Chapter 3

Answer Key

What Is Cryptography?

Encryption for Confidentiality

Terminology

The Simple Cipher

Cryptanalysis

1. a) Define cryptography.

   The use of mathematical operations to protect messages traveling between parties or stored on a computer.

   b) What is confidentiality?

   Confidentiality means that people who intercept messages cannot read them.

   c) Distinguish between plaintext and ciphertext.

   The plaintext is the original message to be delivered. When the plaintext is encrypted, it becomes ciphertext and cannot be read by an interceptor. However, the receiver can decrypt the ciphertext back to plaintext.

   d) Which is transmitted across the network—the plaintext or the ciphertext?

   Ciphertext

   e) What is a cipher?

   A cipher is a mathematical process used in encryption and decryption.

   f) What is a key?

   A random string of 40 to 4,000 bits (ones and zeros)

   g) What must be kept secret in encryption for confidentiality?

As long as the key is kept secret, both parties will still have confidentiality.

h) What is a cryptanalyst?

Someone who cracks encryption

2. Complete the enciphering in **Error! Reference source not found.**.

n	4	r
o	8	w
w	15	l
i	16	y
s	23	p
t	16	j
h	3	k
e	9	n
t	12	f
i	20	c
m	6	s
e	25	d

Substitution and Transposition Ciphers

Substitution Ciphers

Transposition Ciphers

Real Encryption

3. a) Which leaves letters unchanged—transposition or substitution ciphers?

Transposition leaves letters unchanged.

b) Which leaves letters in their original positions—transposition or substitution ciphers?

Substitution ciphers

4. Complete the enciphering in **Error! Reference source not found.**.

11	h
12	n
13	i
21	t
22	w
23	t
31	e
32	o
33	s

	Key Part 1		
Key Part 2	1	3	2
2	n	o	w
3	i	s	t
1	h	e	t

Cipher text = hnitwteos

Ciphers and Codes

5. a) In codes, what do code symbols represent?

   In codes, code symbols represent complete words or phrases.

   b) What is the advantage of codes?

   The advantage of codes is that people can do encoding and decoding manually, without a computer.

   c) What are the disadvantages?

   The disadvantage of codes is that code books must be distributed ahead of time, and if one code book is intercepted, all confidentiality is lost.

6. Finish encoding the message in **Error! Reference source not found.**.

   17434 63717 8397 11131 34058 53764 73104 26733 29798 72135 54678 61552

Symmetric Key Encryption

7. a) Why is the word *symmetric* used in symmetric key encryption?

   Because two parties only use a single key for encryption and decryption in both directions

   b) When two parties communicate with each other using symmetric key encryption, how many keys are used in total?

   Only 1 key is used in symmetric key encryption.

   c) What type of encryption cipher is almost always used in encryption for confidentiality?

   Nearly all encryption for confidentiality uses symmetric key encryption ciphers.

8. a) What is the best way to thwart exhaustive searches by cryptanalysts?

   Simply make the key so long that the time needed for attackers to crack the key is far too long for practicality.

   b) If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 45 bits?

   Because each bit doubles the time it takes to crack a key, extending the key length by 2 bits would increase the time to crack by 2^2 = 4.

If a key is 43 bits long, it'll take 4.4E+12 tries, and if it is 45 bits long, the crack will take 1.76E+13 tries.

c) If it is extended to 50 bits?

Extending the key to 50 bits = 2^7 increase = 128 times longer to crack.

d) If a key is 40 bits long, how many keys must be tried, on average, to crack it?

240 bits can generate 1,099,511,627,776 combinations.

Normally, a cryptanalyst must try half of all possible combinations to succeed.

Half of 1,099,511,627,776 is 549,755,813,888.

So on average, a brute-force password cracker will need about 550 billion tries.

e) How long must a symmetric encryption key be to be considered strong today?

Symmetric encryption keys must be 100 bits or longer to be considered a strong key.

Human Issues in Cryptography

9. Why is cryptography not an automatic protection?

Cryptography is not an automatic protection because it is not infallible. The humans that utilize cryptography can do things that either completely compromise the key or provide sufficient data to allow more efficient cracking of the key. Companies must have and enforce processes that do not compromise the strengths of cryptography.

It is not an automatic protection because if a sender or receiver fails to keep the key secret, an eavesdropper may learn the key and read every message. Poor communication discipline in general can defeat the strongest cipher and longest key. Also, communicating partners can have a false sense of security because they will think that the cracked encryption method is still protecting them. The reality of cryptography is that it is not an automatic protection. It only works if companies have and enforce organizational processes that do not compromise the technical strengths of cryptography.

Symmetric Key Encryption Ciphers

RC4

10. a) What are the two advantages of RC4?

First, RC4 is extremely fast and uses only a small amount of RAM.[1] This means that it is ideal for small handheld devices and was viable for even the earliest 802.11 wireless access points. Second, RC4 can use a broad range of key lengths. For most ciphers, longer key length is better. However, RC4 was widely used primarily because its shortest optional key length is 40 bits.

b) Why is an RC4 key length of 40 bits commonly used?

An RC4 key length of 40 bits is commonly used because national export limits in many countries once limited commercial products up to 40-bit encryption.

c) Is this a strong key?

No. It is less than 100 bits long, so it is not strong. It was selected *because* it was weak.

The Data Encryption Standard (DES)

11. a) How long is a DES key?

