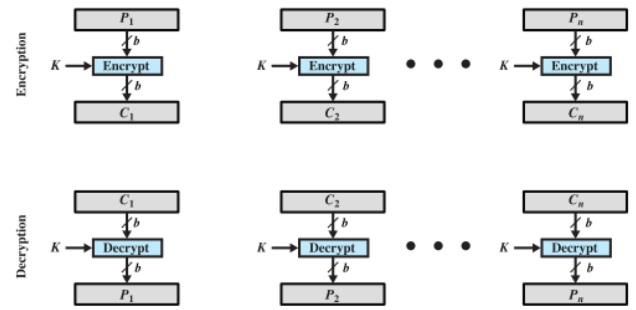
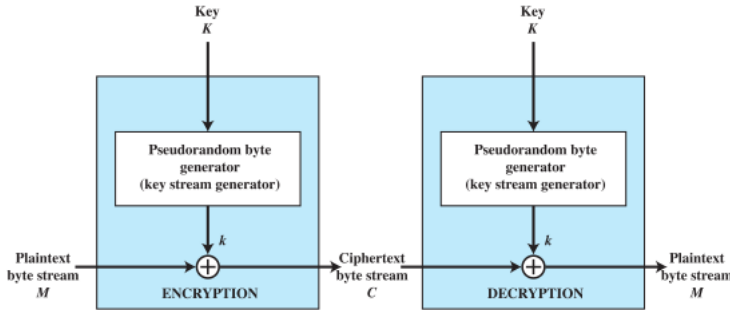


Figure 2.1 Simplified Model of Symmetric Encryption



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

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

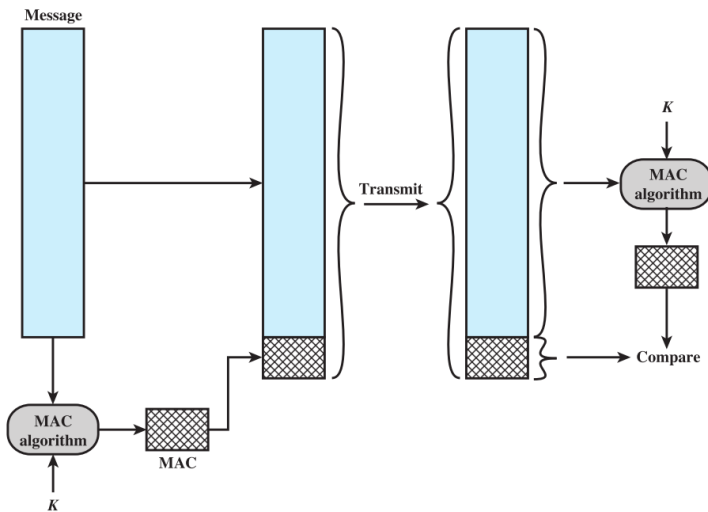
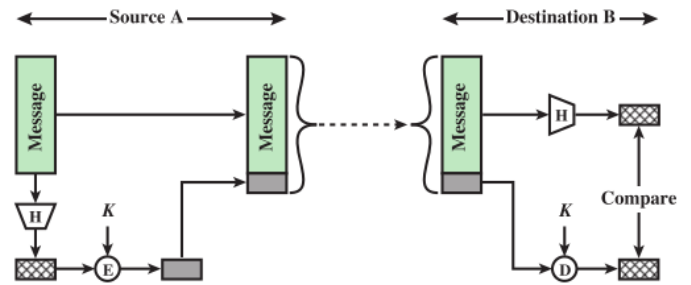
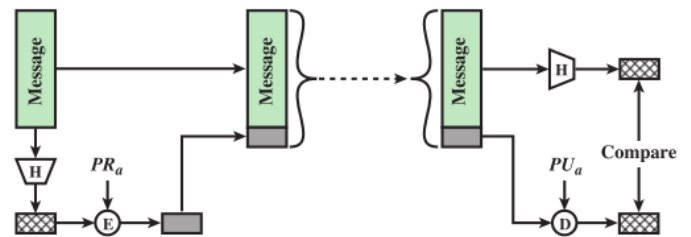


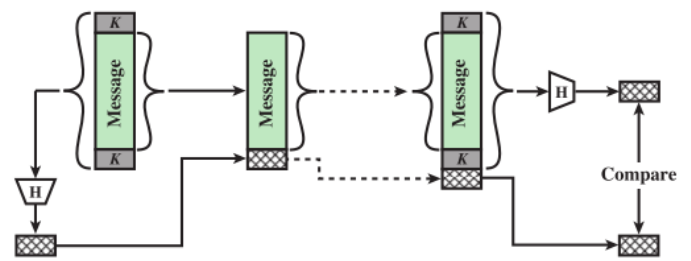
Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).



