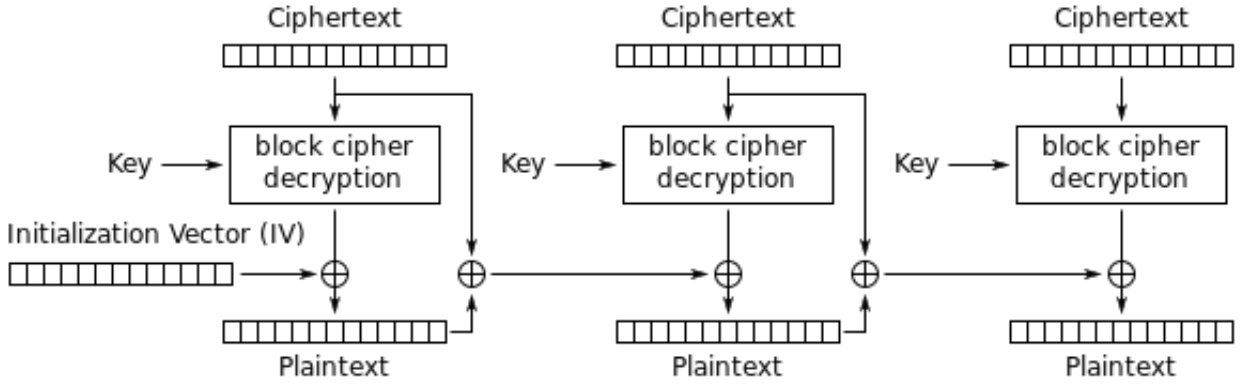
Block Cipher Mode of Operations

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 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?

Answer: No, since CBC is used, Trudy cannot easily see if there are repeating blocks.

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

Answer:

dec(0011) = 0100

dec(1011) = 1100

dec(0011) = 0100

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

Answer:

PT 1 = dec(CT 1) ⊕ IV = dec(0011) ⊕ 1010 = 0100 ⊕ 1010 = 1110

PT 2 = dec(CT 2) ⊕ CT 1 ⊕ PT 1 = dec(1011) ⊕ 0011 ⊕ 1110 = 1100 ⊕ 0011 ⊕ 1110 = 0001

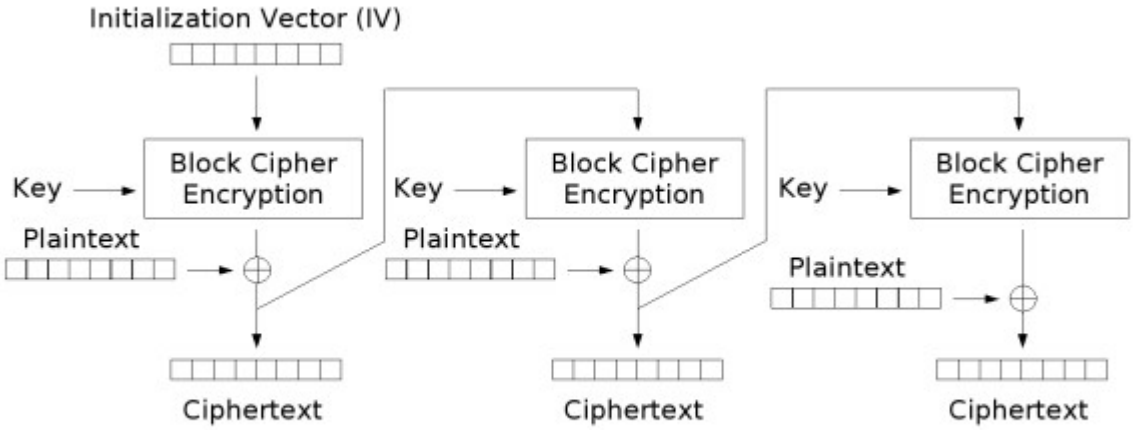
PT 3 = dec(CT 3) ⊕ CT 2 ⊕ PT 2 = dec(0011) ⊕ 1011 ⊕ 0001 = 0100 ⊕ 1011 ⊕ 0001 = 1110

