PRACTICE PROBLEMS

CRYPTOGRAPHY AND NETWORK SECURITY

PRINCIPLES AND PRACTICE

SIXTH EDITION

WILLIAM STALLINGS

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 Which of the following activities might be considered a possible source of threat to a company's network, and why?

a. The daily courier service personnel who drop off and pick up packages.

b. Former employees who left the company because of downsizing.

c. An employee traveling on company business to another city.

d. The building management company where an organization has its offices has decided to install a fire sprinkler system.

CHAPTER 2 CLASSICAL ENCRYPTION TECHNIQUES

2.1 The index of coincidence is an important concept in classical cryptanalysis. For this problem, please read the background document on this subject in the Documents folder in the protected section of this book's Web site.
Consider a language with three letters, a, b, and c, with frequencies .6, .3, and .1. Suppose that a long message (1000 characters) in this language is encrypted with a Vigenere cipher and we plan to break it using an index of coincidence attack. About how big is the largest index of coincidence we are likely to see?

2.2 What is the main drawback of the one-time pad cryptosystem?

2.3 You have intercepted a message encrypted with an affine cipher. The ciphertext starts with BBDJ and you know the plaintext starts with oops. Find the key.

2.4 Eve has captured an encryption device that she knows is an affine cipher (mod 26). She conducts a chosen plaintext attack and feeds in the letters A and B into the cipher to get the ciphertexts H and O. What was the key (α, β) for the underlying affine cipher?

2.5 Another well-known concept from classical cryptanalysis is the Kasiski test. For this problem, please read the background document on this subject in the Documents folder in the protected section of this book's Web site.
You have found an old ciphertext, where you know that the plaintext discusses cryptographic methods. You suspect that a Vigenere cipher has been used and therefore look for repeated strings in the ciphertext. You find that the string TICRMQUIRTJR occurs twice in the ciphertext. The first occurrence starts at character position 10 in the text and the second at character position 241 (we start counting from 1). You make the inspired guess that this ciphertext sequence is the encryption of the plaintext word *cryptography*. If this guess is correct, what is the key?

2.6 Consider a substitution cipher where 52 symbols were used instead of 26. In particular, each symbol in the cipher text is for either a lowercase English letter, or an uppercase English letter. (For example, let E be the encryption function then we could have E(S) = p and E(s)=m.) Such a

modification augments the key space to 52! Does this provide added security compared to a standard substitution cipher? Why or why not?

2.7 We consider the one-time pad with messages and keystreams both binary sequences. Suppose that the system is used erroneously, so that two messages have been encrypted using the same key. What information can an adversary that hears the two ciphertexts deduce about the plaintexts?

2.8 You have found one small piece of matching plaintext and ciphertext for a Hill cipher using a 2×2 matrix key with mod 17 entries. In particular, the plaintext $\begin{pmatrix} 12 \\ 5 \end{pmatrix}$ maps to the ciphertext $\begin{pmatrix} 14 \\ 10 \end{pmatrix}$. (Note that we are using the convention that these entries appear as column vectors when the encryption is applied.) Using this given information and nothing else, how many possible keys could there be? List two of these possible keys

CHAPTER 3 BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD

3.1 State Kirchhoff's principle. Explain briefly why a cryptosystem designed by someone who follows this principle is likely to be stronger than one designed by someone who does not.

3.2 Assuming you can do 2^{20} encryptions per second and the key size is 40 bits, how long would a brute force attack take? Give a scenario where this would be practical and another where it wouldn't. What happens if you double the key size?

3.3 Consider the following strategy for speeding up the DES implementation. First, the 32-bit permutations after the S-boxes are removed. Next, the expansion function E is modified as follows. Divide the 32-bit input into 8 blocks of 4 bits. Then, expand each block into 6 bits by replicating the 3rd and 4th bits and placing them in the 5th and 6th bits of output. That is $x_1, x_2, x_3, x_4 \rightarrow x_1, x_2, x_3, x_4, x_3, x_4$. Show how to break the full 16-round DES in this case. Analyze the complexity of your attack.