DES keys are 56 bits long (64 bits with 8 redundant bits to allow parties to detect incorrect keys).

b) Is this a strong length?

DES is only 56 bits, therefore, it is not strong. (It needs to be 100 or more.)

c) Describe block encryption with DES.

The DES key is 56 bits long. It comes in a block of 64 bits, of which 56 bits represent the key. The other 8 bits are redundant in the sense that you can compute them if you know the other 56 bits. This redundancy allows parties to detect incorrect keys. DES encrypts messages 64 bits at a time. The inputs for the encryption are the key and the 64-bit block of plaintext. The output is a 64-bit block of ciphertext.

Triple DES (3DES)

12. a) How does 3DES work?

It applies DES 3 times, with two or three different keys.

b) What are the two common effective key lengths in 3DES?

112 bit and 168 bit are the two common effective key lengths in 3DES.

c) Are these lengths strong enough for communication in corporations?

3DES is strong enough for communication in corporations.

d) What is the disadvantage of 3DES?

[1] One way to see why RC4 is fast is to note that RC4 can be implemented in only about 50 lines of code. In contrast, the gold-standard AES algorithm requires 350 lines of code (http://www.informit.com). More lines of code generally correspond to longer processing time per key.

DES is slow and having to apply DES three times is extremely slow, therefore, extremely expensive in terms of processing cost. 3DES is prohibitively slow for use on personal computers.

Advanced Encryption Standard (AES)

13. a) What is the big advantage of AES over 3DES?

It offers 3 alternative key lengths instead of two. AES is efficient enough in terms of processing power and RAM requirements to be used on a wide variety of devices.

b) What are the three key lengths offered by AES?

128 bit, 192 bit and 256 bit.

c) Which strong symmetric key encryption cipher can be used with small mobile devices?

AES can be used with small mobile devices.

d) Which symmetric key encryption cipher probably will dominate symmetric key encryption in the near future?

AES

Other Symmetric Key Encryption Ciphers

14. a) It is claimed that new and proprietary encryption ciphers are good because cryptanalysts will not know them. Comment on this.

The fact that a cryptanalyst does not know a proprietary encryption cipher does not mean that it is a good, strong cipher. In reality, it is very difficult to create a vulnerability-free cipher that is not cracked quickly by an expert cryptanalyst.

b) What is security through obscurity, and why is it bad?

It relies on attackers not to obtain learnable information and it is bad because it could result in catastrophic loss of security if known.

Cryptographic Systems

15. a) Distinguish between cryptography and cryptographic systems.

Cryptography is the use of mathematical operations to protect messages traveling between parties or stored on a computer. Cryptographic systems are packaged sets of cryptographic countermeasures for protecting data and its transmission.

b) Distinguish between cryptographic systems and cryptographic system standards.

Cryptographic systems follow specific cryptographic system standards.

c) Why is the first handshaking stage the negotiation of security methods and options?

Because most cryptographic system standards offer multiple methods, the first handshaking stage must negotiate the specific security parameters (cryptographic methods and options to be used in communication).

The first handshaking stage is the initial negotiation of security parameters.

d) What is an impostor?

An impostor is someone who pretends to be someone else.

e) What is authentication?

Proving your identity to communicate to a partner

f) What is mutual authentication?

When both parties authenticate themselves to the other

g) Why is a secure keying phase necessary?

Secure keying is necessary because if the key is not protected, it can be stolen and this will defeat the purpose of encrypting the data.

16. a) What three protections do cryptographic systems provide on a message-by-message basis?

An electronic signature, message integrity, and message encryption.

b) What is an electronic signature?

An electronic signature is a field in a message that authenticates the message.

c) What two protections do electronic signatures usually provide?

Electronic signatures provide both message-by-message authentication and message integrity.

d) Distinguish between the handshaking stages and ongoing communication.

The handshaking stage only happens about .1% of the time and the on-going communication stage happens about 99.9% of the time.

The Negotiation Stage

Cipher Suite Options

Cipher Suite Policies

17. a) In SSL/TLS, what is a cipher suite?

A cipher suite is a specific set of options for a particular cryptographic system standard.

b) Why do companies wish to create policies that define security methods and options for a particular application that is used between corporate partners?

Due to wide variation in the strengths of cipher suites, companies must develop risk-based policies for the selection of cipher suites, only allowing cipher suites with suitable strength for the risks facing the application.

Initial Authentication Stage

Authentication Terminology

18. a) In authentication, distinguish between the supplicant and the verifier.

In authentication, the party trying to prove its identity to the other is called the supplicant**.** The other party is the verifier**.**

b) What are credentials?

They are proofs of identity.

c) How many supplicants and verifiers are there in mutual authentication between two parties? Explain.

There are two supplicants and two verifiers. In mutual authentication, the two parties take turns being supplicants and verifiers.

Hashing

19. a) In hashing, what is the hash?

When hashing is applied to a binary message, the result (called the hash) is far shorter than the original message, typically only 128 to 512 bits long.

b) Is encryption reversible?

Encryption is reversible.

c) Is hashing reversible?

Hashing is irreversible.

d) Is hashing repeatable?

Hashing is repeatable.

e) When a hashing algorithm is applied, does the hash have a fixed length or a variable length?

It will have a fixed length.

f) What is the hash size of MD5?

