Computer Security Principles and Practice 4th edition Stallings Solutions Manual

SKU: 9780134794105-SOLUTIONS

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

CHAPTER 2 CRYPTOGRAPHIC TOOLS

ANSWERS TO QUESTIONS

2.1 Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

2.2 One secret key.

2.3 (1) a strong encryption algorithm; (2) Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

2.4 Message encryption, message authentication code, hash function.

2.5 An authenticator that is a cryptographic function of both the data to be authenticated and a secret key.

2.6 **(a)** A hash code is computed from the source message, encrypted using symmetric encryption and a secret key, and appended to the message. At the receiver, the same hash code is computed. The incoming code is decrypted using the same key and compared with the computed hash code. **(b)** This is the same procedure as in (a) except that public-key encryption is used; the sender encrypts the hash code with the sender's private key, and the receiver decrypts the hash code with the sender's public key. **(c)** A secret value is appended to a message and then a hash code is calculated using the message plus secret value as input. Then the message (without the secret value) and the hash code are transmitted. The receiver appends the same secret value to the message and computes the hash value over the message plus secret value. This is then compared to the received hash code.

2.7

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that H(x) = h.
5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

2.8 **Plaintext:** This is the readable message or data that is fed into the algorithm as input. **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext. **Public and private keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts. **Decryption algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

2.9 **Encryption/decryption:** The sender encrypts a message with the recipient's public key. **Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message. **Key exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

2.10 The key used in conventional encryption is typically referred to as a **secret key**. The two keys used for public-key encryption are referred to as the **public key** and the **private key**.

2.11 A **digital signature** is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

2.12 A **pubic-key certificate** consists of a public key plus a User ID of the key owner, with the whole block signed by a trusted third party. Typically, the third party is a certificate authority (CA) that is trusted by the user community, such as a government agency or a financial institution.

2.13 Several different approaches are possible, involving the private key(s) of one or both parties. One approach is Diffie-Hellman key exchange. Another approach is for the sender to encrypt a secret key with the recipient's public key.

ANSWERS TO PROBLEMS

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

2.1 Yes. The eavesdropper is left with two strings, one sent in each direction, and their XOR is the secret key.

2.2 a.

2	8	10	7	9	6	3	1	4	5
C	R	Y	P	T	O	G	A	H	I
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

4	2	8	10	5	6	3	7	1	9
N	E	T	W	O	R	K	S	C	U
T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D
I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

```
ISRNG  BUTLF  RRAFR  LIDLP  FTIYO  NVSEE  TBEHI  HTETA
EYHAT  TUCME  HRGTA  IOENT  TUSRU  IEADR  FOETO  LHMET
NTEDS  IFWRO  HUTEL  EITDS
```

b. The two matrices are used in reverse order. First, the ciphertext is laid out in columns in the second matrix, taking into account the order dictated by the second memory word. Then, the contents of the second matrix are read left to right, top to bottom and laid out in columns in the first matrix, taking into account the order dictated by the first memory word. The plaintext is then read left to right, top to bottom.

c. Although this is a weak method, it may have use with time-sensitive information and an adversary without immediate access to good cryptanalysis t(e.g., tactical use). Plus it doesn't require anything more than paper and pencil, and can be easily remembered.

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

2.3 a. Let -X be the additive inverse of X. That is -X $\boxed{+}$ X = 0. Then:

$$P = (C \boxed{+} -K_1) \oplus K_0$$

b. First, calculate –C'. Then –C' = (P' $\oplus$ K_0) $\boxed{+}$ (– K_1). We then have:

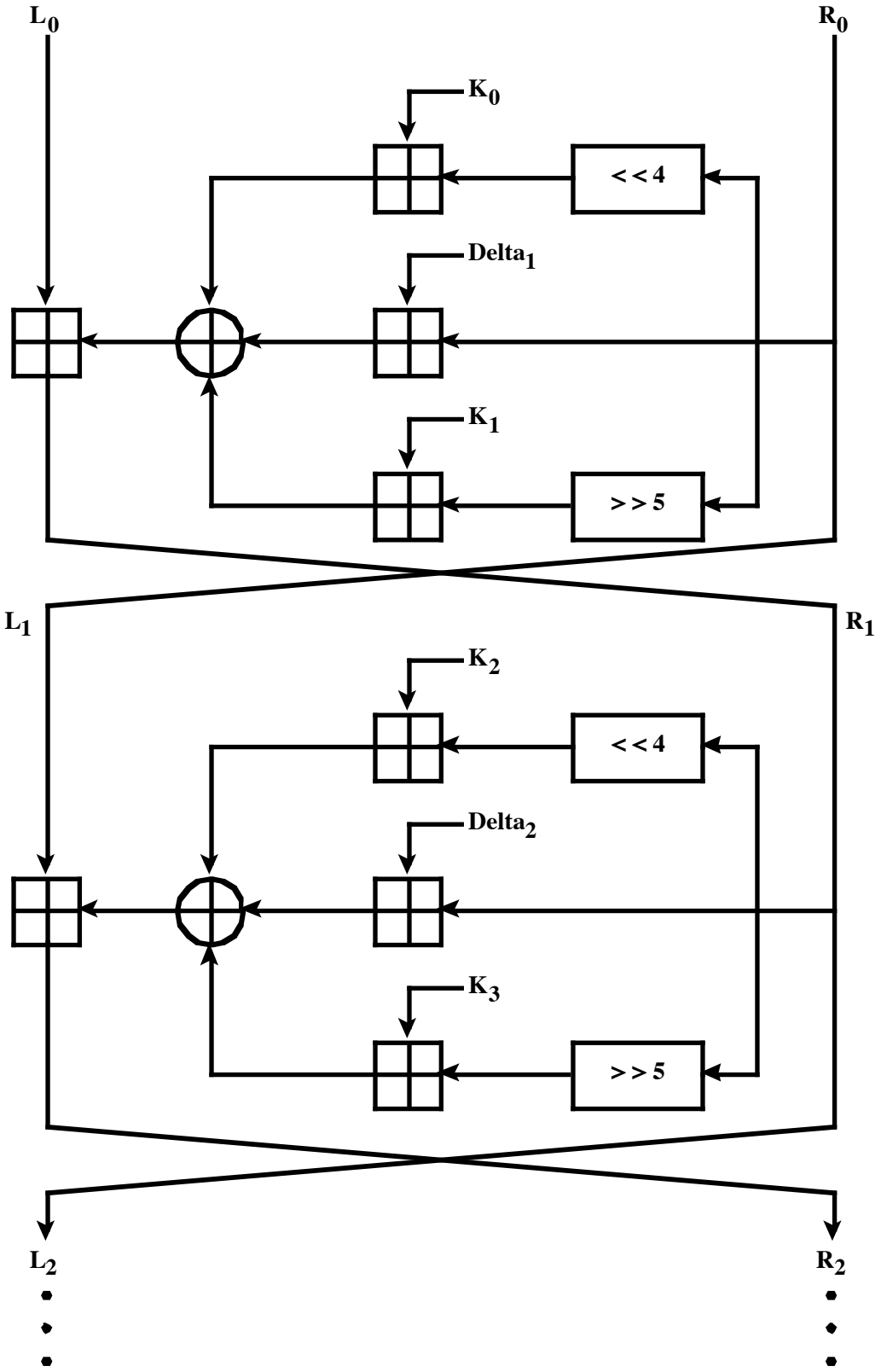
C $\boxed{+}$ –C' = (P $\oplus$ K_0) $\boxed{+}$ (P' $\oplus$ K_0)

However, the operations $\boxed{+}$ and $\oplus$ are not associative or distributive with one another, so it is not possible to solve this equation for K_0.

2.4 a. The constants ensure that encryption/decryption in each round is different.