3.4 Review the concept of the entropy or uncertainty function H in Appendix F for the following questions. We also need to introduce two terms. Recall from Chapter 3, that an n-bit block cipher can have at most $2^n!$ keys. A **random cipher** is an n-bit block cipher that does have $2^n!$ keys. Thus, for a random cipher, given any n-bit ciphertext and any given n-bit plaintext, there exists a key that maps this ciphertext into this plaintext. Thus, the ciphertext contains no information that can be used to deduce the key. Now, let C and K be uniformly distributed random variables denoting, respectively the ciphertext block and the key. Under the **random cipher model**, $M = D(K, C)$ is a random variable uniformly distributed over all possible pre-images of C (i.e., all possible decryptions of C). We consider the random cipher model with sets M of plaintexts, C of ciphertexts and K of keys. We consider the random cipher model with sets M of plaintexts, C of ciphertexts and K of keys.

a. Give an interpretation of the equation

$$H(C, M, K) = 0$$

and motivate why this holds.

b. Prove

$$H(C, M, K) \leq H(M) + H(K).$$

You may use without proof general (in)equalities for entropy and the equality from (a).

c. In fact, one would expect equality to hold in (a). Why?

3.5 As you know, DES is insecure because of its short key length (56 bits). An improvement, proposed by Rivest, is DESX. DESX has key length 120 bits, seen as a pair $K = (k_1, k_2)$, where k_1 is 56 bits and k_2 is 64 bits. The encryption of a one-block message m is

$$\text{DESX}(K, m) = k_2 \oplus \text{DES}(k_1, (m \oplus k_2))$$

a. Explain how decryption is done.

b. Explain why the inner XOR is necessary, i.e. explain an attack against

$$\text{DESX}'(K, m) = k_2 \oplus \text{DES}(k_1, m)$$

that is much better than brute force.

CHAPTER 4 BASIC CONCEPTS IN NUMBER THEORY AND FINITE FIELDS

4.1 Use the extended Euclidean algorithm to compute the greatest common divisor d of 654 and 123 and to find integers m and n such that $654m + 123n = d$.

4.2 What is the value of $123^{241} \bmod 35$? (Give your answer as an integer between 0 and 34, inclusive.).

4.3 If $a \neq 0$ show that the set of values d such that d divides a is a finite set.

4.4 Determine the gcd of $a(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$ and $b(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$ over GF(2).

4.5 Find x in the following equations:

a. $2^x \equiv 5 \pmod{11}$
b. $3^x \equiv 5 \pmod{16}$
c. $2^x \equiv 5 \pmod{31}$
d. $3^x \equiv 5 \pmod{32}$

4.6 Find the following multiplicative inverses:

a. $3^{-1} \pmod 5$
b. $3^{-1} \pmod{10}$
c. $3^{-1} \pmod{15}$
d. $3^{-1} \pmod{23}$
e. $7^{-1} \pmod{17}$
f. $10^{-1} \pmod{26}$
g. $5^{-1} \pmod{31}$
h. $27^{-1} \pmod{47}$
i. $1234^{-1} \pmod{10001}$

CHAPTER 5 ADVANCED ENCRYPTION STANDARD

5.1 Briefly describe the Shift Rows and Byte Substitution layers of AES. Explain why we can apply them in either order with the same result.

5.2 Show the first eight words of the key expansion for a 128-bit key of all ones.

CHAPTER 6 BLOCK CIPHER OPERATION

6.1 An affine encryption $C = E([a, b], p) = (ap + b) \bmod 26$ can be considered a double encryption, where one encryption is multiplying by a and the other is a shift by b. Show that the meet-in-the-middle attack from above takes at most 38 steps (not including comparison operations).

6.2 Consider a sensor X that periodically sends a 64-octet measurement to a receiver Y. One day the administrator decides that X should encrypt the measurement data using DES in CBC mode. How many octets does X now send for each measurement? Explain your answer.

6.3 In the definition of OFB, justify the derivation of the encryption expression

$$C_j = P_j \oplus E(K, [C_{j-1} \oplus P_{j-1}])$$

CHAPTER 7 PSEUDORANDOM NUMBER GENERATION AND STREAM CIPHERS

For the first five problems, you need to review the concept of a linear feedback shift register (LFSR), which is explained in the document LFSR.pdf in the Documents folder in the protected section of this book's Web site.

7.1 Consider an LFSR of length n bits.

a. Explain why the generated key sequence cannot have a period longer than
$2^n - 1$ bits.

b. Explain why an LFSR that generates maximal period sequences must have an even number of ones in its tap sequence.