128 bits

g) What is the hash size of SHA-1?

160 bits

h) What is the hash size of SHA-256?

The hash size of SHA-256 is 256 bits.

i) Which hashing algorithms should not be used because they have been found to be vulnerable?

Unfortunately, cryptanalysts have recently found weaknesses in both MD5 and SHA-1. Only stronger versions of SHA should be used today, and MD5 should not be used at all.

Initial Authentication with MS-CHAP

20. a) Is MS-CHAP used for initial authentication or message-by-message authentication?

MS-CHAP is used for initial authentication.

b) How does the supplicant create the response message?

The MS-CHAP supplicant creates the response message by (1) adding the shared "secret" password to the challenge message, (2) hashing the resulting string. The hash is the response message.

c) How does the verifier check the response message?

To test the response message, the server repeats the client's actions. The server takes the challenge message it sent to the user, appends the user's password, which it also knows, and applies the same hashing algorithm the supplicant used. (Recall that hashing is repeatable.) If the server's hash is identical to the response message, then the user must know the account's password (6). The server logs in the authenticated user.

d) What type of encryption does MS-CHAP use? (This is a tricky question but an important one.)

MS-CHAP does not use encryption at all; it uses hashing and the common secret password to authenticate.

e) In MS-CHAP, does the server authenticate itself to the client?

In MS-CHAP, the server does not authenticate itself to the client.

The Keying Stage

Session Keys

Public Key Encryption for Confidentiality

21. a) When Alice sends a message to Bob, what key will she use to encrypt the message?

Bob's public key.

b) Why is "the public key" not a good answer to Question 21a?

You need to be very specific about which public key will be used. Since Alice is sending a message for Bob to see, she should use Bob's public key so that Bob can use his private key to decrypt.

c) What key will Bob use to decrypt the message?

Bob will use his own private key to decrypt the message.

d) Why is "the private key" not a good answer to Question 21b?

Everyone has a public key and a private key. You must always specify whose public or private key you are talking about. For example, Alice used Bob's public key to encrypt the message, so only *Bob's* private key is going to be able to decrypt the message properly. Alice's private key will not do it.

e) In a classroom with 30 students and a teacher, how many public keys will there be?

30

f) How many private keys?

30

22. a) What is the main drawback to public key encryption?

Because it is extremely complex, public key encryption is slow and expensive to use.

b) What is the most popular public key encryption cipher?

RSA

c) What is the other commonly used public key encryption cipher?

ECC (elliptic curve cryptography) is increasing in use.

d) Which need to be longer—symmetric keys or public keys? Justify your answer.

Because public-private key pairs rarely change, they must be longer than symmetric keys (which are briefly used during sessions) in order to avoid cracking.

e) How long are strong RSA keys?

1,024 bits

f) How long are strong ECC keys?

512 bits

23. Julia encrypts a message to David using public key encryption for confidentiality. After encrypting the message, can Julia decrypt it?

No. Only David can decrypt it because only David knows his private key.

Symmetric Key Keying Using Public Key Encryption

24. Explain how public key encryption can facilitate symmetric session key exchange.

It can be used in keying. One party creates a symmetric session key, then encrypts the key with public key encryption and sends it to the other party.

Symmetric Key Keying Using Diffie-Hellman Key Agreement

25. a) What is the purpose of Diffie-Hellman key agreement?

Keying

b) Can an attacker who captures the exchanged keying information compute the symmetric session key?

No

Message-by-Message Authentication

Electronic Signatures

Public Key Encryption for Authentication

26. a) In public key encryption for authentication, which key does the supplicant use to encrypt?

The supplicant uses his/her own private key to encrypt the message.

b) Does the verifier decrypt the ciphertext with the supplicant's public key? (If not, explain what key it does use.)

No, the verifier uses the true party's public key to decrypt the message sent by the supplicant. Using the supplicant's private key would always authenticate the impostor.

c) Who is the true party?

The true party is the person the supplicant claims to be.

d) What does the sender attempt to prove it knows that only the true party should know?

The sender attempts to prove it knows the true party's private key.

Message-by-Message Authentication with Digital Signatures

27. a) In public key authentication, what must the sender know that an impostor should not be able to learn?

The true party's private key

b) For what type of authentication is a digital signature used—initial authentication or message-by-message authentication?

Digital signatures are used for message-by-message authentication.

c) How does the supplicant create a message digest?

The supplicant creates the message digest by hashing the plaintext message.

d) How does the supplicant create a digital signature?

The supplicant creates a digital signature by encrypting the message digest with its own private key.

e) In public key encryption, what is "signing?"

Signing is the act of encrypting the message digest with its own private key.

f) What combined message does the supplicant send?

It is the digital signature plus the plaintext

g) How is the combined message encrypted for confidentiality?

The sender will use symmetric key encryption.

h) How does the verifier check the digital signature?

The verifier checks the digital signature by hashing the plaintext message with the same algorithm used by the sender. The verifier then decrypts the digital signature it received with the true party's public key, resulting in a message digest. The verifier compares the two message digests – if they are the same, then it's good-to-go.

i) Does the verifier use the sender's public key or the true party's public key to test the digital signature?

The verifier must use the true party's public key to test the digital signature.

28. a) Besides authentication, what security benefit does a digital signature provide?

Digital signatures also provide message integrity.

b) Explain what this benefit means.