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

b. First two rounds:



Computer Security Principles and Practice 4th edition Stallings Solutions Manual

c. First, let's define the encryption process:

$L_2 = L_0 \boxplus [(R_0 << 4) \boxplus K_0] \oplus [R_0 \boxplus \delta_1] \oplus [(R_0 >> 5) \boxplus K_1]$

$R_2 = R_0 \boxplus [(L_2 << 4) \boxplus K_2] \oplus [L_2 \boxplus \delta_2] \oplus [(L_2 >> 5) \boxplus K_3]$

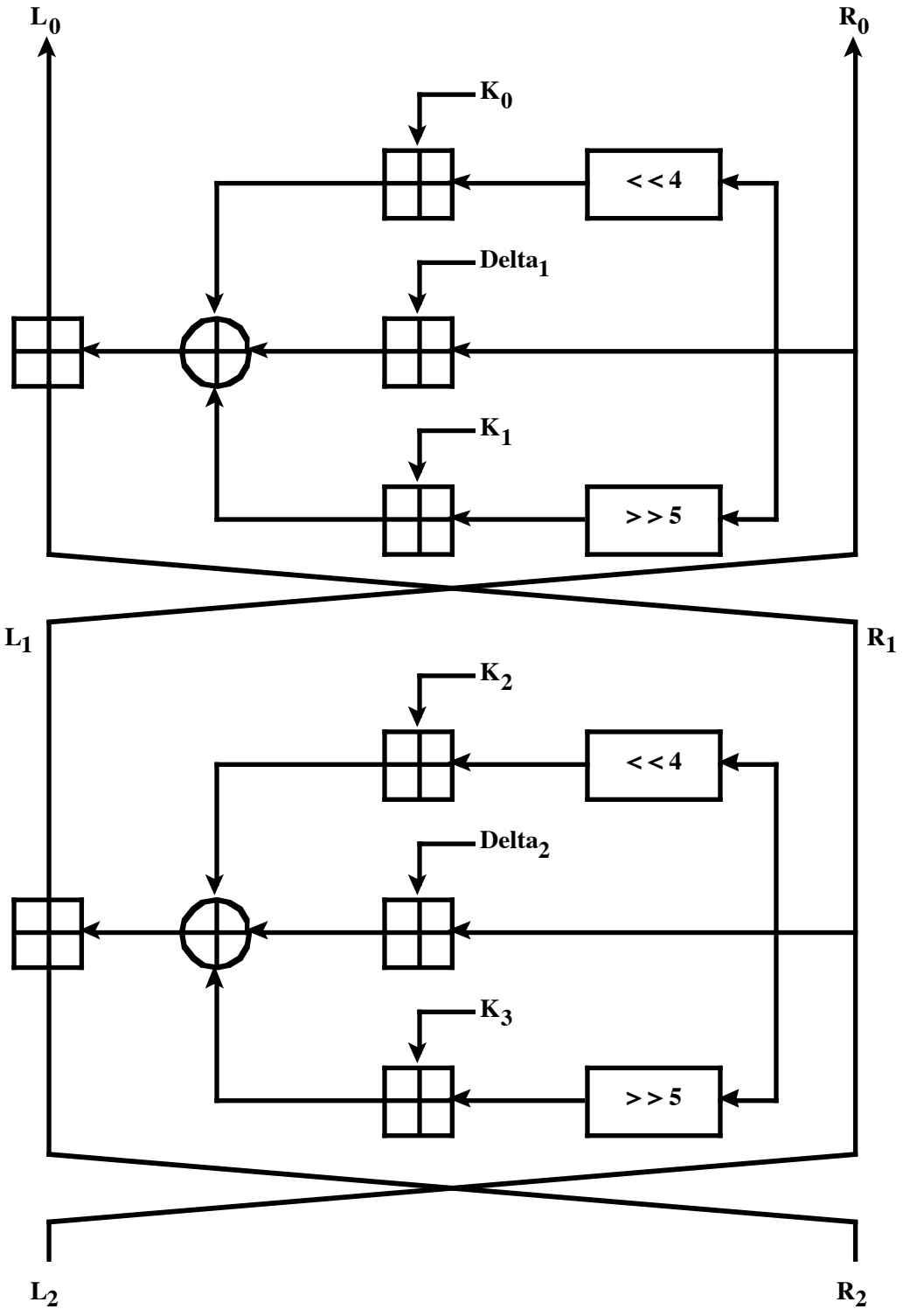
Now the decryption process. The input is the ciphertext (L_2, R_2), and the output is the plaintext (L_0, R_0). Decryption is essentially the same as encryption, with the subkeys and delta values applied in reverse order. Also note that it is not necessary to use subtraction because there is an even number of additions in each equation.

$R_0 = R_2 \boxplus [(L_2 << 4) \boxplus K_2] \oplus [L_2 \boxplus \delta_2] \oplus [(L_2 >> 5) \boxplus K_3]$

$L_0 = L_2 \boxplus [(R_0 << 4) \boxplus K_0] \oplus [R_0 \boxplus \delta_1] \oplus [(R_0 >> 5) \boxplus K_1]$

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

d.



2.5 **a.** Will be detected with both (i) DS and (ii) MAC.
b. Won't be detected by either (Remark: use timestamps).
c. (i) DS: Bob simply has to verify the message with the public key from both. Obviously, only Alice's public key results in a successful verification.

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

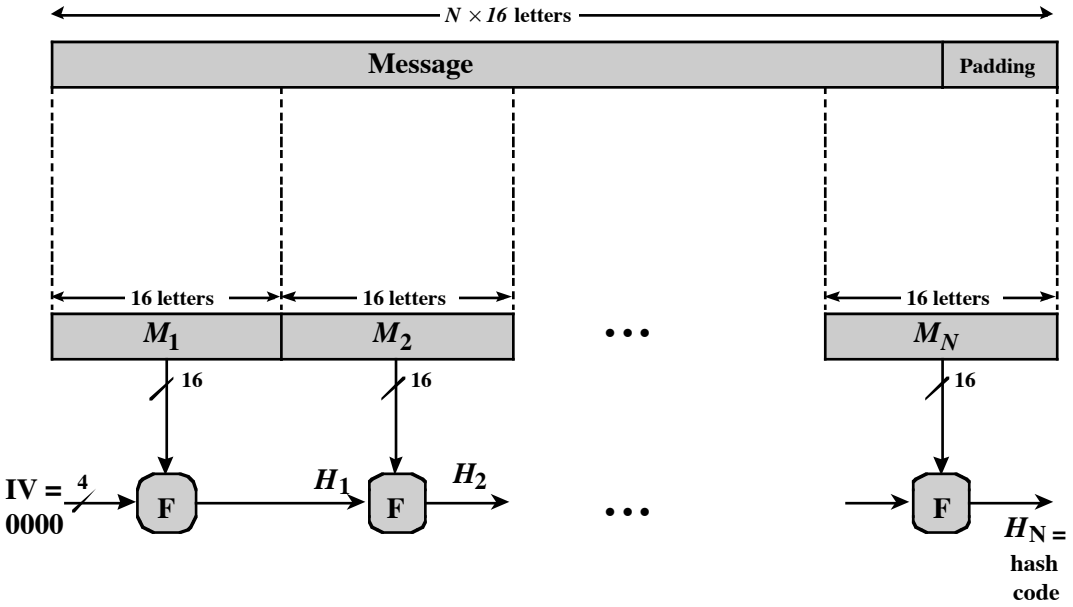
(ii) MAC: Bob has to challenge both, Oscar and Bob, to reveal their secret key to him (which he knows anyway). Only Bob can do that.

d. (i) DS: Alice has to force Bob to prove his claim by sending her a copy of the message in question with the signature. Then Alice can show that message and signature can be verified with Bob's public key) Bob must have generated the message.
(ii) MAC: No, Bob can claim that Alice generated this message.