7.2 The following sequence of 50 binary digits is the beginning of the output sequence from a linear feedback shift register (LFSR). Construct an LFSR of minimal length that produces this output.

00100001111101010011000100001111101010011000100001

7.3 Alice has decided to use a stream cipher for encryption, i.e.

$$c = m \oplus b(k)$$

where the binary string m is the plaintext, $b(k)$ is the keystream, depending on the secret key k, and c is the ciphertext. As keystream generator she has decided to use an LFSR. Her messages are English text encoded with 8 bits per letter and message lengths are always 25 letters.

a. Alice wants the keystream to have the property that the keystream used for each message is shorter than one full period. What is the minimum size of the key k (in bits)?

b. Alice's messages have the property that they all start with Alice. The adversary knows this and has access to one ciphertext c. Will he be able to break the encryption, if Alice chooses the minimum key size from (a)?

7.4 Construct an LFSR (linear feedback shift register) of minimal length that produces the output $(1001110)^{\infty}$.

7.5 Consider an LFSR of length n that generates an output of maximal period $2^n - 1$. How many zeros are there in a period?

7.6 If $p = 11$ and $q = 19$, use the BBS algorithm to produce the kth bit if $X_{k-1} = 100$.

CHAPTER 8 INTRODUCTION TO NUMBER THEORY

8.1 There are many examples of two consecutive odd numbers, both of which are prime, such as 11 and 13; 29 and 33. Are there any examples of three consecutive numbers being prime? *Hint:* this does not require a complex proof, just some thought on your part.

8.2 In this problem we consider the Pohlig-Hellman cryptosystem, which is a secret key encryption method based on the difficulty of the discrete log problem. The setting is Z_p for some large prime p, which need not be secret. In order to exchange messages, Alice and Bob agree on a secret key K, $1 \le K \le p - 2$, from which a second key D is computed. Encryption of M is $C = M^K \bmod p$. Decryption is $M = C^D \bmod p$ for a suitably chosen D.

a. Alice and Bob agree on p and K and they must both compute D in order to be able to decrypt. What condition must K satisfy and how can they compute D?

b. The only difference between this cryptosystem and RSA is in the modulus; in RSA one works in Z_n, where $n = p \times q$. Explain why this difference makes it possible to use RSA as a public key system, while the Pohlig-Hellman system could only be used with secret keys.

8.3 Prove that if n is a nonprime integer, then n has a prime number p such that $p \le \sqrt{n}$.

8.4 For which positive integers does $\phi(3n) = 3\phi(n)$?

8.5 Find the unique solution for:

$$x \equiv 3 \pmod 2; \quad x \equiv 5 \pmod 3; \quad x \equiv 7 \pmod 5$$

8.6 Using $p = 7$, verify Fermat's theorem for all positive $a < 7$.

8.7 Explain how Fermat's theorem can be used to test for primes.

8.8 Use Fermat's theorem to show that 10 is not a prime number.

CHAPTER 9 PUBLIC-KEY CRYPTOGRAPHY AND RSA

9.1 We now look at a 3-person group encryption scheme based on the same principle as RSA. Suppose that some trusted entity generates two primes p and q and forms $n = pq$. Now, instead of choosing e_A and d_A (as in RSA), the trusted entity chooses k_1, k_2, and k_3 such that gcd (k_j, n) = 1 and $k_1k_2k_3 = 1 \pmod{\phi(n)}$. The three users A, B, and C are given the following keys:

A: (k_1; k_2; n)

B: (k_2; k_3; n)

C: (k_1; k_3; n)

a. Suppose user A generates a message m such that gcd (m, n) = 1. A wants to encrypt m so that both B and C can decrypt the ciphertext. To accomplish this, A forms the ciphertext $y = m^{k_1k_2} \bmod n$. Explain how B would decrypt y, and explain how C would decrypt y.

b. Suppose A and B have been collaborating on some class project and have produced the message m (with gcd(m, n)=1). They would like to create a ciphertext that they can send C so that only C can decrypt it, and such that once encrypted neither A nor B can decrypt to recover m. Explain how can this be accomplished.

9.2 For RSA, it is often recommended to choose a small public key exponent to increase efficiency. A common choice is $e = 3$. Why not $e = 2$?