If the message is changed in transit, the receiver has the ability to reject the altered message.

c) Do most message-by-message authentication methods provide message integrity as a by-product?

Yes. Message digests will change if the message has been altered. Thus, message-by-message authentication does provide message integrity as a by-product.

29. a) Contrast the key the sender uses for encryption in public key encryption for confidentiality and public key encryption for authentication.

In public key encryption for confidentiality, the sender uses the public key of the recipient in the cipher. In public key encryption for authentication, the sender uses its own private key to create a digital signature that can be read by its true party public key.

b) Contrast the key the receiver uses for decryption in public key encryption for confidentiality and public key encryption for authentication. (Careful!)

The receiver decrypts with the *receiver's private key*, which only the receiver knows. The receiver (verifier) then decrypts the message with the *true party's public key*.

Digital Certificates

30. a) From what kind of organization can a verifier receive digital certificates?

The certificate authority (CA)

b) Are most CAs regulated?

CAs in many countries are not regulated, thus the verifier must only accept digital certificates from CAs it trusts by reputation.

c) Does a digital certificate indicate that the person or firm named in the certificate is trustworthy? Explain.

A digital certificate does not indicate that a person is honest, just that he or she has a certain public key.

31. a) What are the two most critical fields in the digital certificate?

The name of the true party and the true party's public key

b) What field in a digital certificate allows the receiver of a certificate to determine if the certificate has been altered?

The verifier can use the CA's well-known public key to test the digital certificate's digital signature; if the test works, the digital certificate is authentic and unmodified.

c) What three things must the receiver of a digital certificate check to ensure that a digital certificate is valid?

First, the verifier must check that the digital certificate is authentic and has not been modified.

Second, each digital certificate has dates before and after which it is not valid. The receiver must check whether the digital certificate is in its valid period.

Third, even during a digital certificate's valid period, a certificate authority may revoke a digital certificate.

d) What are the two ways to check a certificate's revocation status?

Although CRLs work, the CRLs of large certificate authorities are quite long. Downloading and checking a long CRL can significantly delay the start of communication. Fortunately, most CAs offer a more streamlined way to check the CRL. This is the Online Certificate Status Protocol (OCSP). Using OCSP, a program can simply send in the serial number of a digital certificate to the CA. The CA will send back a response saying whether the serial number is good, revoked, or unknown.

32. a) Does a digital signature by itself provide authentication? Explain why or why not.

A digital signature is simply something that the sender has produced. It only provides authentication when tested with the public key of the true party, which is found in the true party's digital certificate.

b) Does a digital certificate by itself provide authentication? Explain why or why not.

A digital certificate by itself does not provide authentication. Certificates provide the public key of the true party, but anyone can have the true party's public certificate, so something else (the digital signature) is needed.

c) How are digital signatures and digital certificates used together in authentication?

Digital signatures and certificates must be used together to provide authentication. The digital certificate provides the public key that the authentication method, the digital signature, uses to authenticate the applicant.

Key-Hashed Message Authentication Codes (HMACs)

33. a) What two cryptographic protections does an HMAC provide?

Authentication and message integrity

b) Do HMACs use symmetric key encryption, public key encryption, or hashing?

HMACs use a combination of hashing and symmetric key encryption.

Hashing

c) What is the benefit of HMACs over digital signatures?

HMACs are much faster and less expensive than using PKE and digital signatures, which is important during the exchange of a large number of messages during a session.

Nonrepudiation

34. a) Why can't HMACs provide nonrepudiation?

HMACs fail to give nonrepudiation because the sender and receiver *both* know the secret key. Consequently, the alleged sender could argue in court that the receiver could have forged the HMAC on the message; so the HMAC did not prove that the sender, in fact, sent it.

b) Why is it usually not a problem that HMACs fail to provide nonrepudiation?

Nonrepudiation is usually dealt with at the application layer. As long as the application document is nonrepudiable, it does not matter whether the packets that transmit it are repudiable.

Replay Attacks and Defenses

35. a) What is a replay attack?

It's where an adversary intercepts an encrypted message and transmits it again later.

b) Can the attacker read the contents of the replayed message?

No, they can only retransmit the message.

c) Why are replay attacks attempted?

Replay attacks are attempted because in poorly designed cryptographic systems, an attacker can record an encrypted set of commands to log in or do something else, then play them back to create the same response.

d) What are the three ways to thwart replay attacks?

Three ways to thwart replay attacks include 1) including a time stamp on each message so they cannot be recycled, 2) using sequence numbers in each encrypted message so the receiver knows to delete a message with the same sequence number of an earlier message, and 3) including a nonce (randomly generate number) in each client request. The nonce is never reused, thus if it receives a message with a repeat nonce, it is a bad message.

e) How do time stamps thwart replay attacks?

Time stamps thwart replay attacks by ensuring "freshness." If an attacker transmits a message that is older than a preset cutoff value, the receiver rejects it.

f) How do sequence numbers thwart replay attacks?

Sequence numbers thwart replay attacks because by examining sequence numbers, the receiver can detect a retransmitted message. The replayed message will have the sequence number of the earlier original message.

g) How do nonces thwart replay attacks?

Nonces thwart replay attacks because the client never uses the same nonce twice. The response from the server includes the same nonce sent in the request. By comparing a nonce in a request with previous nonces, the server can ensure that the request is not a repeat of an earlier one. The client, in turn, can ensure that the response is not a repeat of a previous response.

h) In what types of applications can nonces be used?

