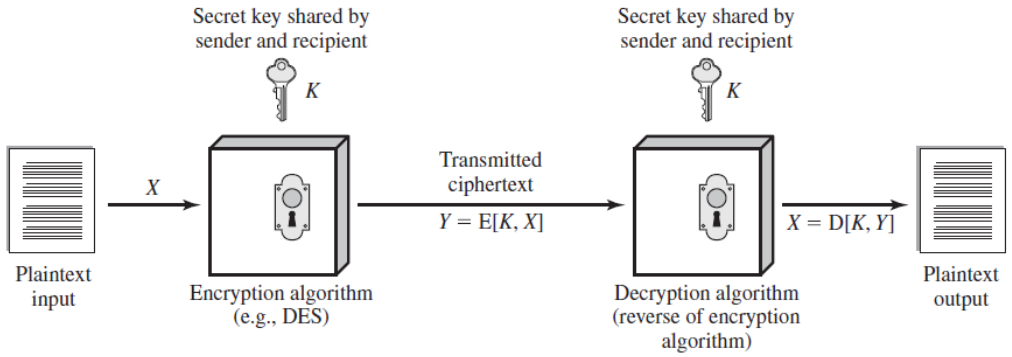
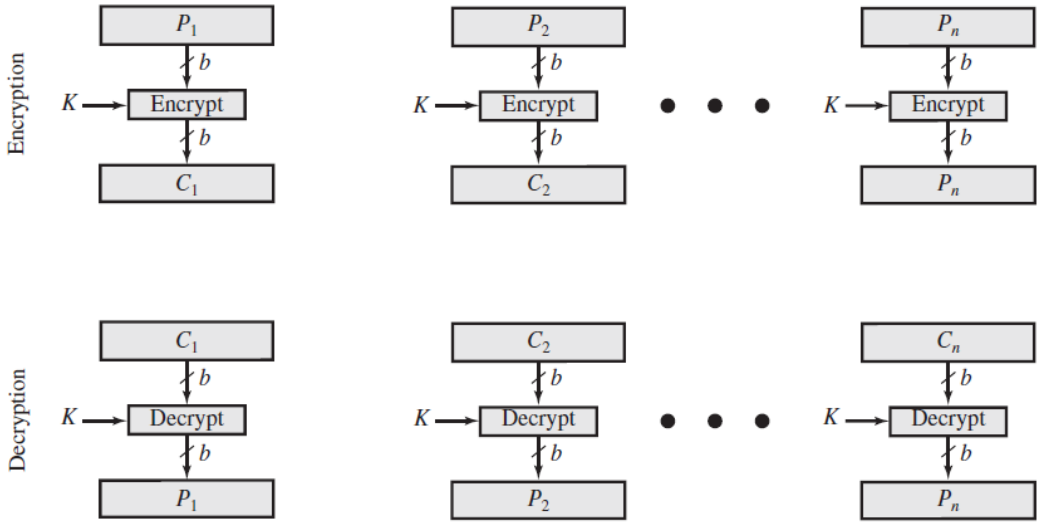
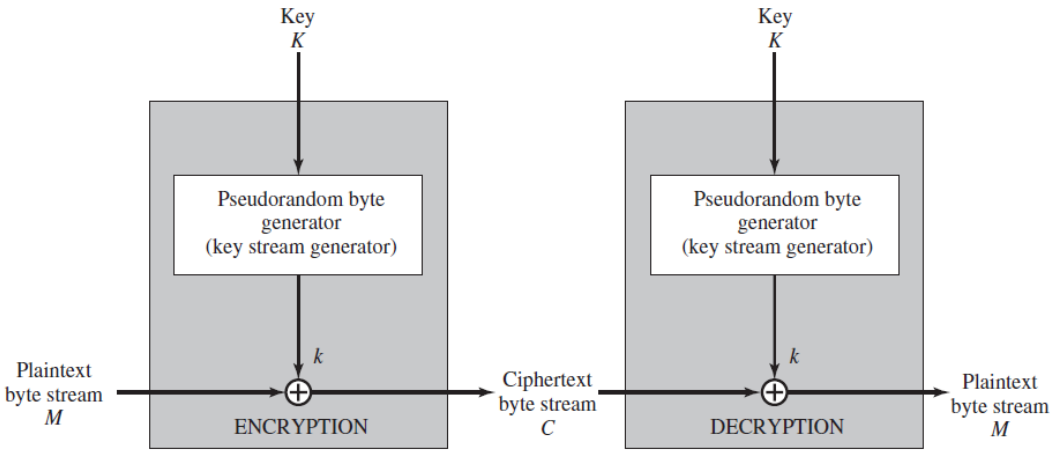


Figure 2.1 **Simplified Model of Symmetric Encryption**



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Figure 2.2 Types of Symmetric Encryption