Block Cipher Mode of Operations

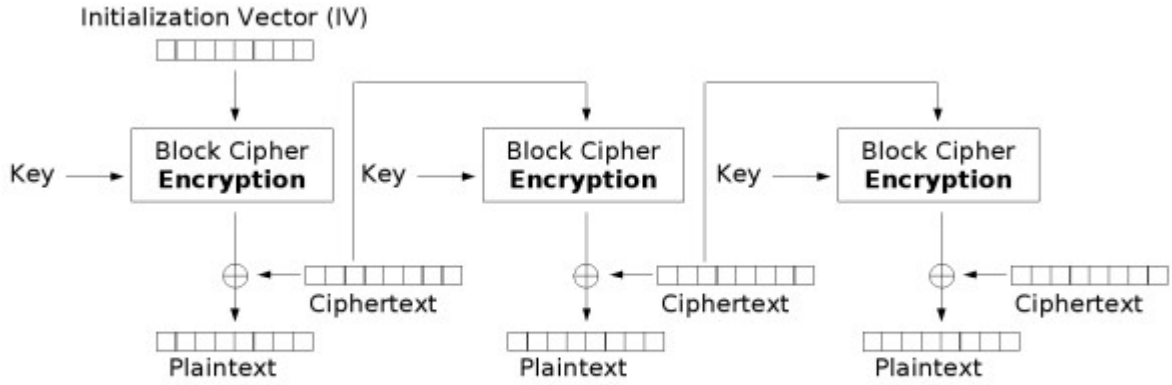
Input	**Output**	**Input**	**Output**
0000	0111	1000	1111
0001	0110	1001	1110
0010	0101	1010	1101
0011	0100	1011	1100

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?

Answer: The block cipher mode of operations ensures that plaintext blocks that are the same do not generate the same ciphertext blocks.

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

Answer: 1011 0100 1100

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

Answer: 1110 1000 1111

Alternatively, can do it the mathematical way:

PT1 = E(IV) xor CT1 = E(0101) xor 1100 = 0010 xor 1100 = 1110

PT2 = E(CT1) xor CT2 = E(1100) xor 0011 = 1011 xor 0011 = 1000

PT3 = E(CT2) xor CT3 = E(0011) xor 1011 = 0100 xor 1011 = 1111

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

Answer:

$n = pq = 5 * 11 = 55$

$\varphi = (p-1)(q-1) = (5-1)(11-1) = (4)(10) = 40$

5b. [2 pts] Choose the smallest possible public (encryption) exponent *e*

Answer:

Find e such that:

$1 < e < \varphi$;

GCD(e, φ)=1

Not possible *e*: 1, 2, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, …

Possible *e*: 3, 7, 11, 13, 17, 19, 23, …

Choose *e*=3

5c. [3 pts] Choose a private (decryption) exponent *d*

Answer:

$ed \bmod \varphi = 1$ or $(ed - 1) \bmod \varphi = 0$

$e = 3$; $\varphi = 40$

$3d \bmod 40 = 1$

Try k = (3d-1)/40; d = (40k+1)/3, for k = 1, 2, 3, ...

k=1; d=41/3 ... **NO**

k=2; d=(40(2)+1)/3 = 81/3 = 27 ... **YES**

Choose d = 27

5d. [2 pts] Encrypt the plaintext message *m*=25 with the public key

Answer: $c = m^e \bmod n = (25)^3 \bmod 55 = 5$

$25 \bmod 55 = 25$

$25^2 \bmod 55$

$= ((25^1 \bmod 55)(25^1 \bmod 55)) \bmod 55$

$= ((25)(25)) \bmod 55 = 625 \bmod 55$

$= 75 \bmod 55 = 20$

$25^3 \bmod 55$

$= ((25^2 \bmod 55)(25^1 \bmod 55)) \bmod 55$

$= ((20)(25)) \bmod 55 = 500 \bmod 55 = 5$

5e. [3 pts] Decrypt your solution in part d to obtain the original message *m*=25

Answer: $m = c^e \bmod n = (5)^{27} \bmod 55 = 25$

$5 \bmod 55 = 5$

$5^2 \bmod 55 = 25$

$5^4 \bmod 55 = 625 \bmod 55 = 20$

$5^8 \bmod 55 = 400 \bmod 55 = 15$

$5^{16} \bmod 55 = 225 \bmod 55 = 5$

$5^{24} \bmod 55 = 75 \bmod 55 = 20$

$5^{27} \bmod 55 = 5*25*20 \bmod 55$

$= 2500 \bmod 55 = 300 \bmod 55 = 25$

5f: [2 pts] What mathematical property provides the security of RSA encryption?