Nonces can only be used in applications that rely entirely (or almost entirely) on request-response client/server interactions.

Quantum Security

36. a) What is quantum key distribution?

It's a way to deliver enormously long keys to communication partners.

b) What are the two advantages of quantum key distribution?

The two advantages of quantum key distribution are 1) quantum keys are enormously long and make traditional forms of key cracking useless, and 2) it becomes quickly apparent if someone tries to intercept and inject bad messages into a stream, and thus can be easily discarded.

c) Why is quantum key cracking a major threat to many traditional cryptographic methods?

Because quantum computing offers the potential of being able to crack keys that are hundreds or thousands of bits long in a very short time, tradition cryptographic methods would no longer be secure using today's accepted strong key lengths.

CRYPTOGRAPHIC SYSTEMS

37. a) What is the definition of a VPN?

It's a cryptographic system that provides secure communication over an untrusted network.

b) Why do companies transmit over the Internet?

Companies transmit over the Internet because the Internet is effectively omnipresent and the cost-per-bit transferred is so low that it makes economic sense compared to the more expensive transmission over WAN technologies such as Frame Relay.

c) Why do they transmit over untrusted wireless networks?

VPNs on wireless LANs, in turn, allow a company to enjoy the benefits of mobility despite the questionable security of many WLANs, especially those in wireless hot spots.

d) Distinguish between the three types of VPNs.

A host-to-host VPN connects a single client over an untrusted network to a single server. A remote access VPN connects a single remote PC over an untrusted network to a site network. Site-to-site VPNs protect all traffic flowing over an untrusted network between a pair of sites.

e) What does a VPN gateway do for a remote access VPN?

Remote access users connect to a VPN gateway, which authenticates them and gives them access to authorized resources within the site. Note that this gateway gives remote users access to multiple computers within the site, while a host-to-host VPN only gives you access to a single computer.

f) What does a VPN gateway do for a site-to-site VPN?

With site-to-site VPNs, sending VPN gateways encrypt outgoing messages. Receiving VPN gateways then decrypt incoming messages and pass these messages to the correct destination hosts in the receiving site.

g) Which types of VPNs use VPN gateways?

Remote access and site-to-site VPNs use VPN gateways.

The types of VPNs that use VPN gateways are remote access VPNs and site-to-site VPNs.

SSL/TLS

38. a) Distinguish between SSL and TLS.

When you make a purchase over the Internet, your sensitive traffic is almost always protected by a cryptographic system standard that was originally called Secure Sockets Layer (SSL) when the Netscape Corporation created it. Netscape passed the standardization effort to the IETF, which renamed the standard Transport Layer Security (TLS) to emphasize that it works at the transport layer.

b) For what type of VPN was SSL/TLS developed?

Host-to-host VPNs

c) For what type of VPN is SSL/TLS increasingly being used?

Remote access VPN

39. a) At what layer does SSL/TLS operate?

SSL/TLS operates at the transport layer.

b) What types of applications can SSL/TLS protect?

SSL/TLS only protects SSL/TLS-aware applications that have been specifically created to work with SSL/TLS.

c) What are the two commonly SSL/TLS-aware applications?

Web applications and e-mail

d) Why is SSL/TLS popular?

Every computer has a browser, and all browsers are SSL/TLS-aware. This means there is no setup on clients. Also, all webservers and most mailservers know how to work with SSL/TLS.

40. a) SSL/TLS was created for host-to-host (browser-webserver) communication. What device can turn SSL/TLS into a remote access VPN?

The SSL/TLS border gateway

b) In SSL/TLS remote access VPNs, to what device does the client authenticate itself?

In SSL/TLS remote access VPNs, the client authenticates itself to a SSL/TLS gateway.

c) When a remote client transmits in an SSL/TLS VPN, how far does confidential transmission definitely extend?

Confidential transmission in an SSL/TLS VPN extends between the client's browser and SSL/TLS gateway.

d) What three services do SSL/TLS gateways commonly provide?

Access to internal webservers

Webification for nonweb applications, such as database applications

Access to internal subnets

e) What is webification?

It is converting messages into webpages for the browser to present to the user.

f) What software does the client need for basic SSL/TLS VPN operation?

Only a Web browser

g) For what purposes may the client need additional downloaded software?

To allow clients transparent access to a subnet and to erase browsing history on a PC while traveling

h) Why may installing the additional downloaded software on the browser be problematic?

Installing additional downloaded software usually requires administrator access on a PC. Internet cafes and other public computers do not allow administrator access for general users, and thus may not be able to access the servers.

i) Why is SSL/TLS attractive as a remote access VPN technology?

It can provide remote access to almost any PC without modification or configuration because only a browser is needed.

j) What problems do companies face if they use it as a remote access VPN technology?

SSL/TLS implementation has a tendency to be limited and clumsy, with unstandardized SSL/TLS gateways. Using remote access VPNs requires strong due diligence with respect to needs assessment and product analysis, as well as a significant interaction by the networking staff.

k) Which of the three types of VPNs can SSL/TLS support?

SSL/TLS can support the host-to-host and remote access VPNs. SSL/TLS cannot support site-to-site VPNs.

IPSEC

41. a) At what layer does IPsec operate?

It operates at the internet layer.

b) What layers does IPsec protect?