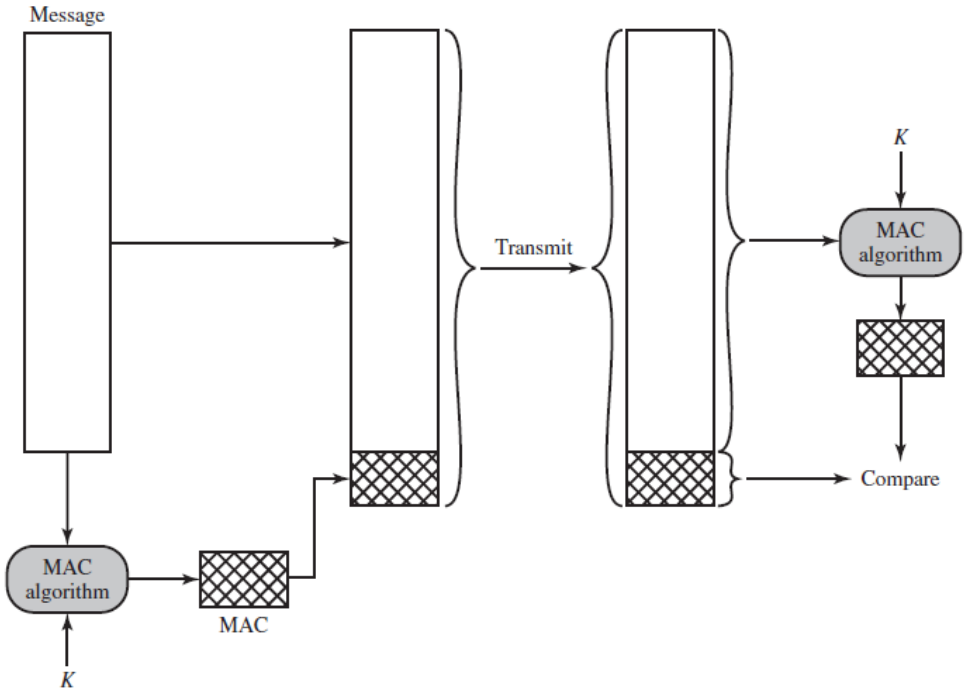
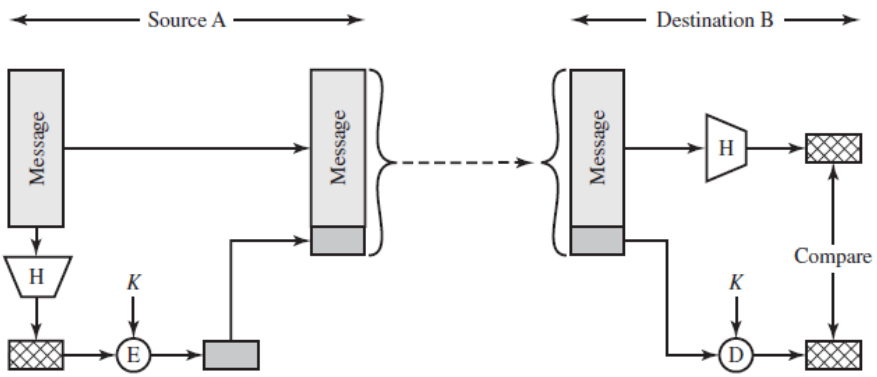
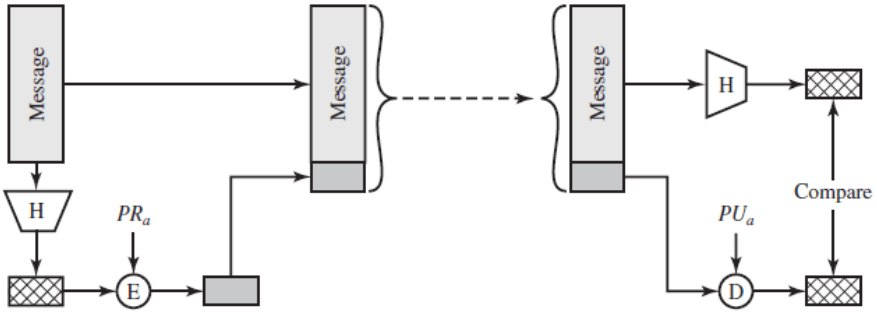


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC)