Answer: The difficulty of factoring n to obtain p and q is what gives RSA strength

---

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*

Answer: $A = g^a \bmod n = 6^5 \bmod 17 = 7$

6b. [2 pts] calculate Bob's public key *B*

Answer: $B = g^b \bmod n = 6^{11} \bmod 17 = 5$

$6 \bmod 17 = 6$

$6^2 \bmod 17 = 2$

$6^4 \bmod 17 = 4$

$6^5 \bmod 17 = 7$

$6^{10} \bmod 17 = 15$

6^{11} mod 17 = 90 mod 17 = 5

6c. [4 pts] calculate the shared key *K*

Answer:

$K_A = B^a$ mod n = 5^5 mod 17 = 14

$K_B = A^b$ mod n = 7^{11} mod 17 = 14

5 mod 17 = 5

5^2 mod 17 = 8

5^4 mod 17 = 64-51 = 13

5^5 mod 17 = 65 mod 17 = 14

5^8 mod 17 = 169 mod 17 = 16

5^{10} mod 17 = 128 mod 17 = 9

5^{11} mod 17 = 45 mod 17 = 11

7 mod 17 = 7

7^2 mod 17 = 49 mod 17 = 15

7^4 mod 17 = 225 mod 17 = 55 mod 17 = 4

7^8 mod 17 = 16

7^{10} mod 17 = 15*16 mod 17 = (225 + 15) mod 17 = 240 mod 17 = 70 mod 17 = 2

7^{11} mod 17 = 14

17*2 = 34

17*3 = 51

17*4 = 68

13*5 = 65

6d. [3 pts] In the Diffie--Hellman exchange, what values can Trudy see, and what values she cannot?

Answer: In order for DH to work, the values A, B, g, n must be exchanged, while the values a, b, and K must never be released.

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.

Answer: No, the IV does not need to be kept secret because as long as the encryption function is secret, then the IV does not need to be kept secret, such as a SALT.

7b. [3 pts] Decrypt Ciphertext 000110001100011 without using any mode

Answer: By using the function m(c), the solution is 11011 11011 11011

7c. [6 pts] Decrypt Ciphertext 000110001100011 using CBC and IV=10110

Answer:

PT1 = D(CT1) xor IV = (00011 xor 11000) xor 10110 = 01101

PT2 = D(CT2) xor CT1 = (00011 xor 11000) xor 00011 = 11000

PT3 = D(CT3) xor CT2) = (00011 xor 11000) xor 00011 = 11000

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*

Answer:

$n = pq = 7 * 11 = 77$
$\varphi = (p-1)(q-1) = (7-1)(11-1) = (6)(10) = 60$

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

Answer:

Find e such that:

$1 < e < \varphi$;

GCD(e, φ)=1

Not possible *e*: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22,

Possible *e*: 7, 11, 13, 17, 19, 23

Choose *e*=7

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

Answer:

$ed \bmod \varphi = 1$ or $(ed - 1) \bmod \varphi = 0$

$e = 7$; $\varphi = 60$

$(7d - 1) \bmod 60 = 0$

Try k = (7d-1)/60; d = (60k+1)/7, for k = 1, 2, 3, ...

k=1: d=61/7 ... **NO**

k=2: d=121/7 ... **NO**

k=3: d=181/7 ... **NO**

k=4: d=241/7 ... **NO**

k=5: d=301/7 = 43 ... **YES**

Choose d = 43

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

Answer: $c = m^e \bmod n = (18)^7 \bmod 77 = 39$

$18 \bmod 77 = 18$

$18^2 \bmod 77 = 324 \bmod 77 = 16$

$18^4 \bmod 77$

$= ((18^2 \bmod 77)(18^2 \bmod 77)) \bmod 77$

$= ((16)(16)) \bmod 77 = 256 \bmod 77$

$= 25$

$18^6 \bmod 77 = 25*16 \bmod 77$

$= 400 \bmod 77 = 15$

$18^7 \bmod 77 = 18*15 \bmod 77$

$= 270 \bmod 77 = 39$

77*3 = 231

77*4 = 308

77*5 = 385

77*6 = 462

77*8 = 616

77*9 = 693

18*18 = 180 + 64 + 80 = 324

16 * 16 = 160 + 94 = 256

25 * 16 = 250 + 150 = 400

18*15 = 225 + 45 = 270

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

Answer: Yes, the e and d are interchangeable. It's a property of RSA that when one key is used to encrypt, the other one will be used for decryption.

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?