The internet, transport, and application layer

c) Compare the amount of cryptographic security in IPsec with that in SSL/TLS.

With SSL/TLS, there is only security to applications that are SSL/TLS-aware, while IPsec protects everything in the data field within the IP packet.

d) Compare centralized management in IPsec and SSL/TLS.

SSL/TLS has no central management. IPsec, in contrast, can centrally manage IPsec on all connections between hosts.

e) Why is IPsec's transparent protection attractive compared with SSL/TLS' non-transparent protection?

SSL/TLS works at the transport layer and does not give transparent protection to application layer messages. IPsec works at the internet layer and gives transparent protection to transport layer and application layer messages.

f) Which versions of IP can use IPsec?

Versions 4 and 6

IPsec Transport Mode

IPsec Tunnel Mode

42. a) Distinguish between transport and tunnel modes in IPsec in terms of packet protection.

IPSec transport mode provides end-to-end, host-to-host VPN security. IPsec tunnel mode only protects traffic between two IPsec gateways at different sites.

b) What are the attractions of each?

The attraction of IPsec transport mode is that it provides the most complete, end-to-end protection. The attraction of IPsec tunnel mode is that it is cheaper to implement IPsec between IPsec gateways than all possible clients and servers between different sites. Also, IPsec tunnel mode is firewall-friendly.

c) What are the problematic issues of each?

IPsec transport mode requires that each client and server be set up with a private key-digital certificate pair, placing the private key on each computer and then managing the digital certificates over its life cycle.

Thus, the implementation and management overhead of IPsec transport mode is high. Additionally, IPsec transport mode encrypts all IP traffic, not allowing firewalls to filter individual packets. IPsec tunnel mode is cheaper to implement and maintain, but does not provide full end-to-end protection like the transport mode.

IPsec Security Associations (SAs)

43. a) What does an SA specify? (Do not just spell SA out.)

It is an agreement about what IPsec security methods and options two hosts or two IPsec gateways will use. A security association in IPsec is reminiscent of an SSL/TLS cipher suite.

b) When two parties want to communicate in both directions with security, how many IPsec SAs are necessary?

Security Associations (SAs) are required in each direction of communication. Thus, for two parties to communicate in both directions with security, two IPsec SAs are required.

c) May there be different SAs in the two directions?

Yes

d) What is the advantage of this?

The advantage of using two different SAs in two directions is that a different level of protection may be allowed in each direction. Thus, more sensitive communication transmissions may be assigned stronger IPsec protections.

e) Why do companies wish to create policies for SAs?

Companies wish to create policies for SAs because some cryptographic security standards are inadequate for a company's security needs. Creating a policy for SAs ensures that a company creates SAs that meet acceptable security standards on all applicable devices.

f) Can they do so in SSL/TLS?

No, SSL/TLS does not allow companies to create and enforce policies.

g) How does IPsec set and enforce policies?

IPsec sets and enforces policies via the use of IPsec policy servers that push a list of suitable policies to individual IPsec gateway servers or hosts.

Conclusion

Synopsis

Thought Questions

1. The total processing speed of microprocessors (based on clock rate and number of circuits) is doubling roughly every year. Today, a symmetric session key needs to be 100 bits long to be considered strong. How long will a symmetric session key have to be in 30 years to be considered strong? (Hint: Consider how much longer decryption takes if the key length is increased by a single bit.)

   Only 130 bits long. Each additional bit doubles the effective search time, so only one bit must be added each year.

2. Longer keys are more difficult to crack. Most symmetric keys today are 100 to 300 bits long. Why don't systems use far longer symmetric keys—say, 1,000 bit keys?

   The longer the key, the more processing power and RAM it takes to operate. Thus, it makes sense for systems to use the minimum key length for a given threat, and 100 to 300 is considered very strong at this time.

3. Brute force is used to crack a 100-bit key. The key is cracked in only 5,000 tries. How can this be?

   On average, it will take many tries to crack a 100-bit key. However, the cracking process is random, so the key may be found much more quickly (or more slowly).

4. In practice, public key authentication is used heavily for initial authentication but rarely for message-by-message authentication. Given the intense processing power required for public key authentication and the fact that public key authentication gives the strongest authentication, explain these two usage patterns.

   The verifier would send a challenge message in the clear.

   The supplicant would encrypt the challenge message with the supplicant's own private key, creating the response message.

   The supplicant would send the response message to the verifier.

   The verifier would decrypt the response message with the true party's public key. If this results in the challenge message, the supplicant must be the true party.

5. Did we see symmetric key encryption used for authentication in this chapter? If so, how was it used?

   No. It is only used in encryption for confidentially.

6. Describe the entries in the second row of **Error! Reference source not found.**. Comment on the strengths of the choices it uses.

Uses public key authentication (RSA) for initial authentication. Only export-grade authentication, so not strong initial authentication.

The same for digital signatures.

For symmetric key encryption, uses RC4 with 40-bit keys. Weak key length.

Uses MD5 for HMACs. MD-5 is a vulnerable algorithm.

a) For the second-to-last row of **Error! Reference source not found.**, comment on the strengths of its symmetric encryption cipher and of its hashing algorithm.

For symmetric key encryption, uses 3DES. Strong, but very slow.

Uses SHA-1 for HMACs. This is vulnerable.

b) Describe the entries in the last row of **Error! Reference source not found.**. Comment on the strengths of the choices it uses.