Authentication approaches other than mac

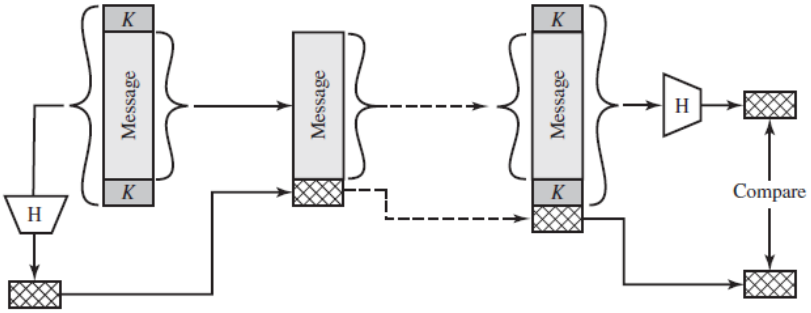


(a) Using symmetric encryption



(b) Using public-key encryption

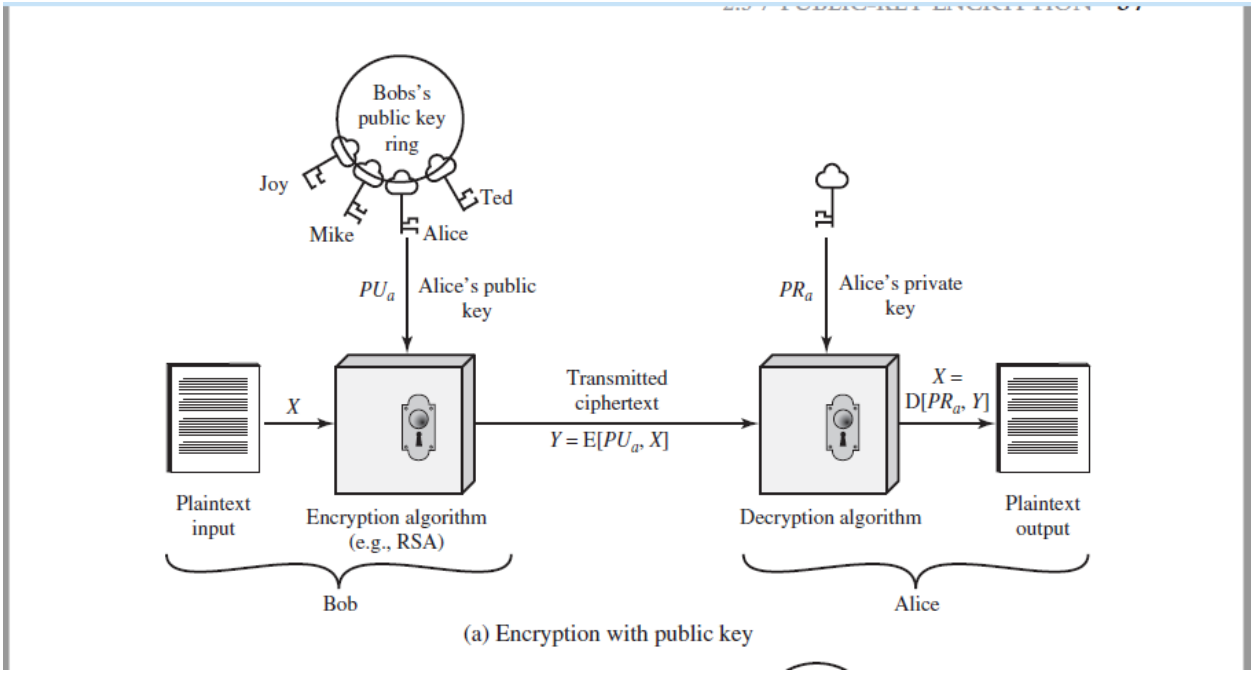
(b) Using public-key encryption



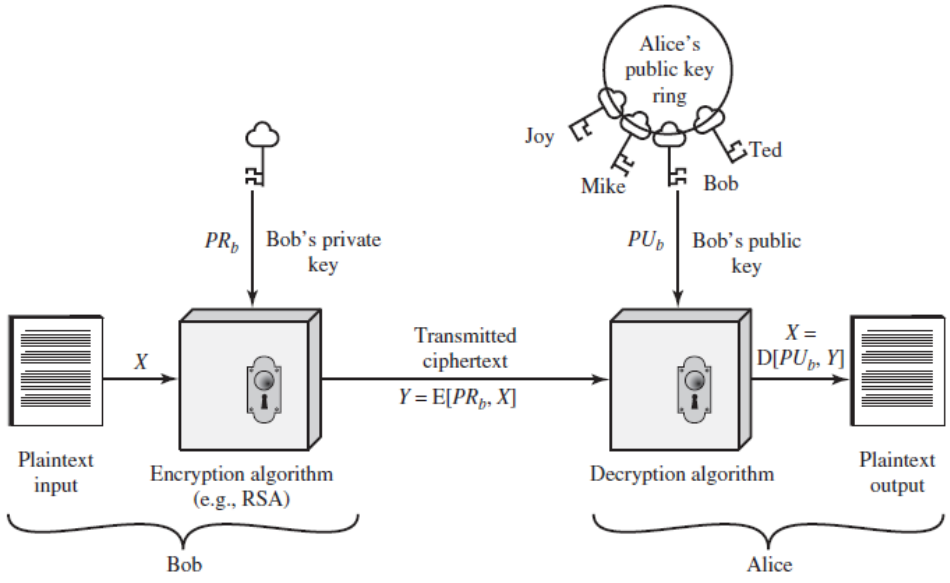
(c) Using secret value

Figure 2.5 Message Authentication Using a One-Way Hash Function

PUBLIC KEY ENCRYPTION



(a) Encryption with public key



(b) Encryption with private key

Figure 2.6 Public-Key Cryptography

First is related to confidentiality, 2nd is for integrity

Public key certificates

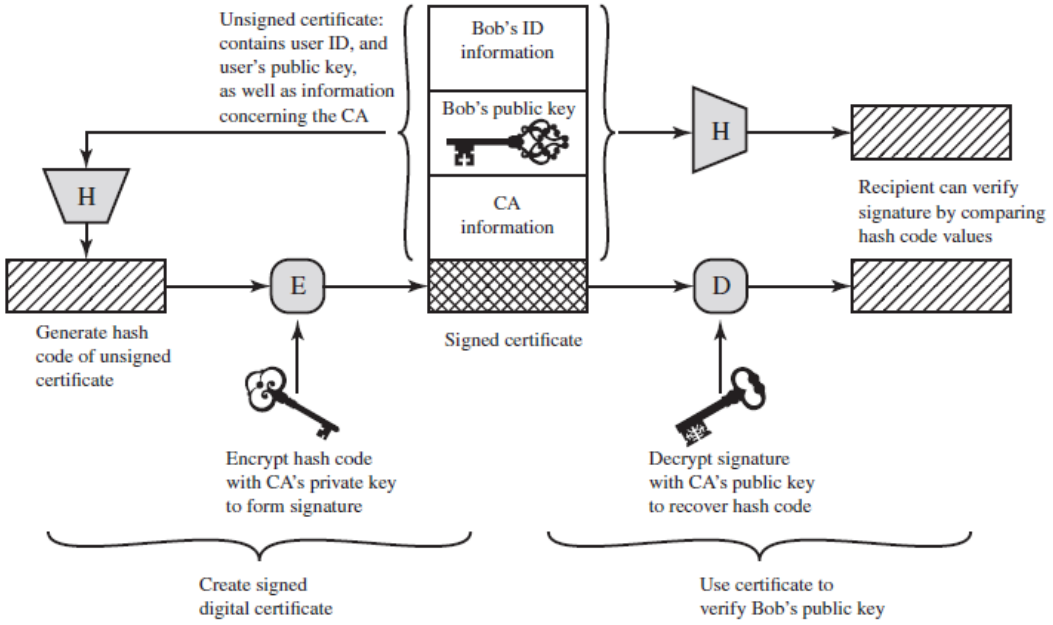
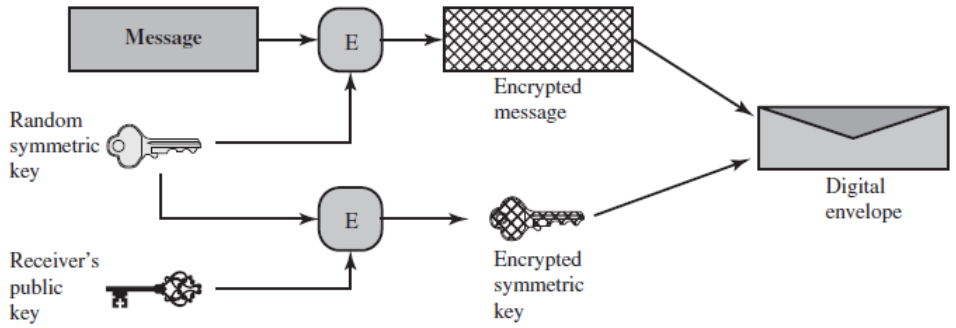
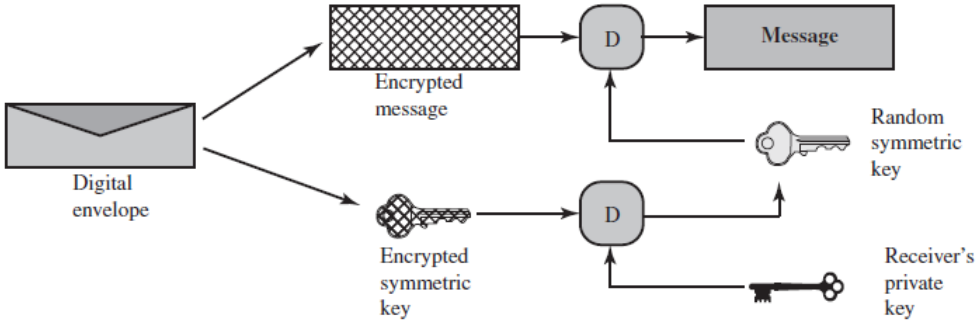