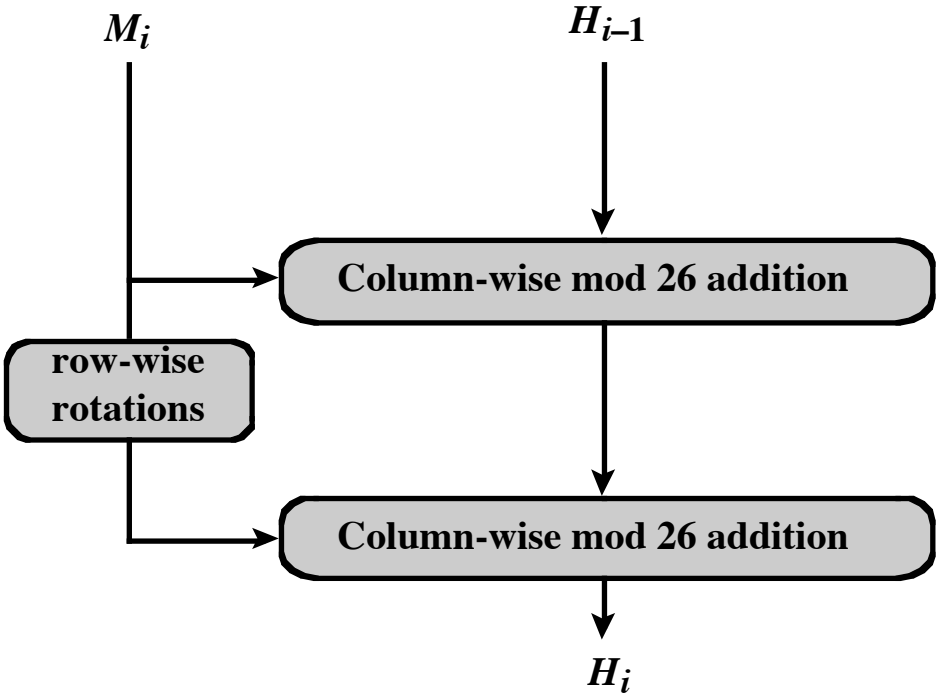
2.6 The statement is false. Such a function cannot be one-to-one because the number of inputs to the function is of arbitrary, but the number of unique outputs is 2^n. Thus, there are multiple inputs that map into the same output.

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

2.7 a. Overall structure:



Compression function F:



b. BFQG

c. Simple algebra is all you need to generate a result:

AYHGDAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

2.8

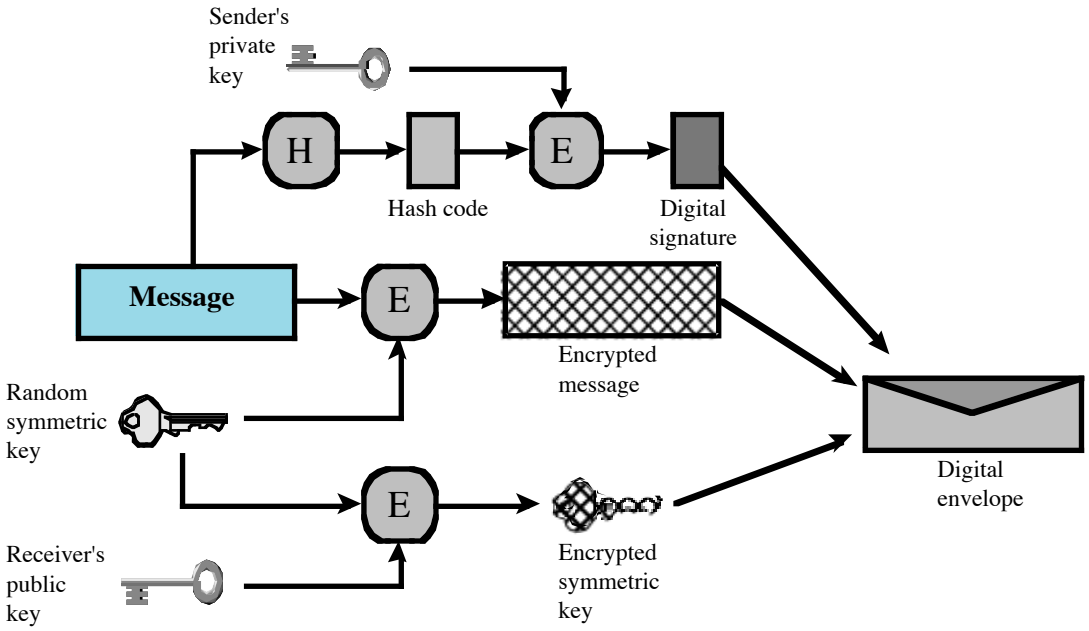
a. $M3 =$

5	2	1	4	5
1	4	3	2	2
3	1	2	5	3
4	3	4	1	4
2	5	5	3	1

b. Assume a plaintext message p is to be encrypted by Alice and sent to Bob. Bob makes use of M1 and M3, and Alice makes use of M2. Bob chooses a random number, k, as his private key, and maps k by M1 to get x, which he sends as his public key to Alice. Alice uses x to encrypt p with M2 to get z, the ciphertext, which she sends to Bob. Bob uses k to decrypt z by means of M3, yielding the plaintext message p.

c. If the numbers are large enough, and M1 and M2 are sufficiently random to make it impractical to work backwards, p cannot be found without knowing k.

2.9 We show the creation of a digital envelope:



Computer Security Principles and Practice 4th edition Stallings Solutions Manual

CHAPTER 3 USER AUTHENTICATION

ANSWERS TO QUESTIONS

3.1 **Something the individual knows:** Examples includes a password, a personal identification number (PIN), or answers to a prearranged set of questions.
Something the individual possesses: Examples include electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token.
Something the individual is (static biometrics): Examples include recognition by fingerprint, retina, and face.
Something the individual does (dynamic biometrics): Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.

3.2 We can identify the following attack strategies and countermeasures:
Offline dictionary attack: Typically, strong access controls are used to protect the system's password file. However, experience shows that determined hackers can frequently bypass such controls and gain access to the file. The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by that ID/password combination.
Specific account attack: The attacker targets a specific account and submits password guesses until the correct password is discovered.
Popular password attack: A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess.
Password guessing against single user: The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password.
Workstation hijacking: The attacker waits until a logged-in workstation is unattended.
Exploiting user mistakes: If the system assigns a password, then the user is more likely to write it down because it is difficult to remember. This situation creates the potential for an adversary to read the written password. A user may intentionally share a password, to enable a colleague to share files, for example. Also, attackers are frequently

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Suggested Reading Assignments

Computer Security
Fourth Edition

William Stallings
Lawrie Brown

Copyright 2018: William Stallings

Chapter 1 Overview

Anderson, J. *Computer Security Threat Monitoring and Surveillance.* Fort Washington, PA: James P. Anderson Co., April 1980.

Chapter 2 Cryptographic Tools

Schneier, B. "Why Cryptography is Harder Than It Looks." Information Security Bulletin, 1997

Chapter 3 User Authentication

Wagner, D., and Goldberg, I. "Proofs of Security for the UNIX Password Hashing Algorithm." Proceedings, ASIACRYPT '00, 2000.

Chapter 4 Access Control

Sandhu, R. "Lattice-Based Access Control Models." Computer, November 1993.

Barkley, J. "Comparing Simple Role-Based Access Control Models and Access Control Lists." Proceedings of the Second ACM Workshop on Role-Based Access Control, 1997.

Chapter 5 Database Security

Griffiths, P., and Wade, B. "An Authorization Mechanism for a Relational Database System." ACM Transactions on Database Systems, September 1976.

Chapter 6 Malware

Levine, J.; Grizzard, J.; and Owen, H. "A Methodology to Detect and Characterize Kernel Level Rootkit Exploits Involving Redirection of the System Call Table." Proceedings, Second IEEE International Information Assurance Workshop, 2004

Chapter 7 Denial of Service

Yuan, J., and Mills, K. "Monitoring the Macroscopic Effect of DDoS Flooding Attacks." IEEE Transactions on Dependable and Secure Computing, October-December 2005.

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Chapter 8 Intrusion Detection

Anagostakis, K., et al. "Detecting Targeted Attacks Using Shadow Honeypots." 14th USENIX Security Symposium, 2005.

Chapter 9 Firewalls

Ioannidis, S. "Implementing a Distributed Firewall." ACM CCS '00, 2000.

Guster, D "A Firewall Configuration Strategy for the Protection of Computer Networked Labs in a College Setting." Journal of Computing Sciences in Colleges, October 2001.

Chapter 10 Buffer Overflow

Levy, E., "Smashing The Stack For Fun And Profit." Phrack Magazine, file 14, Issue 49, November 1996.

Chapter 11 Other Software Security Issues

Miller, B.; Cooksey, G.; and Moore, F. “An Empirical Study of the Robustness of MacOS Applications Using Random Testing.” First International Workshop on Random Testing. Portland, Maine, ACM, 2006

Chapter 12 OS Security

Jiang, X., and Solihin, Y “Architectural Framework for Supporting Operating System Survivability” IEEE International Symposium on High-Performance Computer Architecture, 2011.

Chapter 16 Physical Security

Jones, D., et al. " Physical Security and Vulnerability Modeling for Infrastructure Facilities." Proceedings of the 39th Hawaii International Conference on System Sciences - 2006

Chapter 17 Human Resources

Siponen, N. "Five Dimensions of Information Security Awareness." Computers and Society, June 2001.