Uses public key authentication (RSA) for initial authentication. Strong initial authentication.

The same for digital signatures.

For symmetric key encryption, uses AES with 256-bit keys. Very strong.

Uses SHA-256 for HMACs. Very strong.

7. How are digital certificates and drivers' licenses similar, and how are they different?

Similar

- Issued by an authority
- Associate a name with an identifier
- Time limitation
- Can be checked for revocation

Different

- Named person has permission to drive and perhaps limitations (e.g., corrective lenses, etc.)
- Picture verification
- Driver's license cannot be used for remote verification

8. How are digital certificates and passports similar, and how are they different?

Similar

- Time limitation

Different

- Named person is a citizen of a country
- Picture verification, sometimes biometrics

9. How are digital certificates and university diplomas similar, and how are they different?

Similar

- Bearer may not be the named party

Different

Named party has a degree

Digital certificates can be checked for validity more easily

10. How are digital certificates and movie tickets similar, and how are they different?

Similar

Expiration date

Different

Bearer is entitled to enter theater

Tickets: verification of identity is irrelevant

11. Identify potential security threats associated with authentication via digital signatures and digital certificates. Explain each and describe how you would address each threat.

Someone applies for a digital certificate fraudulently and gets it. Strong independent authentication is needed before certificates are given out.

The CA is a fake company. Only accept the certificates of CAs you trust.

Someone in a legitimate CA fraudulently issues a false certificate.

An attacker obtains the true party's private key. This will allow the attacker to impersonate the individual, and the individual's digital certificate will "authenticate" the key thief. Revoke the digital certificate immediately and require that all users do certificate revocation checking whenever they do authentication via digital certificates and digital signatures.

An attacker can walk up to the user's computer or plant a Trojan horse or other malware that takes over the user's computer. The attacker can then use the private key stored on the user's computer.

A digital certificate can be modified. If the verifier does not check the certificate's digital signature, this change will go undetected.

If key lengths are short, cryptanalysis will be possible.

12. The chapter described how public key authentication is used for message-by-message authentication in digital signatures. However, public key authentication is widely used for *initial* authentication. Describe the processes that the supplicant and verifier would use if public key encryption were used in initial challenge-response authentication. Draw heavily on your understanding of digital signatures, but put this information in challenge–response context.

The verifier would send a challenge message to the supplicant.

The supplicant would encrypt the challenge message with its own private key. It would send this response message to the verifier.

The verifier would decrypt the response message with the true party's public key. If the verifier learns the true party's public key through a digital certificate supplied by a certificate authority, it must verify the digital certificate.

If the decrypted response message matches the original challenge message, the supplicant must know the true party's private key and so must be the true party. The supplicant is authenticated.

13. If a supplicant gives you a digital certificate, should you accept it? Explain. (Think about this carefully. The answer is not obvious.)

    Yes. The digital signature in the digital certificate will let you know if the digital certificate was altered to replace the true party's public key with an impostor's public key.

14. Pretty Good Privacy (PGP) uses public key encryption *and* symmetric key encryption to encrypt long documents. How might this be possible?

    PGP first encrypts the document with a symmetric key.

    It then uses public key encryption to encrypt the symmetric key.

    Finally, PGP adds the encrypted symmetric key to the document.

    The receiver decrypts the symmetric key with the receiver's own private key.

    The receiver then uses the decrypted symmetric key to decrypt the document encrypted with the symmetric key.

Hands-On Projects

NOTE: Screenshots for individual students will vary.

PROJECT 1

AxCrypt® is a great third-party encryption tool. You just select the files you want encrypted, enter your password, and you're done. It is even available as an option in the shortcut menu when you right-click a file. AxCrypt will automatically re-encrypt the file after you are done modifying it. It uses 128-bit AES and is completely free. Let's look at some of the functionality built into AxCrypt.

1. Download AxCrypt from http://www.axantum.com/AxCrypt.
2. Click Download.
3. Click on the appropriate version for your operating system.
4. Click Save.
5. Select your download folder.
6. If the program doesn't automatically open, browse to your download folder.
7. Right-click AxCrypt-Setup.exe.
8. Click Run as administrator.
9. Click Yes if prompted.
10. Click I Agree.
11. Click Custom Installation.
12. Deselect all the bloatware (from Amazon).
13. Click Install.
14. Deselect Register.

15. Click Finish.
16. Save all your work, exit all other programs, and reboot your computer. Once your computer is rebooted you can continue on to the next step.
17. Right-click your desktop.
18. Click New and Text Document.
19. Name the file YourName.txt. Replace YourName with your first and last name.
20. Right-click the file named YourName.txt.
21. Select AxCrypt, and Encrypt.
22. Enter the password "tiger1234" (without quotes).
23. Click OK.
24. Double-click the new YourName-txt.axx file you just created.
25. Enter the password "tiger1234" (without quotes).
26. Click OK.
27. Close the text file that you just opened.
28. Take a screenshot of your desktop showing the newly created files.
29. Right-click the file named YourName-txt.axx.
30. Select AxCrypt and Decrypt.
31. Enter the password "tiger1234" (without quotes).
32. Click OK.
33. Right-click the file named YourName.txt. (This time you're going to make an executable file that can be opened by anyone. They won't have to have Axcrypt installed on their computer to be able to open the .exe.)
34. Select AxCrypt, and Encrypt copy to .EXE.
35. Enter the password "tiger1234" (without quotes).
36. Click OK.
37. Take a screenshot of your newly created YourName-txt.exe file.