Figure 2.7 Publi



(a) Creation of a digital envelope



(b) Opening a digital envelope

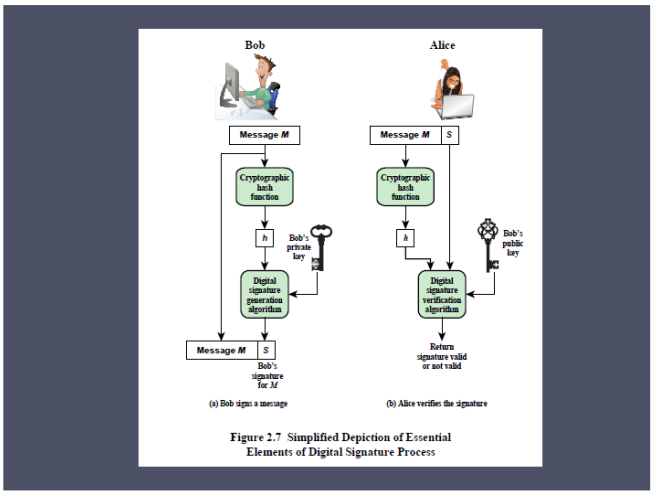


Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process

Chapter 3 user auth

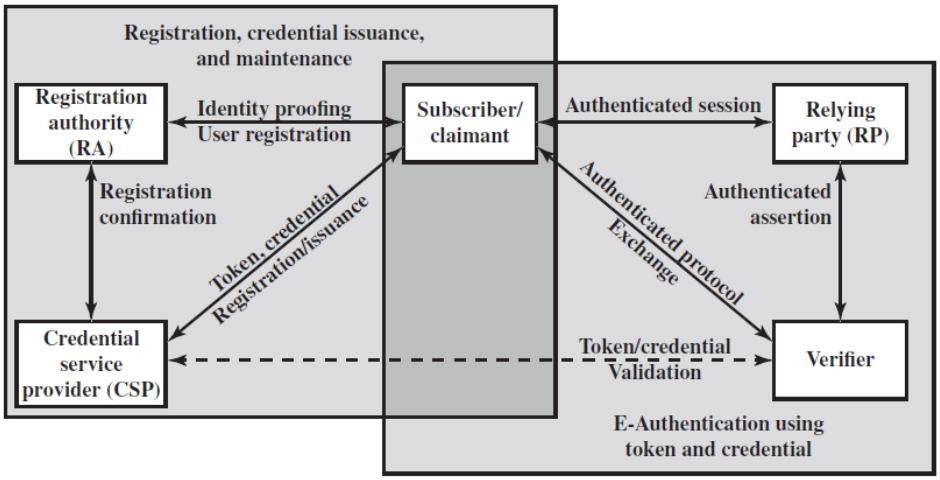


Figure 3.1 The NIST SP 800-63-2 E-Authentication Architectural Model

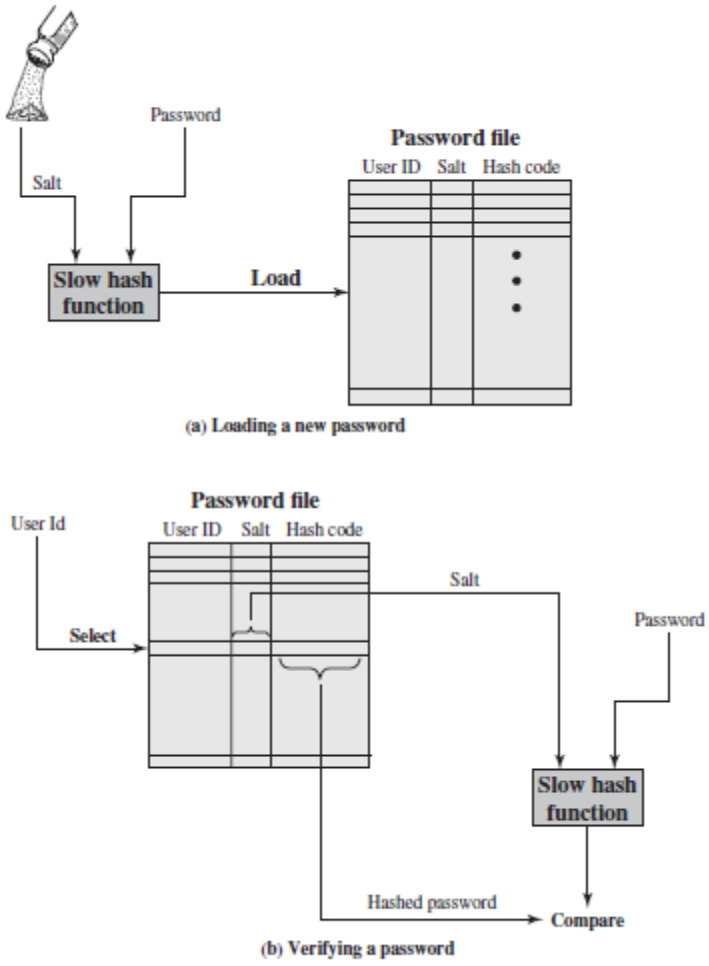


Figure 3.2 **UNIX Password Scheme**

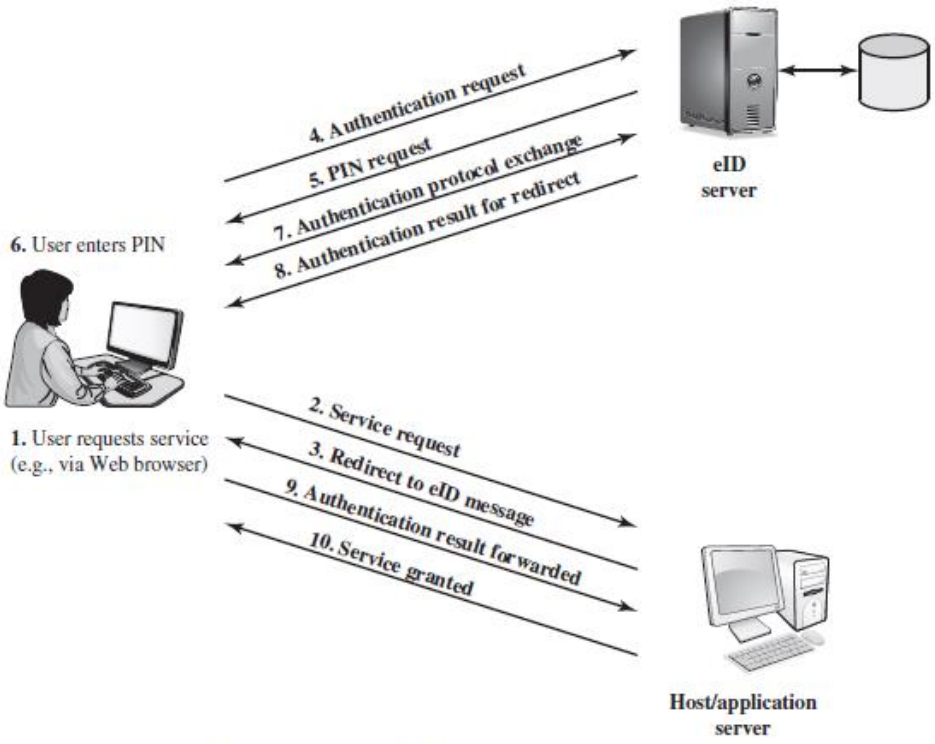
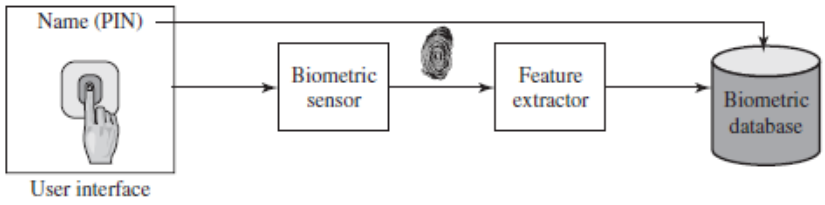
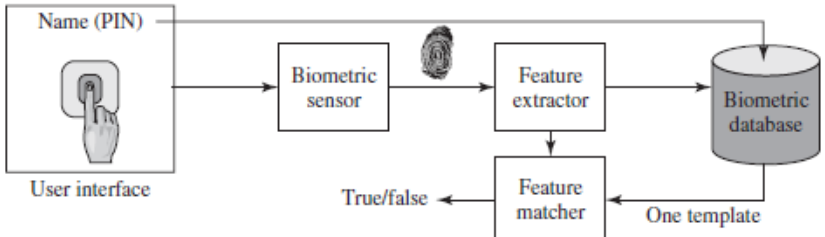


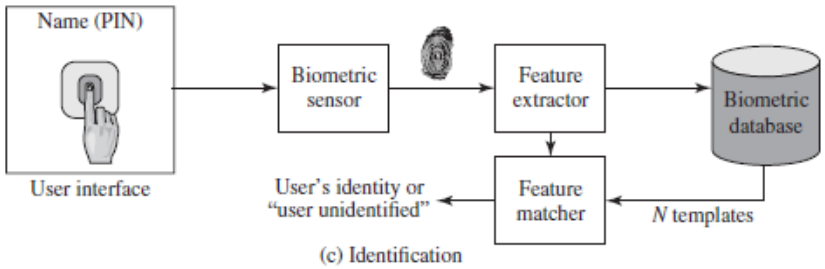
Figure 3.6 **User Authentication with eID**