Chapter 18 Security Auditing

Zhou, J., and Vigna, G. "Detecting Attacks That Exploit Application-Logic Errors Through Application-Level Auditing." Proceedings, 20th Annual Computer Security Applications Conference (ACSAC'04), 2004.

Yongzheng, W., and Yap, H. "A User-level Framework for Auditing and Monitoring." Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), 2005.

Chapter 19 Legal and Ethical Aspects

Tavani, H. " Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace." Computers and Society, September 2000.

Leiwo, J., and Heikkuri, S. "An Analysis of Ethics as Foundation of Information Security in Distributed Systems." 31st Hawaiian International Conference on System Sciences, 1998.

Chapter 20 Symmetric Encryption

Blaze, M., et al. "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security." RSA Document, 1996.

RFC 1750 Randomness Recommendations for Security. December 1994

Chapter 21 Public-Key Cryptography

Asymmetric Encryption: Evolution and Enhancements
Cryptobytes Volume 2, No. 1 - Spring 1996

Chapter 22 Internet Security

Neuman, B. "Security, Payment, and Privacy for Network Commerce." IEEE Journal on Selected Areas in Communications, October 1995.

Chapter 23 Internet Authentication

Yu, T., et al. "The Perils of Unauthenticated Encryption: Kerberos Version 4." Proceedings of the Network and Distributed System Security Symposium. The Internet Society, February 2004

Chapter 24 Wireless Network Security

Welch, D., and Lathrop, S. "Wireless Security Threat Taxonomy." Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003

Chapter 27 Trusted Computing

Bell, D. "Looking Back at the Bell-Lapadula Model." Proceedings, 21st Annual IEEE Computer Security Applications Conference, 2005.

Mackenzie, D., and Pottinger, G. " Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the U.S. Military." IEEE Annals of the History of Computing, Vol. 19, No. 3, 1997

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Chapter 2

Cryptographic Tools

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption
- Two requirements for secure use:
  - Need a strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

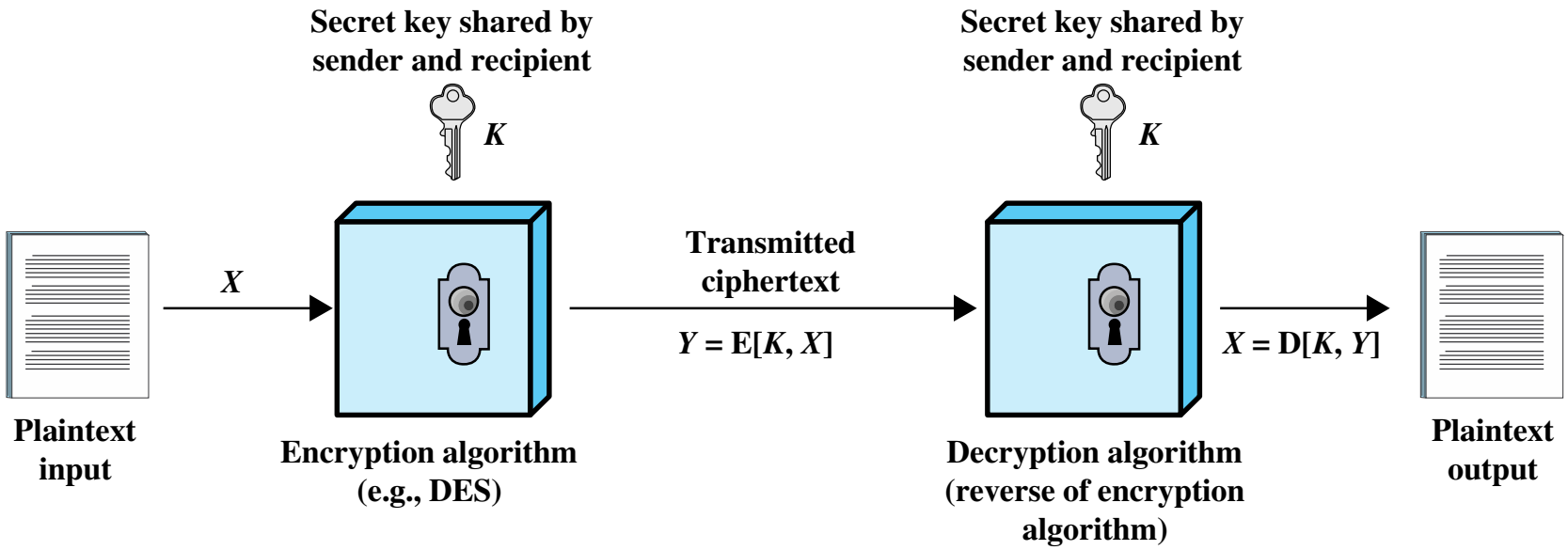


Figure 2.1 Simplified Model of Symmetric Encryption

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful all future and past messages encrypted with that key are compromised

Brute-Force Attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - On average half of all possible keys must be tried to achieve success

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Table 2.1

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Comparison of Three Popular Symmetric Encryption Algorithms

Data Encryption Standard (DES)



- Until recently was the most widely used encryption scheme
  - FIPS PUB 46
  - Referred to as the Data Encryption Algorithm (DEA)
  - Uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
- Strength concerns:
  - Concerns about the algorithm itself
    - DES is the most studied encryption algorithm in existence
  - Concerns about the use of a 56-bit key
    - The speed of commercial off-the-shelf processors makes this key length woefully inadequate

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Table 2.2

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Average Time Required for Exhaustive Key Search

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Triple DES (3DES)

- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
  - 168-bit key length overcomes the vulnerability to brute-force attack of DES
  - Underlying encryption algorithm is the same as in DES
- Drawbacks:
  - Algorithm is sluggish in software
  - Uses a 64-bit block size

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Advanced Encryption Standard (AES)

Needed a replacement for 3DES

3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

- Should have a security strength equal to or better than 3DES
- Significantly improved efficiency
- Symmetric block cipher
- 128 bit data and 128/192/256 bit keys

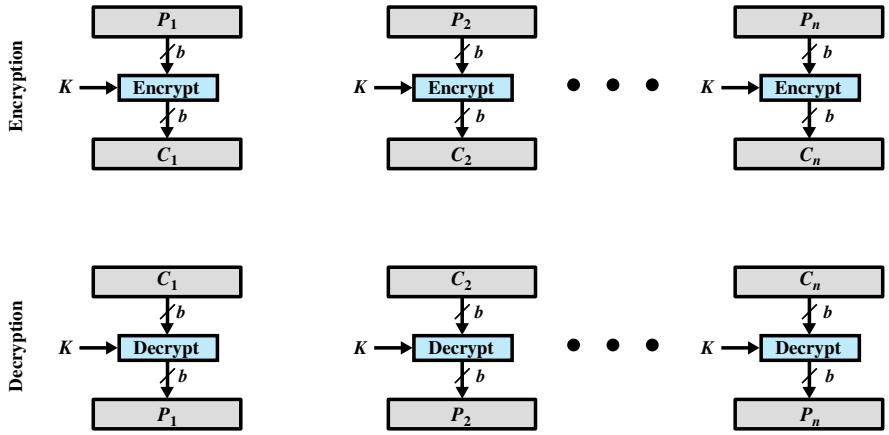
Selected Rijndael in November 2001

Published as FIPS 197

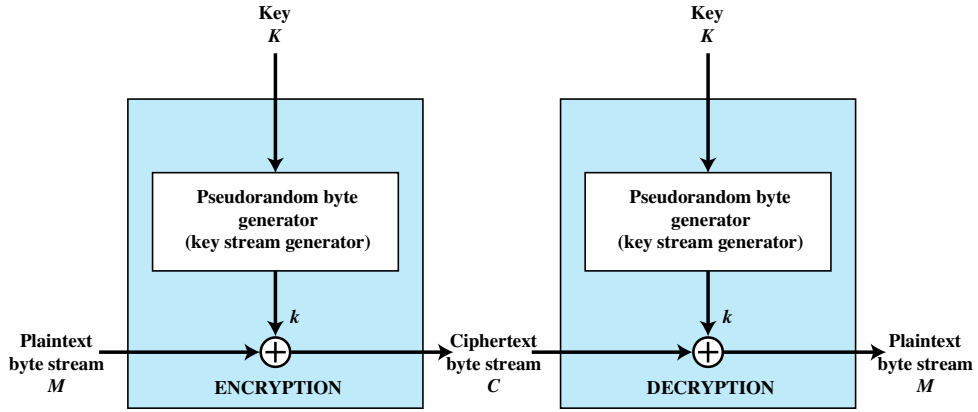
Practical Security Issues

- Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
- Modes of operation
  - Alternative techniques developed to increase the security of symmetric block encryption for large sequences
  - Overcomes the weaknesses of ECB