No answer given.

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
Answer:
n=p*q=57
ϕ=(p-1)*(q-1)=36
7b. [2 pts] Find the five smallest possible values for public (encryption) exponent e
Answer: e, ϕ should be relatively prime so e=5,7,11,13,17
7c. [4 pts] Using the smallest e from 7b, choose a private (decryption) exponent d
Answer:
ed mod ϕ = 1
5d mod 36 = 1
k = (5d-1)/36; d = (36k+1)/5 for k = 1, 2, 3, …
Try k = 1: (36(1) + 1)/5 ?= 0 => 37/5 ?= 0 NO
k = 2: (36(2) + 1)/5 ?= 0 => 73/5 ?= 0 NO
k = 3: (36(3) + 1)/5 ?= 0 => 109/5 NO
k = 4: (36(4) + 1)/5 ?= 0 => 145/5 YES
d=29

7d. [4 pts] Encrypt the plaintext message m=20 with the public key
Answer:
c = me mod n
c = 205 mod 57
20^1 mod 57 = 20
20^2 mod 57 = ((20^1 mod 57)(20^1 mod 57)) mod 57 = 400 mod 57 = 1
20^4 mod 57 = 1
20^5 mod 57 = ((20^1 mod 57) (20^4 mod 57)) mod 57 = (1*20) mod 57 = 20
c = 205 mod 57 = 20

7e: [2 pts] What's the recommended size of the modulus, n, be in today's standards?
Answer: N should be in order of 1024 Bits

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*
Answers:

- A = ga mod n
  - A = 74 mod 13
  - 7^1 mod 13 = 7 – 7^2 mod 13 = ((7^1 mod 13)(7^1 mod 13)) mod 13 = 49 mod 13 = 10
  - 7^4 mod 13 = ((7^2 mod 13)(7^2 mod 13)) mod 13 = 100 mod 13 = 9
  - A = 9
- Bob chooses a secret integer b=5, then sends Alice B = gb mod n – B = 75 mod 13
  - 7^5 mod 13 = ((7^1 mod 13)(7^4 mod 13)) mod 13 = 63 mod 13 = 11
  - B = 11
- Alice computes = Ba mod n Page 5 of 5
  - K = 114 mod 13 – 11^1 mod 13 = 11
  - 11^2 mod 13 = 121 mod 13 = 4
  - 11^4 mod 13 = 16 mod 13 = 3
- Thus shared key K is 3.

8d. [3pts] Why is Diffie-Hellman preferred over RSA for generation of bulk encryption keys?
Answer: RSA is computational intensive, even with today's CPU power its slow to generate 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?
Answer: Trudy cannot easily figure anything out
9b. [3 pts] Decrypt 100110011001 without CBC
Answer: 011001100110
9c. [6 pts] Decrypt 100110011001 using CBC and IV=0101
Answer:
Cipher text X is divided into blocks 1001, 1001, 1001.
IV = 0101
1001(dec) = 0110 XOR IV = 0110 XOR 0101 = 0011
1001(dec) = 0110 XOR Previous Message Block = 0110 XOR 1001 = 1111
1001(dec) = 0110 XOR Previous Message Block = 0110 XOR 1001 = 1111
Thus the plain text is 0011 1111 1111

Scapy: Explain what the following scapy command do:
[4 pts] send(IP(dst="10.10.111.1",ttl=10)/ICMP())

Answer: Send one ICMP echo-request to IP destination 10.10.111.1 with TTL 10. This packet is intended to determine which host is 10 hops away.

8b. [4 pts] sr(IP(dst="10.10.111.0/24")/TCP(dport=(80,81))) See attached file below for a reference on scapy.

Answer: Send SYN packets to IP addresses to the 10.10.111.0/24 network on ports 80 and 81. This is performing a port scan on the network 10.10.111.0/24 for ports 80 and 81.

[4 pts] send(Ether()/IP(src=RandIP(),dst="10.10.111.1")/TCP(dport=80))

Answer: Send one SYN packet from a random source IP to 10.10.111.1 on port number 80.

[4 pts] sr1(IP(dst="10.10.111.0/24")/TCP(dport=(1,100),flags="A"))

Answer: Essentially an TCP ACK scan. Send a TCP ACK packet to the 10.10.111.0/24 network on ports 1 to 100. It outputs the first packet received from scan.