9.3 Consider double encryption using a common modulus n and two public keys $e1$ and $e2$ with corresponding private keys $d1$ and $d2$. So a message m is encrypted first using RSA encryption with the key $e1$; the result is encrypted again using key $e2$. There are two arguments why this does not increase security. One is an argument against double encryption in general and the other against this particular proposal. Give both arguments.

9.4 Public-key algorithms are usually used for encrypting short messages. But if we need to encrypt a longer message we can split it into blocks, use RSA for each block and use a block cipher mode. Which of the two modes, CBC and Counter, would you recommend in such a situation?

9.5 Brian uses an RSA system with public keys n (the modulus) and e_1 (public exponent) with a matching private key d_1. Brian creates RSA keys for his friend Meg using the same public key n, but a different public exponent e_2 and matching private exponent d_2. While Brian was being careless, you discover the values of d_1 and d_2. Though you do not wish to read message intended for Brian or Meg, you do wish to read messages directed towards Sarah, who also uses the public modulus n with the public exponent e_3. Outline a strategy that may help uncover Sarah's private exponent, d_3.

9.6 In this problem we consider the Pohlig-Hellman cryptosystem, which is a secret key encryption method based on the difficulty of the discrete log problem. The setting is Z_p for some large prime p, which need not be secret. In order to exchange messages, Alice and Bob agree on a secret key e, $1 \le d \le p - 2$, from which a second key d is computed. Encryption of M is $C = M^d \bmod p$. Decryption is $M = C^d \bmod p$ for a suitably chosen d. Note that $M < p$.

a. Alice and Bob agree on p and e and they must both compute d in order to be able to decrypt. What condition must e satisfy and how can they compute d?

b. The only difference between this cryptosystem and RSA is in the modulus; in RSA one works in Z_n, where $n = p \times q$. Explain why this difference makes it possible to use RSA as a public key system, while the Pohlig-Hellman system could only be used with secret keys.

9.7 Can a user of RSA choose the encryption exponent e to be even, e.g. $e = 4$?

9.8 Alice wants to send an encrypted message to Bob using RSA, but doesn't know his public key. So, she sends Bob an email asking for the key. Bob replies with his RSA public key (e, n). However, the active adversary intercepts the message and changes one bit in e from 0 to 1, so Alice receives an email claiming that Bob's public key is (e', n), where e' differs from e in one bit. Alice encrypts M with this key and sends it to Bob. Of course, Bob cannot decrypt, since the message was encrypted with the wrong key. So he resends his key and asks Alice to send the encrypted message again, which she does. The adversary eavesdrops to the whole communication without interfering further. Describe how he can now recover M.

9.9 **a.** A web-based auction site uses textbook RSA encryption to maintain the secrecy of bids. The site has public RSA key (n, e). For the sake of this problem we make the completely unrealistic assumption that a bid is sent in a message containing only a single integer,

representing the bid value. Now, Alice has just made a bid and the adversary Mallory has eavesdropped and heard the ciphertext c. Mallory's main aim is to prevent Alice's bid from winning. Of course, he cannot recover Alice's bid, but makes the guess that her bid is an integer that is a multiple of 10. Show that, if Mallory's guess is right, he can himself make a bid that is 10% higher than Alice's

b. To prevent the attack from (a) and other attacks against textbook RSA, messages should be padded using some padding scheme, such as OAEP. Describe some guiding principles in constructing such padding schemes. You do not need to describe the actual padding scheme in detail.

9.10 For $p = 101$ and $q = 103$, find three possible values for e.

CHAPTER 10 OTHER PUBLIC-KEY CRYPTOSYSTEMS

10.1 Here we consider the public key encryption scheme DHIES, which makes use of many cryptographic primitives:

- A subgroup of prime order q of Z_p for some large prime p and a generator g for that subgroup. Typically, q would be a 160-bit and p a 1024-bit prime.
- A symmetric encryption scheme E with keys of n_1 bits.
- A MAC function MAC with keys of n_2 bits.
- A hash function H that produces hash values with n_1+n_2 bits

All these choices are public. Each user chooses a private key $x < q$ and a public key $X = g^x$.