Computer Security Principles and Practice 4th edition Stallings Solutions Manual



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Figure 2.2 Types of Symmetric Encryption

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Block & Stream Ciphers

Block Cipher

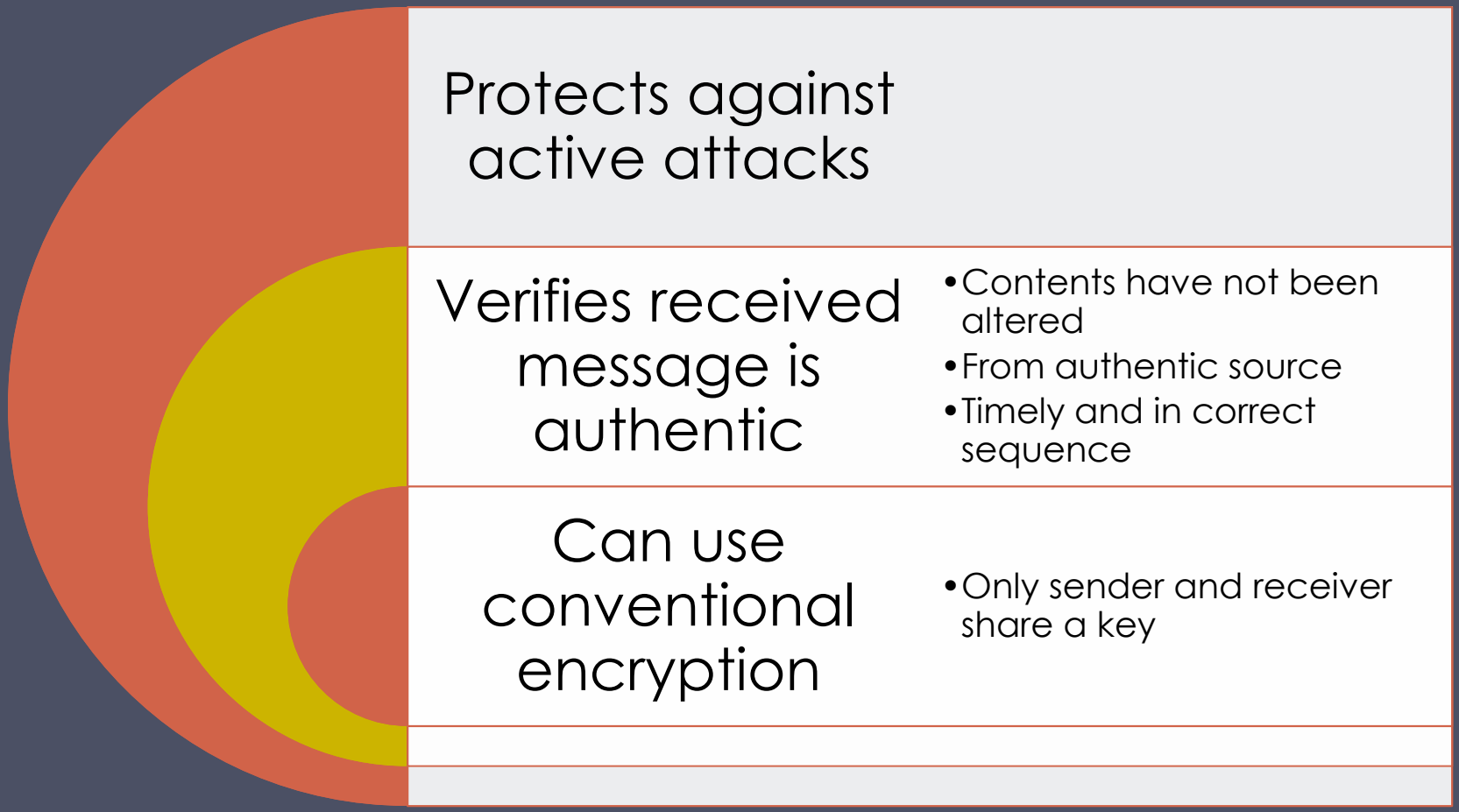
- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Message Authentication



Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Message Authentication Without Confidentiality

- Message encryption by itself does not provide a secure form of authentication
- It is possible to combine authentication and confidentiality in a single algorithm by encrypting a message plus its authentication tag
- Typically message authentication is provided as a separate function from message encryption
- Situations in which message authentication without confidentiality may be preferable include:
  - There are a number of applications in which the same message is broadcast to a number of destinations
  - An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
  - Authentication of a computer program in plaintext is an attractive service
- Thus, there is a place for both authentication and encryption in meeting security requirements

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

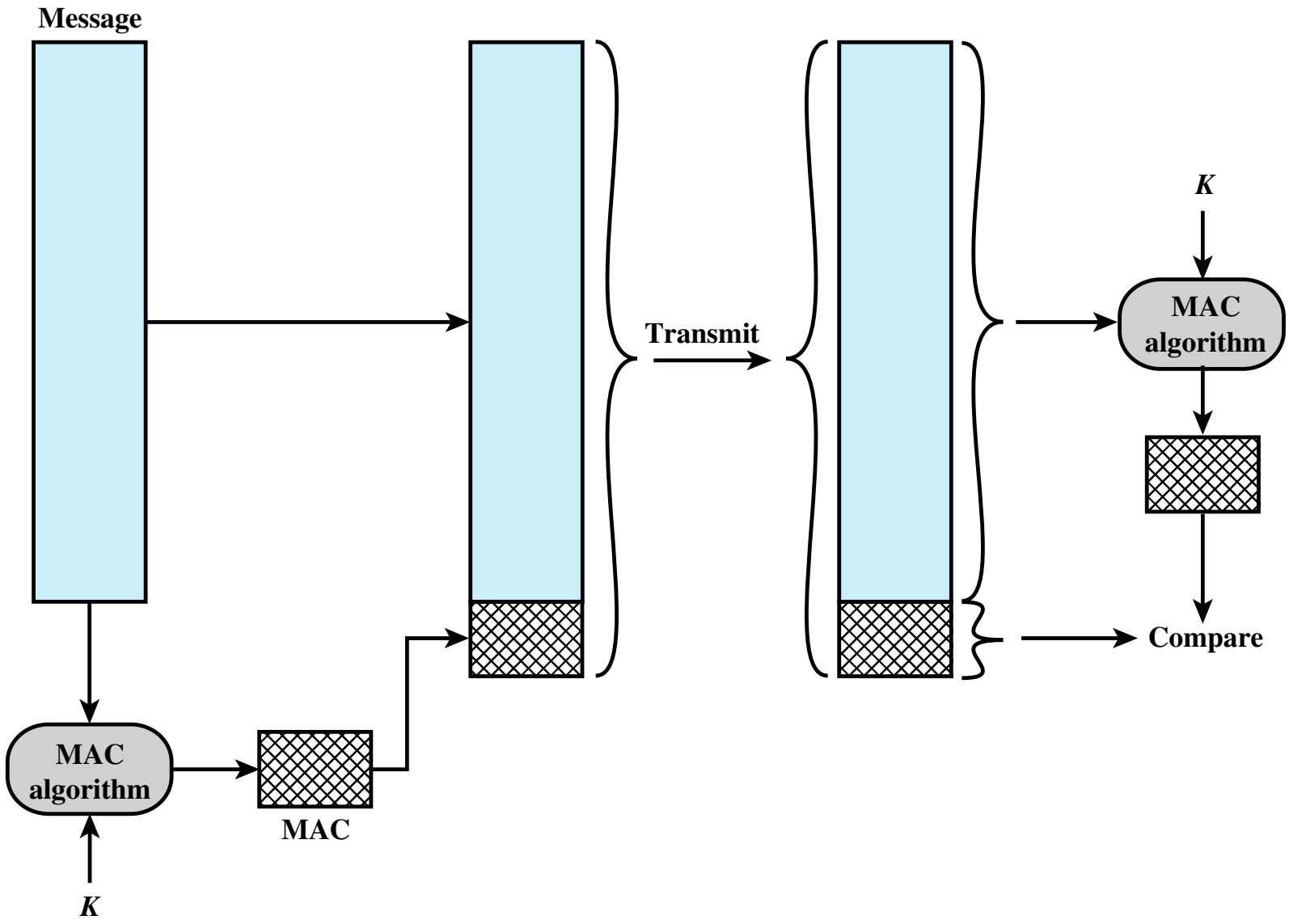


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Computer Security Principles and Practice 4th edition Stallings Solutions Manual