(a) Enrollment



(b) Verification



(c) Identification

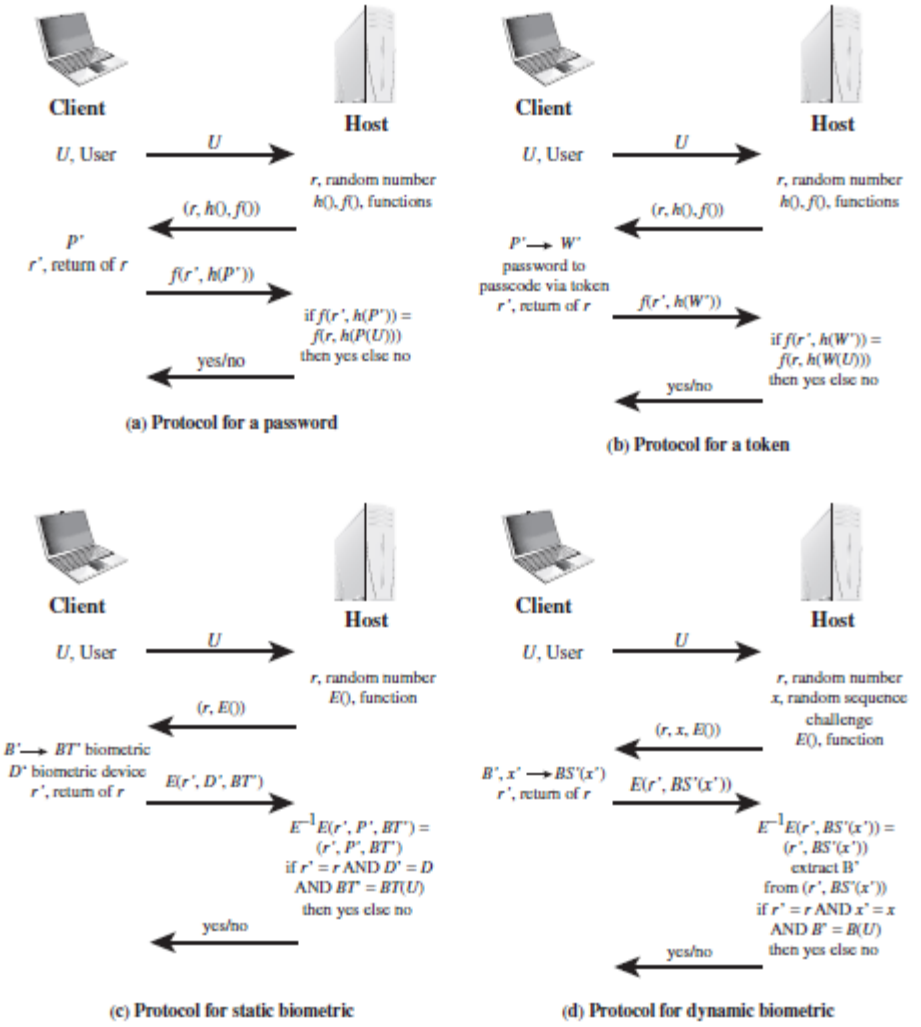
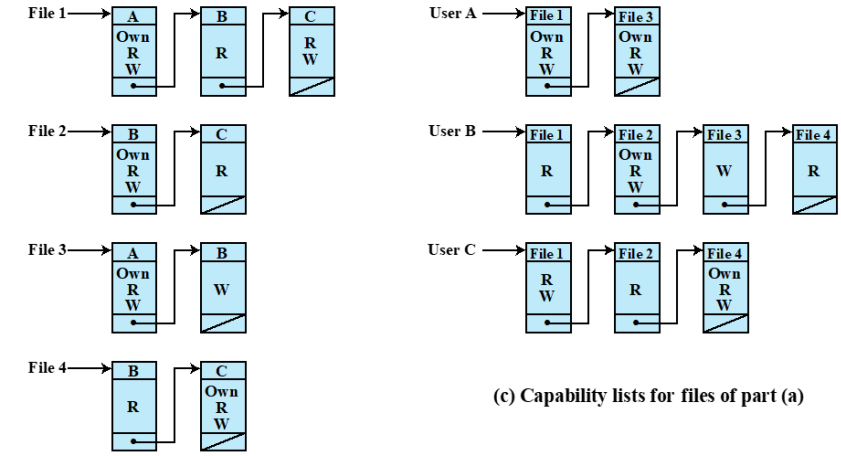


Figure 3.12 **Basic Challenge-Response Protocols for Remote User Authentication**
Source: Based on [OGOR03].

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Figure 4.2 Example of Access Control Structures



(b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

Table 4.2

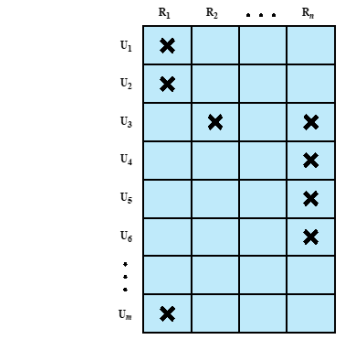
Authorization Table for Files in Figure 4.2

(Table is on page 113 in the textbook)

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

Figure 4.3 Extended Access Control Matrix



		OBJECTS								
		R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
ROLES	R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R_2		control		write *	execute			owner	seek *
	R_n			control		write	stop			

Figure 4.7 Access Control Matrix Representation of RBAC

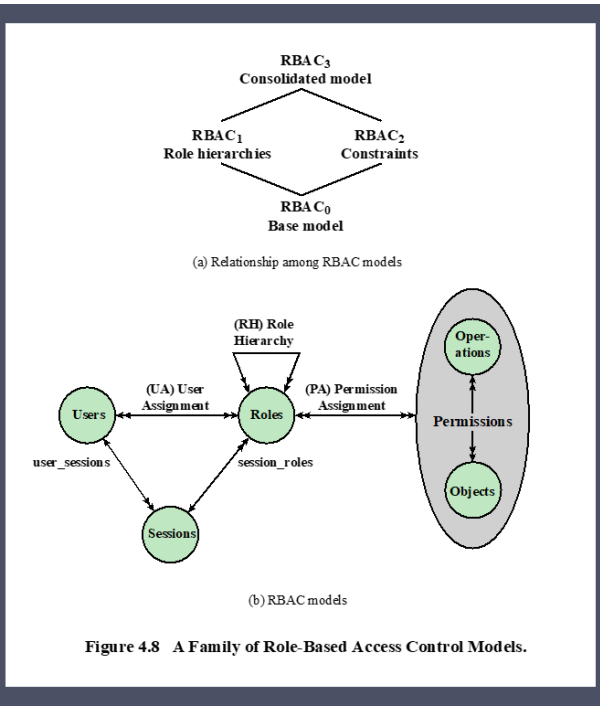


Figure 4.8 A Family of Role-Based Access Control Models.