To encrypt a message m for a user with this key pair, using the pubic key, one proceeds as follows:

- Choose a random $y < q$ and compute $Y = g^y$.
- Compute $K = X^y$.
- Compute $H(K \| Y)$ and parse it as $k_1 \| k_2$.
- Compute $C = E(k_1, m)$.
- Compute $T = MAC(k_2, C)$.
- The encrypted message is $Y \| C \| T$

Note that here m can be of arbitrary length, so this is a hybrid encryption scheme.

a. Describe how the receiver decrypts a received ciphertext.

b. DHIES can be shown to be resistant to CCA2 (adaptive chosen ciphertext) attacks; explain briefly what this means.

c. DHIES can be adapted to work in elliptic curve groups. Describe the changes needed and what advantages this would imply.

CHAPTER 11 CRYPTOGRAPHIC HASH FUNCTIONS

11.1 Define the notion of collision resistance for hash functions.

11.2 Many hash functions are constructed from a simpler building block, called a compression function. Describe this general construction.

11.3 What is the birthday attack on a hash function?

11.4 A particular hash function produces *n*-bit hash values. We generate messages at random in some unspecified way and hash them. Approximately how many messages would you expect that we have to generate before we get a collision?

CHAPTER 12 MESSAGE AUTHENTICATION CODES

12.1 Consider an application that requires an encryption and MAC algorithm be implemented on a processor with a small amount of non-volatile memory. The only cryptographic algorithm that the processor can compute is Triple-DES. But you have space for one 168-bit key. Describe how it is possible to both encrypt and MAC using only a single key. Justify your answer and state any assumptions you use.

12.2 We consider a banking application, where messages m of the form `fromAccount, toAccount, amount` are sent within the bank network, with the meaning that `amount` dollars should be transferred from `fromAccount` to `toAccount`. Each message consists of three blocks, with each block holding one of the three parameters. Messages are encrypted using AES in Counter mode, i.e.

$K_j = \mathrm{E}(K, T_j)$
$C_j = M_j \oplus K_j$

Each of the three parts of a message is sixteen characters, i.e. one block, so messages consist of three blocks.

a. The adversary has an account in the bank and can intercept and change messages. Imagine now that he knows the `toAccount` for a particular message $m = C_1C_2C_3$. Explain how he can modify the message so that the amount is transferred to his own account

b. Explain how the use of a MAC would prevent this attack.

c. Above, E(K, M) denotes using block cipher E with key K on message M. It is possible to define a cipher using similar ideas, but using a hash function instead. Describe how to do it, including how to decrypt.

12.3 Explain why a checksum or CRC, by itself, does not provide security.

CHAPTER 13 DIGITAL SIGNATURES

13.1 What common usage do hash functions have in connection with digital signatures?

CHAPTER 14 KEY MANAGEMENT AND DISTRIBUTION

14.1 Suppose Alice has *a* and Bob has *b*. Alice and Bob also share a secure communication channel. Chris wants to compute $S=a \oplus b$. Alice does not want Chris or Bob to learn *a* and Bob does not want Chris or Alice to learn *b*. How can this be done?

14.2 Explain the problems with key management and how it affects symmetric cryptography.

CHAPTER 15 USER AUTHENTICATION

15.1 We consider an identification protocol based on the discrete log problem. The setting is some cyclic group G of prime order q with generator g. Peggy chooses a private key $x < q$ and has as public key $X = g^x$. The purpose of the following protocol is to convince Victor that Peggy knows x:

- Peggy chooses $r < q$ at random and computes $R = g^r$ and $S = g^{x-r}$. She sends R and S to Victor.
- Victor chooses a random bit b and sends to Peggy.
- If $b = 0$, Peggy sends $z = r$ to Victor; if $b = 1$ she sends $z = x - r$.

a. What computations will Victor now do to check Peggy's values?

b. Show that a false Peggy (i.e. someone who does not know x) can participate in this protocol and have probability 0.5 to pass Victor's check.

c. How would you extend the protocol so that Victor can be reasonably convinced that if Peggy passes, she really knows x?

15.2 **a.** What is meant by "Perfect Forward Secrecy"?

b. Does Kerberos offer "Perfect Forward Secrecy"?

15.3 In the authentication protocol below, pw is A's password and J is a key derived from pw. Can an attacker that can eavesdrop messages (but not intercept or spoof messages) obtain pw by off-line password guessing? If you answer no, explain briefly. If you answer yes, describe the attack.