Computer Security Principles and Practice 4th edition Stallings Solutions Manual

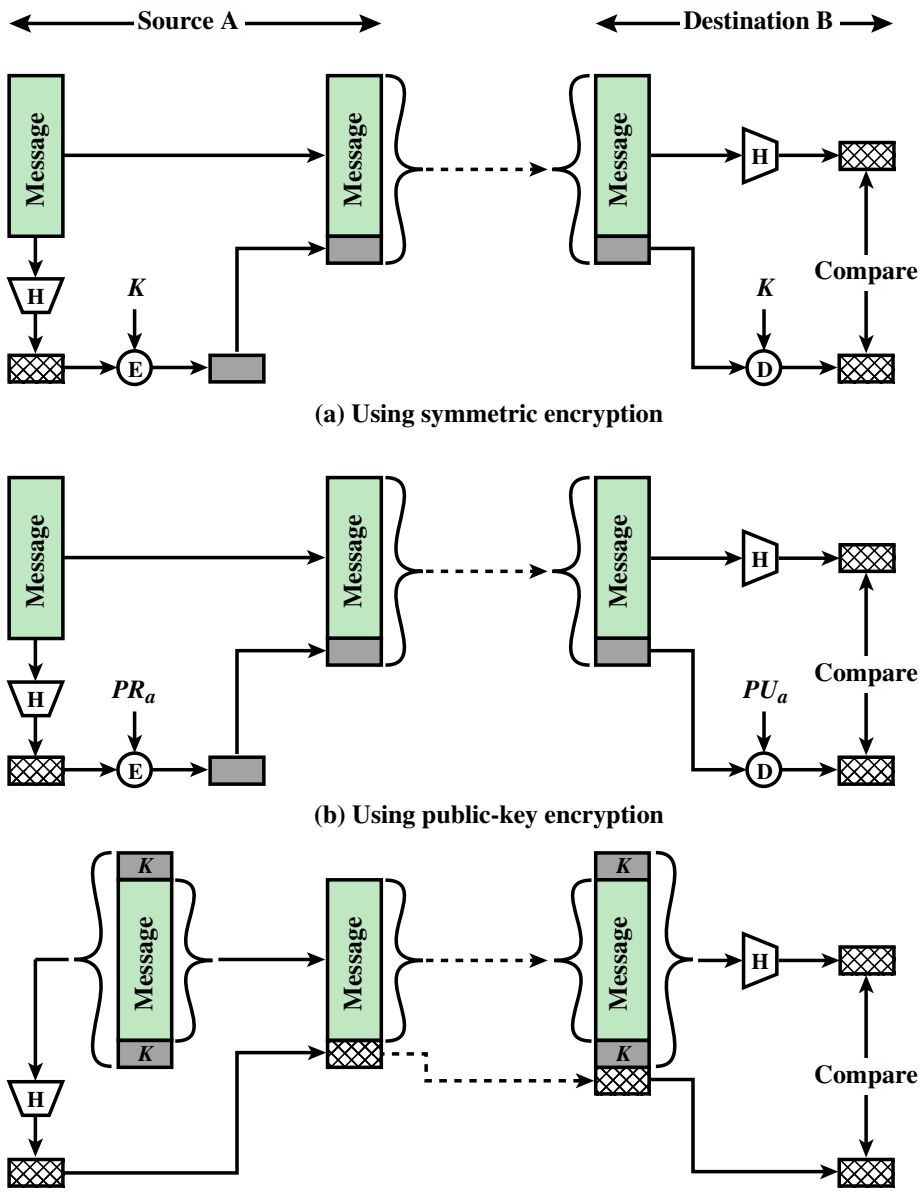


Figure 2.5 Message Authentication Using a One-Way Hash Function.

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

To be useful for message authentication, a hash function H must have the following properties:

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find y ≠ x such that H(y) = H(x)
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Security of Hash Functions

There are two approaches to attacking a secure hash function:

- **Cryptanalysis**
  - Exploit logical weaknesses in the algorithm
- **Brute-force attack**
  - Strength of hash function depends solely on the length of the hash code produced by the algorithm

SHA most widely used hash algorithm

Additional secure hash function applications:

- **Passwords**
  - Hash of a password is stored by an operating system
- **Intrusion detection**
  - Store H(F) for each file on a system and secure the hash values

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Public-Key Encryption Structure

Publicly proposed by Diffie and Hellman in 1976

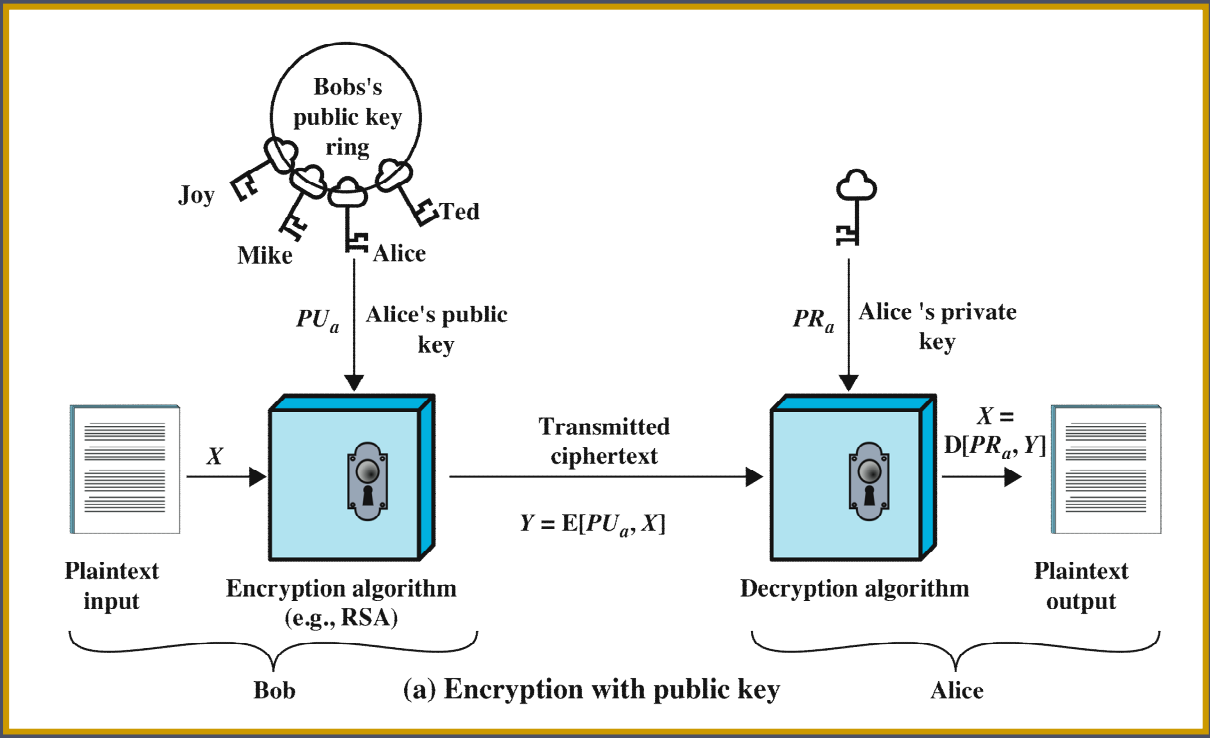
Based on mathematical functions

Asymmetric

- Uses two separate keys
- Public key and private key
- Public key is made public for others to use

Some form of protocol is needed for distribution

Computer Security Principles and Practice 4th edition Stallings Solutions Manual



- **Plaintext**
  - Readable message or data that is fed into the algorithm as input
- **Encryption algorithm**
  - Performs transformations on the plaintext
- **Public and private key**
  - Pair of keys, one for encryption, one for decryption
- **Ciphertext**
  - Scrambled message produced as output
- **Decryption key**
  - Produces the original plaintext