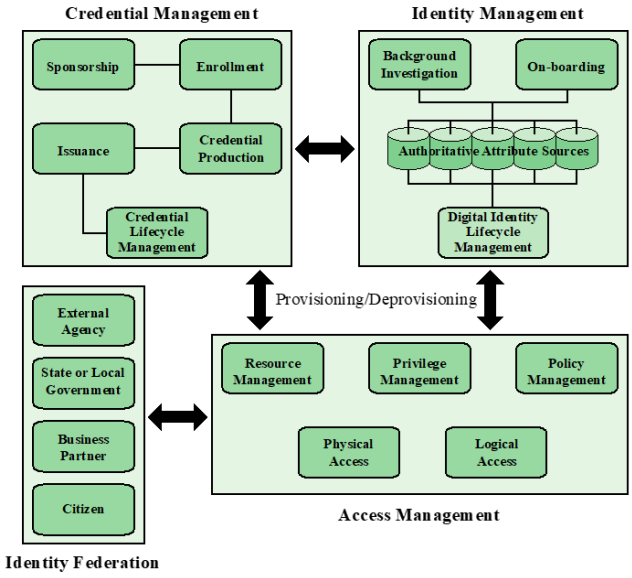


Figure 4.12 Identity, Credential, and Access Management (ICAM)