PROJECT 2

This project uses an Enigma® machine simulator. It functions like the Enigma machines used during WWII. This example has been included to help you better understand how encryption worked in the early days. It's a great learning tool for when you first start exploring the subject of cryptography. Enigma machines provided fairly good encryption strength for their day. Modern cryptographic systems are much more secure than Enigma machines.

Pay attention to the colored paths as you type. The red path goes through the three rotors, bounces off the reflector, becomes green, and then goes back through the three rotors. The right rotor moves with each keystroke. If it completes one full cycle, it will advance the middle rotor and subsequently the left rotor.

1. Open a Web browser and go to http://enigmaco.de/enigma/enigma.swf.
2. Use the left and right arrows to move each of the top three rotors so that each has the letter "A" selected in blue.
3. Click in the Input text box in the bottom of your screen.
4. Slowly type your first name and last name without a space. (In this case it was RandyBoyle. If you make a typing error you can start over by pressing the backspace key.)

5. Take a screenshot.
Note: The text in the Input text box is what you typed. The text in the Output text box is what you would send. You are now going to reset the dials to their original position (in this case AAA) and type the encrypted text (cipher text) you produced in the Output text box. You can copy the cipher text from the screenshot you just took. Subsequently, you should see your name reproduced in the bottom box. This is the equivalent of decrypting the message.
6. Click in the Input text box and backspace your name. (The rotors should be set back to their AAA position.)
7. Refer back to the screenshot you just took and copy down the output (cipher text). (In this case, the cipher text for "RANDYBOYLE" was "VDOLZYMEAC.")
8. Type the cipher text into the Input text box. (Type slowly so you won't make a mistake and have to start over!)
9. Take a screenshot with your name showing in the Output text box.
10. Backspace the text in the Input text box.
11. Slowly press the A key ten times and notice how a different encrypted letter is chosen as output through the rotating dials even though you are hitting the same key each time.
12. Take a screenshot.

Project Thought Questions

1. Why would you need an encrypted file that self-extracts (.exe)?

   The person receiving the file won't need to have AxCrypt on his or her machine in order to open the encrypted file.

2. Will AxCrypt work on multiple files or entire directories (folders)?

   Yes, it will encrypt multiple files and/or directories at a single time.

3. Even if you encrypted a file with AxCrypt, wouldn't someone be able to recover a previous version of the file with a file recovery program? Hint: AxCrypt has a built-in shredder.

   No, AxCrypt permanently shreds the file by wiping the disk space where the file was stored. They won't be able to recover the file once it is encrypted or moved.

4. Could your network administrator open these files after you encrypted them with AxCrypt? Why not?

   It's unlikely that your network administrator will be able to open these files given the level of encryption used by AxCrypt. It would take them many years to crack this level of encryption because of the key length and lack of enough computational cycles.

5. Why did Enigma machines use multiple rotors?

   The use of multiple rotors increased the overall key strength. The movement of rotors performed simple substitution by identifying a

corresponding letter via a changing electrical pathway (polyalphabetic substitution).

6. How did WWII cryptographers know which rotor settings to use?

   Code books were issued that told the sender/receiver which rotors to use, and also indicated the initial position setting.

Case Discussion Questions

1. How could Bloomberg insiders use terminal data to front-run traders?

   Bloomberg insiders could use terminal data to determine trades, trade sentiment, potential deals, etc. before they happened. Insiders could use this information to "front-run" or make trades in advance of events they knew were going to happen.

2. How should Bloomberg handle questions about its ability to protect traders' data?

   Bloomberg needs to quickly and confidently show that they protect traders' data in order to show that they are technically competent to secure their data, and trustworthy to not divulge any confidential data. It needs to show traders that it is doing everything possible to protect their terminal users.

3. How could Bloomberg use encryption to calm trader's fears?

   Bloomberg could implement fully-encrypted communication protocols for all of their products. They could also secure traders' data from internal users and allow an external firm to audit internal access to traders' data. They could also stop scanning messaging data.

4. Why is confidentiality important in a business-to-business relationship?

   Confidentially is important in most business relationships. In this case, the desire for confidentiality may stem from the need to keep deal-related information private. If insiders were able to glean information about a potential deal, they could make large sums of money at the expense of the parties making the deal.

5. Why does EFF publish a report about consumer privacy at large Internet companies?

   EFF publishes their annual privacy report in an effort to encourage companies to protect users' privacy from government overreach. On EFF's website, they indicate, "…but in today's increasingly digital world, online service providers serve as the guardians of our most intimate data — from email content to location information to our social and family connections. The policies adopted by these corporations will have deep and lasting ramifications on whether individual Internet users can communicate free from the shadow of government surveillance."

6. How might privacy concerns affect customer loyalty and new product adoption?

   Customers may be hesitant to sign up for new products or services if they feel the company will later sell their information. For example, the loss of a customer's information (e.g., phone number, etc.) may adversely affect him or her in terms of continual harassing phone calls to buy new products.

Perspective Questions

1. What was the most difficult section for you in this chapter?

   Student answers will vary.

2. What was the most surprising thing you learned in this chapter?

   Student answers will vary.