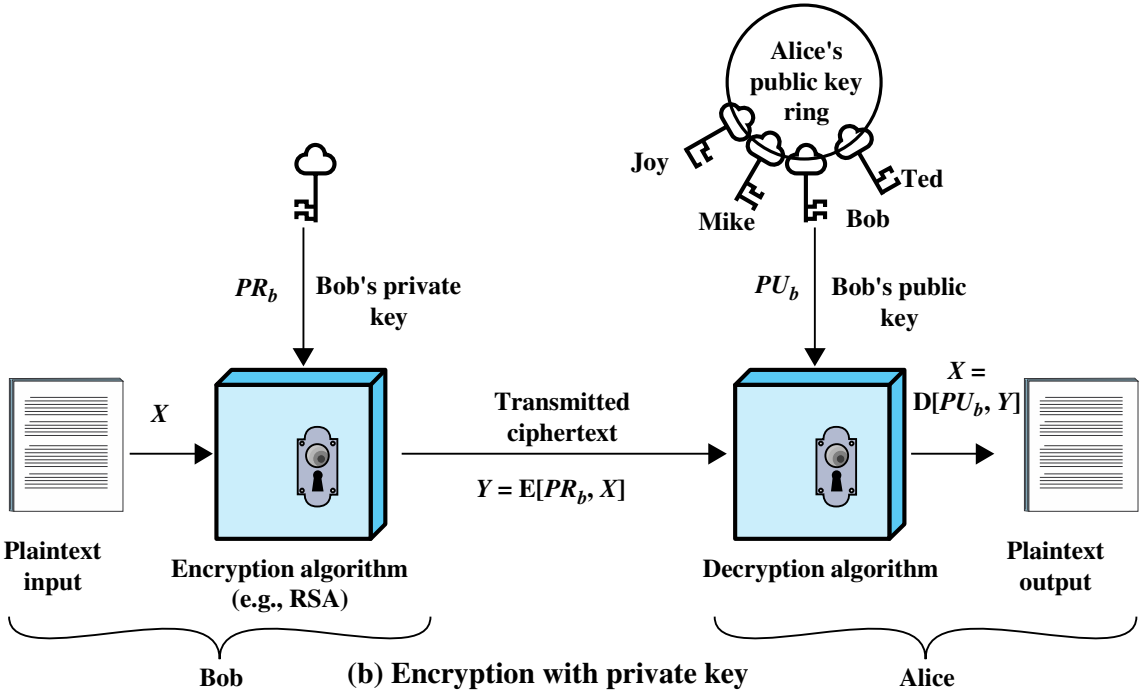


Figure 2.6 Public-Key Cryptography

- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Table 2.3

Applications for Public-Key Cryptosystems

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Requirements for Public-Key Cryptosystems

Computationally easy to create key pairs

Useful if either key can be used for each role



Computationally easy for sender knowing public key to encrypt messages

Computationally infeasible for opponent to otherwise recover original message

Computationally easy for receiver knowing private key to decrypt ciphertext

Computationally infeasible for opponent to determine private key from public key

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Asymmetric Encryption Algorithms

RSA (Rivest, Shamir, Adleman)	Developed in 1977	Most widely accepted and implemented approach to public-key encryption	Block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
Diffie-Hellman key exchange algorithm	Enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages	Limited to the exchange of the keys	
Digital Signature Standard (DSS)	Provides only a digital signature function with SHA-1	Cannot be used for encryption or key exchange	
Elliptic curve cryptography (ECC)	Security like RSA, but with much smaller keys		

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:

  "The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."

- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block

- FIPS 186-4 specifies the use of one of three digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