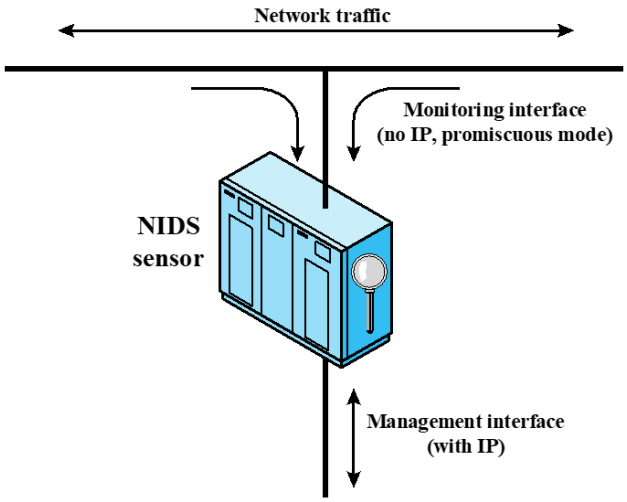


Figure 8.4 Passive NIDS Sensor

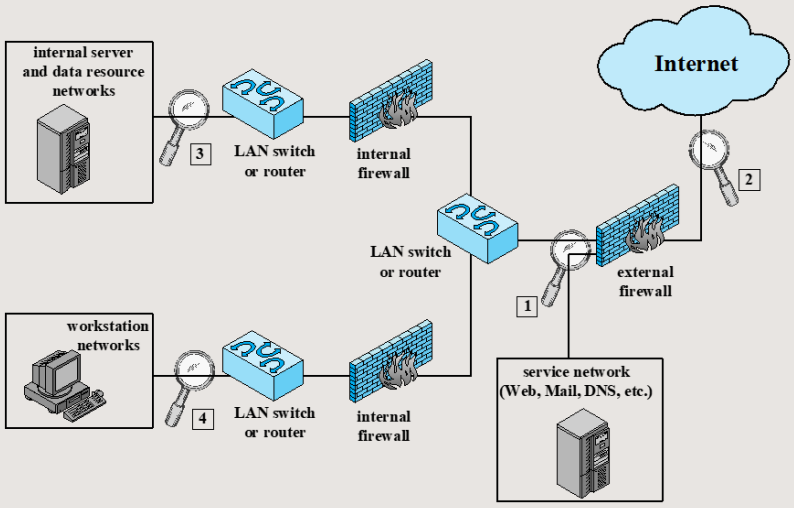


Figure 8.5 Example of NIDS Sensor Deployment

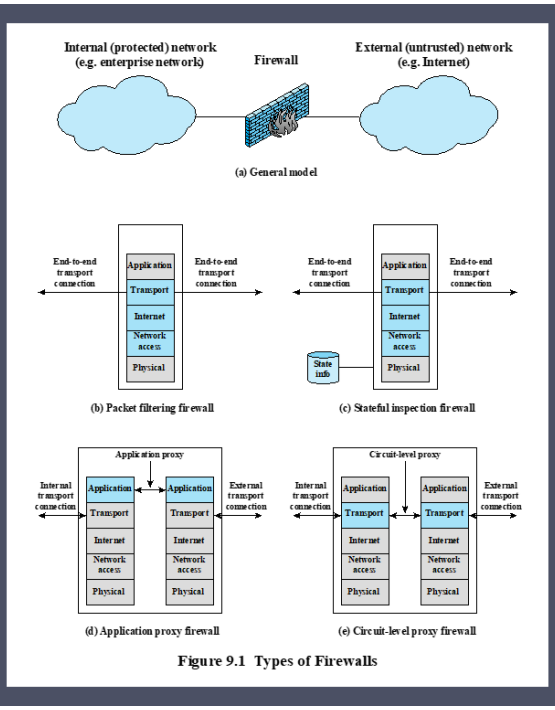


Figure 9.1 Types of Firewalls

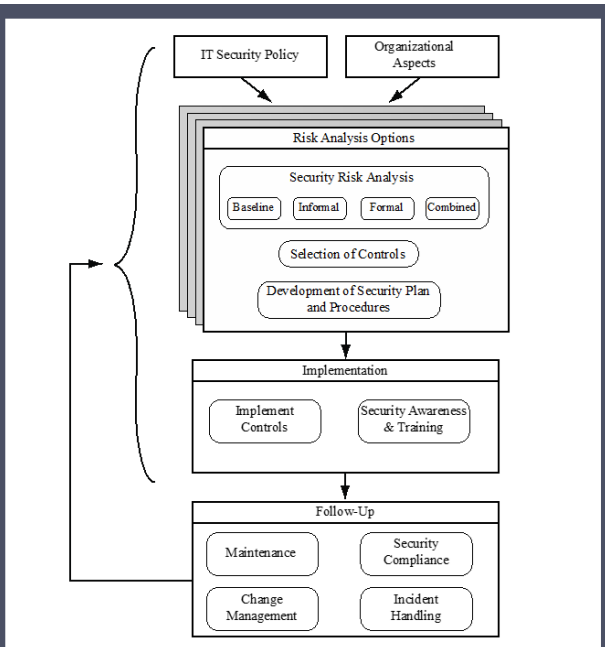


Figure 14.1 Overview of IT Security Management

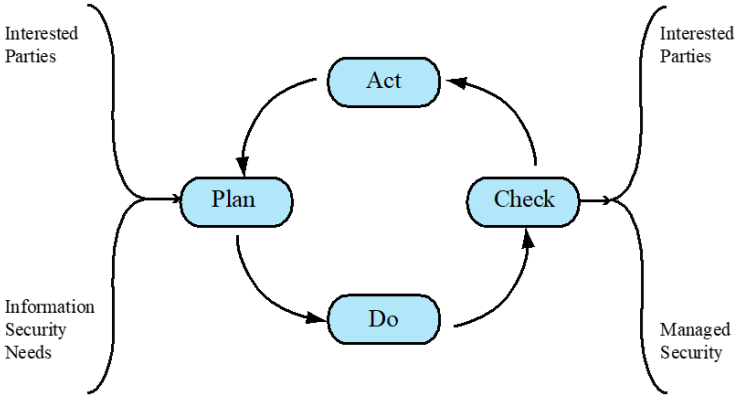