A (has pw)	B (has J)
send [conn] to B	
	generate random challenge R send [R]
compute J from pw compute X ← encrypt(R) with key J send [X] to B	
	compute Y ← decrypt(X) with key J if Y = R then A is authenticated

15.4 The chart below shows an authentication protocol, followed by data exchange, followed by disconnection. Only an initial part of the

authentication protocol is shown; here, pw is A's password, J is a key derived from pw, and L is a high-quality key. Assume an attacker that can (1) eavesdrop messages and (2) intercept and spoof messages sent by A (but not those sent by B). Complete the authentication protocol (i.e., supply the part indicated by the "** …. * *") so that in spite of this attacker

- B authenticates A,
- this authentication is not vulnerable to off-line password guessing, and
- A and B establish a session key S (for encrypting data) such that after A and B disconnect and forget S, even if the attacker learns pw, the attacker cannot decrypt the data exchanged.

	A (has pw)	B (has J, L)
	send [conn] to B	X ← encrypt(L) with key J send [X]
	compute J from pw L' ← decrypt(X) with key J	
*		
*		
*		
*		
*		
*		
*		
*		
	←A and B exchange data →	
	←A and B disconnect →	

CHAPTER 17 TRANSPORT-LEVEL SECURITY

17.1 Differentiate between www, hypertext, and hypermedia.

CHAPTER 18 WIRELESS NETWORK SECURITY

18.1 What do you call a fake hotspot used by hackers to prey on mobile workers, and how does it work?

CHAPTER 19 ELECTRONIC MAIL SECURITY

19.1 What is the way by which one can download normal email or web pages so that the content is hidden?

19.2 Explain the terms "proof of submission" and "non-repudiation" in an electronic mail system. Explain the importance of non-repudiation in an e-commerce system.

CHAPTER 20 IP SECURITY

20.1 Will IPsec make firewalls obsolete?

20.2 An attacker is intent on disrupting the communication by inserting bogus packets into the communications. Discuss whether such an attack would succeed in systems protected by IPsec. Discuss whether such an attack would succeed in systems protected by SSL.

CHAPTER 21 MALICIOUS SOFTWARE

21.1 Explain the following terms: Bot Net; Easter Egg; Logic Bomb.

21.2 Look at the following code snippet. You may assume that escape() argument is always non-null and points to a '\0'- terminated string. What's wrong with this code (from a security point of view)?

```
/*Escapes all newlines in the input string, replacing them
    with"\n".*/
/* Requires: p != NULL; p is a valid '\0'-terminated string */
void escape(char *p)
{
while (*p != '\0')
switch (*p)
{
case '\n':
memcpy(p+2, p+1, strlen(p));
*p++ = '\\'; *p++ = 'n';
break;
default:
p++;
}
}
```

CHAPTER 22 INTRUDERS

22.1 Name some of the ways by which hackers compromise computers without code breaking.

22.2 What is a "Null session" problem?

22.3 How can an intrusion detection system actively respond to an attack?

22.4 Consider the following login protocol.

user knows password P
user knows Hash function H(.) and has a mobile calculator
user gives login name N to machine
machine generates random number R
machine gives R to user
user computes X := Hash(P) XOR Hash(R)
user gives X to machine
machine uses N to obtain P from password table
machine computes Y := Hash(P) XOR Hash(R)
if X=Y then machine allows login

a. Explain what is wrong with it and how can it be broken.

b. Show a simple way to strengthen this protocol against your attack.

CHAPTER 23 FIREWALLS

23.1 Can a packet filter block all incoming email containing the phrase "Make money fast"? If yes, show a packet filtering ruleset that provides this functionality; if no, explain why a (stateless) packet filter cannot do it.

23.2 List and explain three network threats that a firewall does not protect against.

23.3 We have an internal webserver, used only for testing purposes, at IP address 5.6.7.8 on our internal corporate network. The packet filter is situated at a chokepoint between our internal network and the rest of the Internet. Can such a packet filter block all attempts by outside hosts to initiate a direct TCP connection to this internal webserver? If yes, show a packet filtering ruleset that provides this functionality; if no, explain why a (stateless) packet filter cannot do it.

Note: A ruleset is a list of rules, and the first matching rule determines the action taken. A rule is an action followed by a specification of which packets match: e.g.,

```
drop tcp 1.2.3.4:* -> *:25.
```

23.4 Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, and laptops against network threats.

a. A firewall at the network perimeter.

b. Firewalls on every end host machine.

c. A network perimeter firewall and firewalls on every end host machine