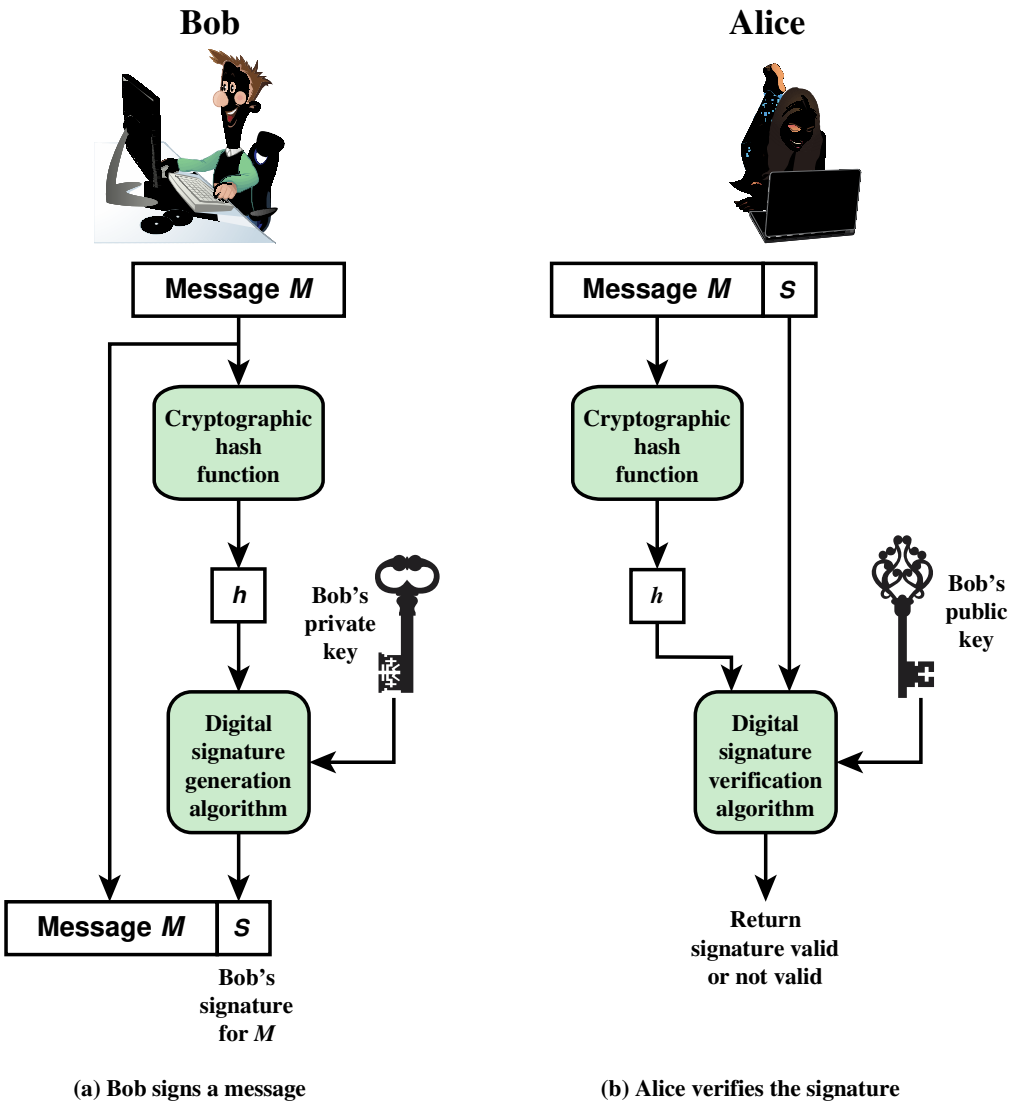


Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

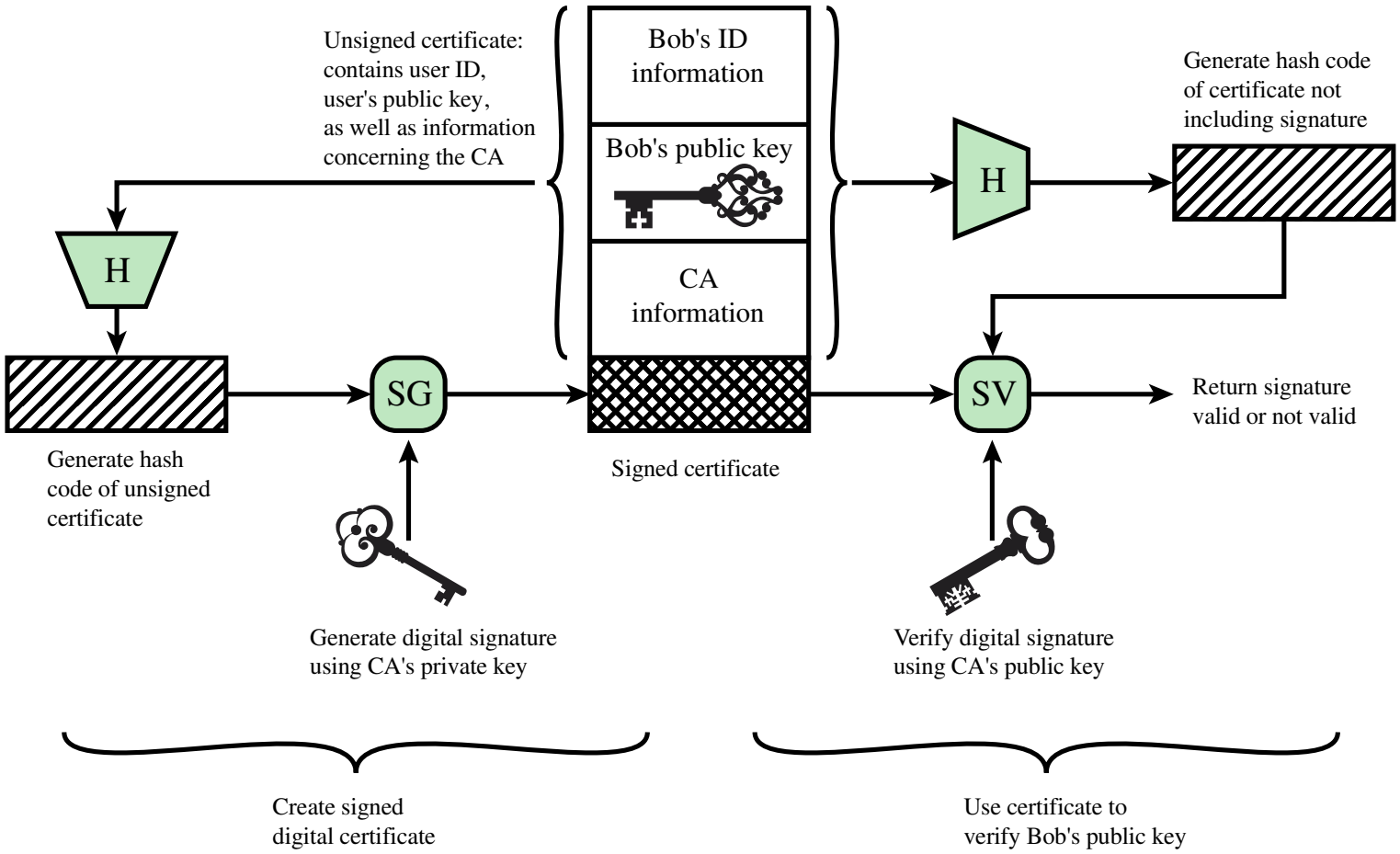
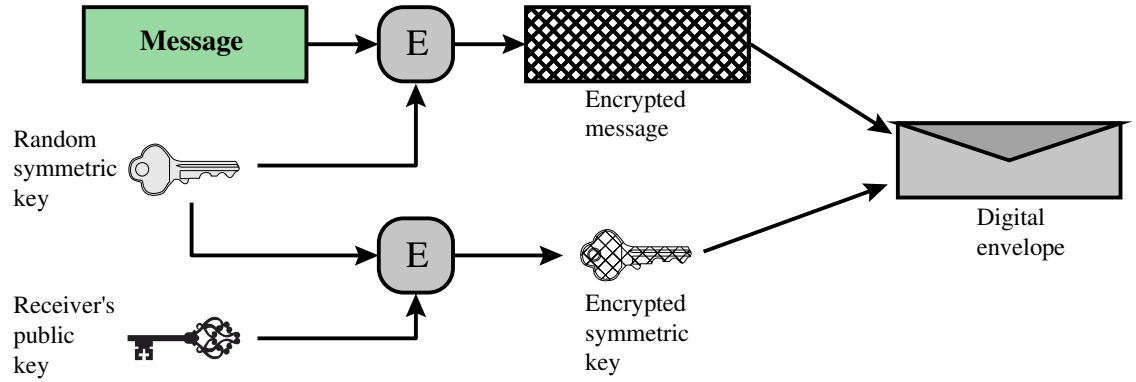
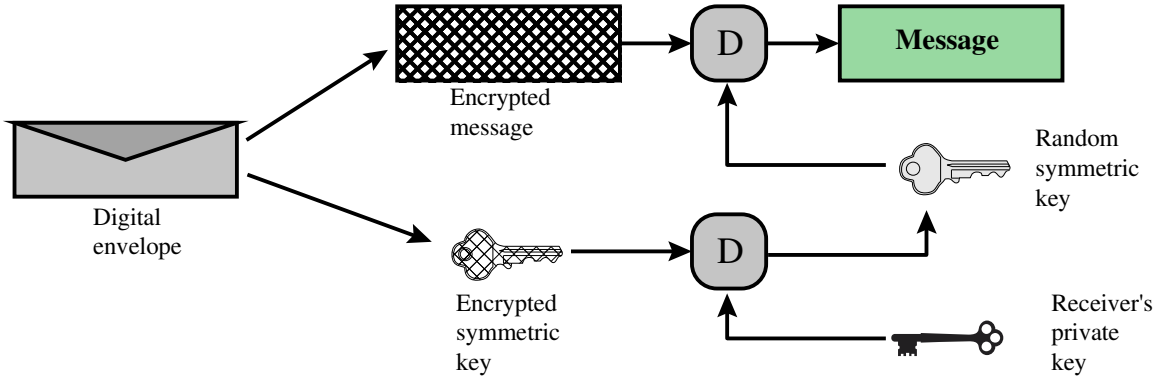


Figure 2.8 Public-Key Certificate Use

Computer Security Principles and Practice 4th edition Stallings Solutions Manual



(a) Creation of a digital envelope



(b) Opening a digital envelope

Figure 2.9 Digital Envelopes

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Random Numbers

Uses include generation of:

- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Symmetric key for use as a temporary session key or in creating a digital envelope
- Handshaking to prevent replay attacks
- Session key

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Random Number Requirements

Randomness

- Criteria:
  - Uniform distribution
    - Frequency of occurrence of each of the numbers should be approximately the same
  - Independence
    - No one value in the sequence can be inferred from the others

Unpredictability

- Each number is statistically independent of other numbers in the sequence
- Opponent should not be able to predict future elements of the sequence on the basis of earlier elements

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Random versus Pseudorandom

Cryptographic applications typically make use of algorithmic techniques for random number generation

- Algorithms are deterministic and therefore produce sequences of numbers that are not statistically random

Pseudorandom numbers are:

- Sequences produced that satisfy statistical randomness tests
- Likely to be predictable

True random number generator (TRNG):

- Uses a nondeterministic source to produce randomness
- Most operate by measuring unpredictable natural processes
  - e.g. radiation, gas discharge, leaky capacitors
- Increasingly provided on modern processors

Computer Security Principles and Practice 4th edition Stallings Solutions Manual

Practical Application: Encryption of Stored Data

Common to encrypt transmitted data

Much less common for stored data

- There is often little protection beyond domain authentication and operating system access controls
- Data are archived for indefinite periods
- Even though erased, until disk sectors are reused data are recoverable

Approaches to encrypt stored data:

- Use a commercially available encryption package
- Back-end appliance
- Library based tape encryption
- Background laptop/PC data encryption

Summary

- Confidentiality with symmetric encryption
  - Symmetric encryption
  - Symmetric block encryption algorithms
  - Stream ciphers
- Message authentication and hash functions
  - Authentication using symmetric encryption
  - Message authentication without message encryption
  - Secure hash functions
  - Other applications of hash functions
- Random and pseudorandom numbers
  - The use of random numbers
  - Random versus pseudorandom
- Public-key encryption
  - Structure
  - Applications for public-key cryptosystems
  - Requirements for public-key cryptography
  - Asymmetric encryption algorithms
- Digital signatures and key management
  - Digital signature
  - Public-key certificates
  - Symmetric key exchange using public-key encryption
  - Digital envelopes
- Practical Application: Encryption of Stored Data

Computer Security Principles and Practice 4th edition Stallings Solutions Manual