Figure 14.2 The Plan - Do - Check - Act Process Model

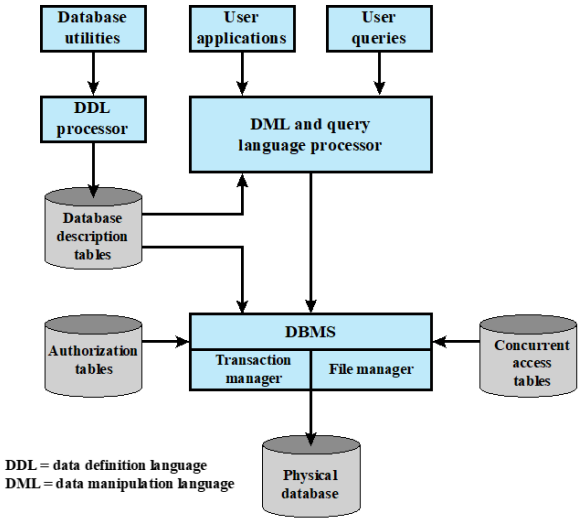


Figure 5.1 DBMS Architecture

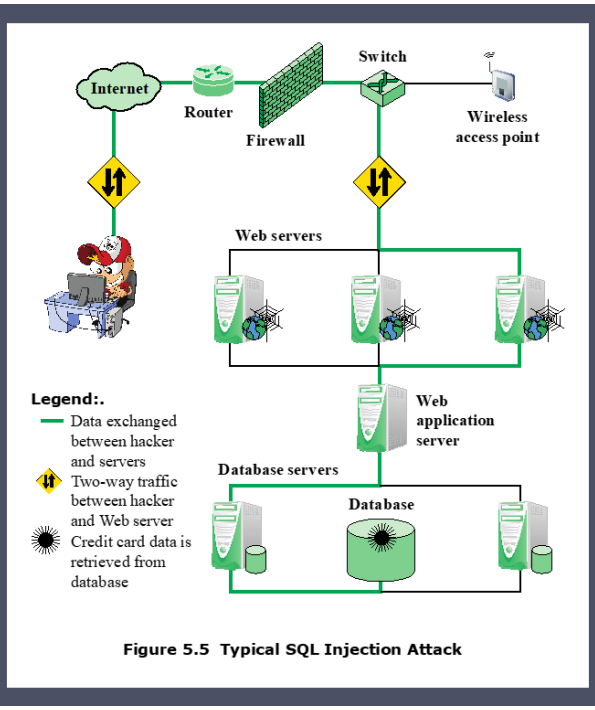


Figure 5.5 Typical SQL Injection Attack

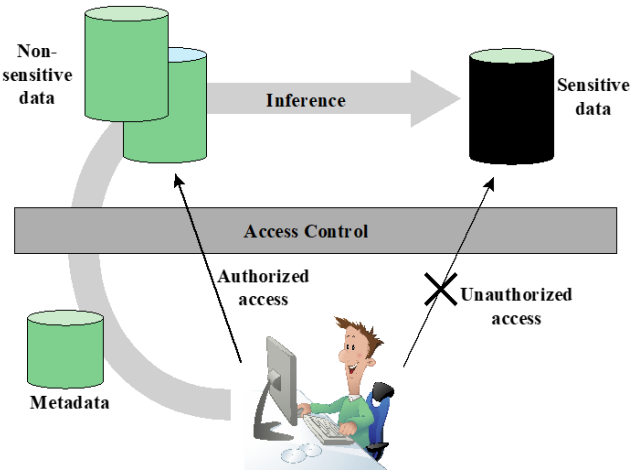


Figure 5.7 Indirect Information Access Via Inference Channel

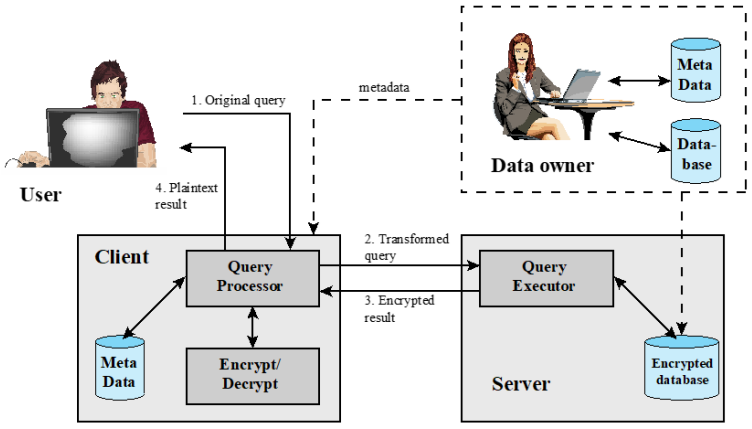


Figure 5.9 A Database Encryption Scheme