[4 pts] ans,unans = sr(IP(dst="10.10.111.0/24", ttl=5)/TCP(dport=139), timeout=1)
ans.nsummary()
unans.nsummary()

Answer:

ans,unans = sr(IP(dst="10.10.111.0/24", ttl=5)/TCP(dport=139), timeout=1)
It is essentially a TCP SYN scan. The code sends a packet to all hosts with destination IP address 10.10.111.0 and subnet mask of 255.255.255.0, with time to live value set to 5, destination port is set to TCP port 139 and with timeout value set to 1.
ans.nsummary() unans.nsummary()
Since sr() function returns both answered and unanswered packets. The result of answered packets is stored in ans variable and result of unanswered packet is stored in unans variable.
ans.nsummary() returns the entire details of the answered packets along with the packet number.
unans.nsummary() returns the entire details of the unanswered packets along with the packet number.

Miscellaneous

[2 pts] Encrypt "HELLO WORLD" with Julius Ceasar's Cipher of key 5 (positive 5).

Answer: MJQQT BTWQI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(Shift right 5)	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

9b. [4 pts] Define what a chosen-plaintext attacks is.

Answer: Have the plaintext of your choice encrypted. E.g., Alice, please encrypt "HELLO"
Known-plaintext attack: you have some plaintext and the associated ciphertext

[4 pts] What attack does SYN Cookies mitigate? How does it do that?

Answer:

TCP SYN-Flooding (TCP Half open attack). Calculate and store in ISN:
First 5 bits: slow timestamp mod 32
Next 3 bits: an encoded value representing maximum segment size
Final 24 bits: cryptograph hash of server IP/port, client IP/port, and value t
Server verifies sequence # before continuing. Specifics not necessary for full points.

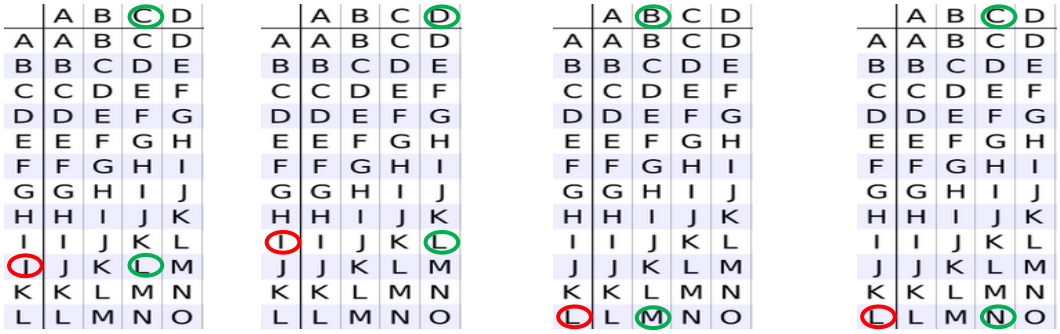
[4 pts] What is Split DNS and what attack is and what it's intended to mitigate?

Answer: Split DNS is to have two DNS servers, one for the internal users, and one for external users. The internal DNS server will have DNS records specifically for internal users only. This is intended to mitigate a brute-force forward DNS attack where a user can brute force DNS names to discover information about the network.

[4 pts] Describe the main reason that an attacker might want install a Reverse WWW Shell onto a target's computer.

Answer: A reverse WWW shell establishes a http/port 80 connection from a host to an external server. An attacker would install a reverse WWW shell because the host is behind a firewall that only allows connections to begin from the internal network.

[4 pts] Using the standard Vigenere (Poly--alphabetic Encryption) table, decrypt the message LLMN using the key CDB. Show work or explain.



Answer:

The table was not given, but it's trivial to recreate the table yourself.

Decrypt L: Lookup Column C / Cell L => Row J

Decrypt L: Lookup Column D / Cell L => Row I

Decrypt M: Lookup Column B / Cell M => Row L

Decrypt N: Lookup Column C / Cell N => Row L

Answer: JILL

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

Answer: Both DNS and NTP amplification attack take a small request to many servers, and it responds with a much larger output directed at the victim. Both these attacks depend on open resolvers, that is, servers that respond to anonymous requests.

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

Answer: Connect scan establishes a three-way handshake while the nmap SYN scan sends a TCP SYN, and then a RST upon receiving an ACK. Additionally, the Connect scan does not require root privileges while the SYN scan does.

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

Answer: By subtracting the numerical value of "X" (24) by "H", (8) we can see that the key is 16 (or -10).