(a) Using symmetric encryption



(b) Using public-key encryption



(c) Using secret value

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

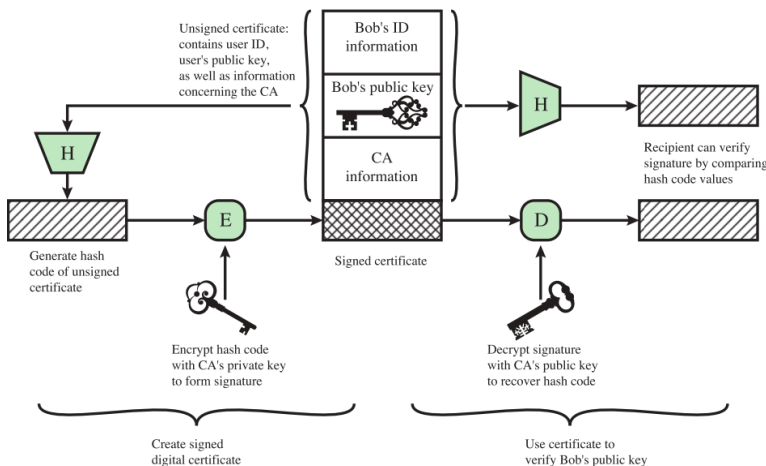


Figure 2.7 Public-Key Certificate Use

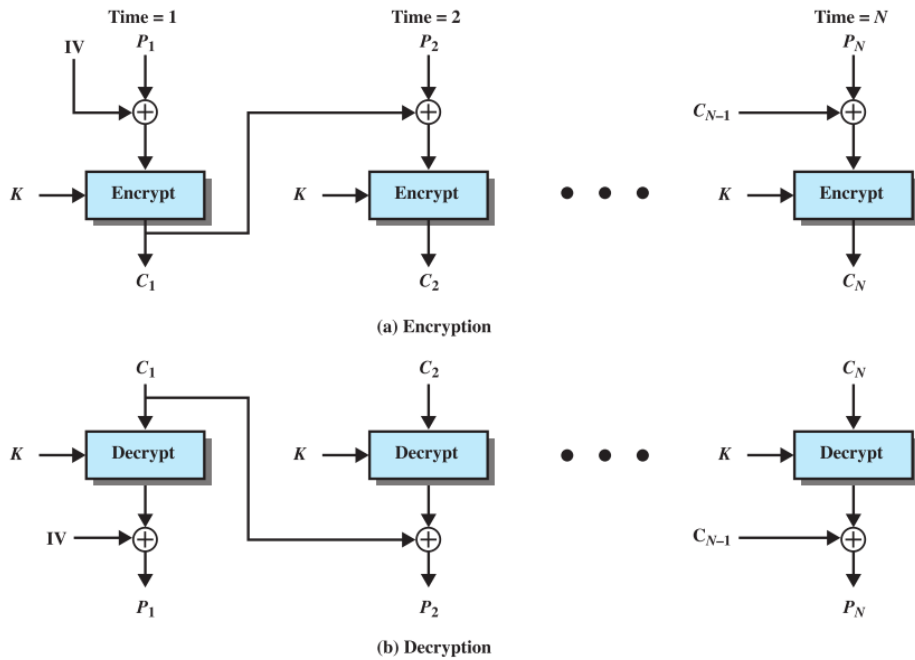


Figure 20.6 Cipher Block Chaining (CBC) Mode

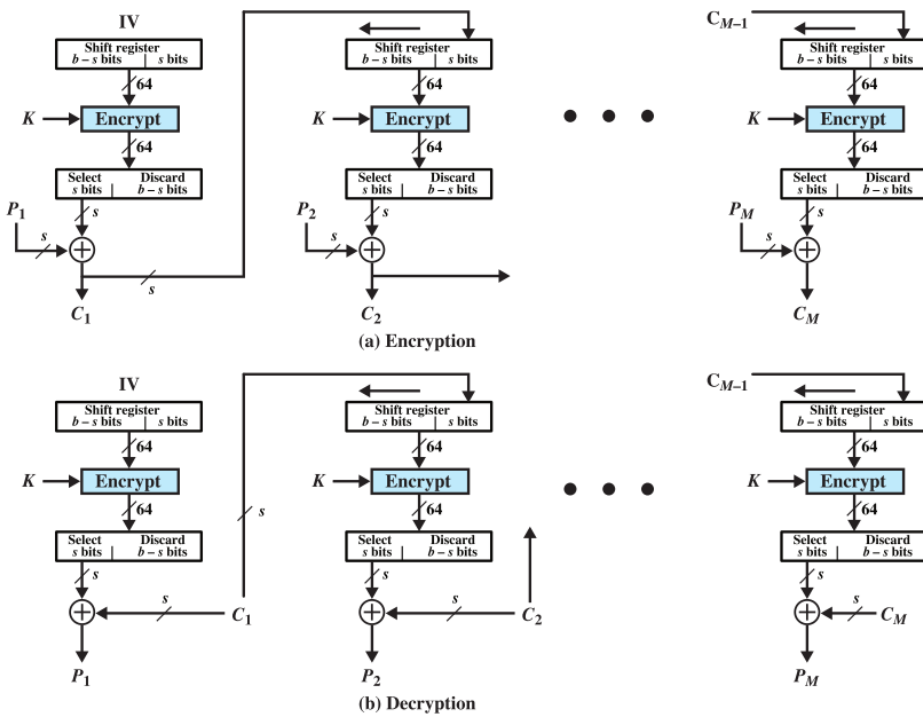


Figure 20.7  $s$ -bit Cipher Feedback (CFB) Mode

Table 21.1 Comparison of SHA Parameters

	SHA-1	SHA-256	SHA-384	SHA-512
Message digest size	160	256	384	512
Message size	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block size	512	512	1024	1024
Word size	32	32	64	64
Number of steps	80	64	80	80

Notes: 1. All sizes are measured in bits.

2. Security refers to the fact that a birthday attack on a message digest of size  $n$  produces a collision with a work factor of approximately  $2^{n/2}$ .

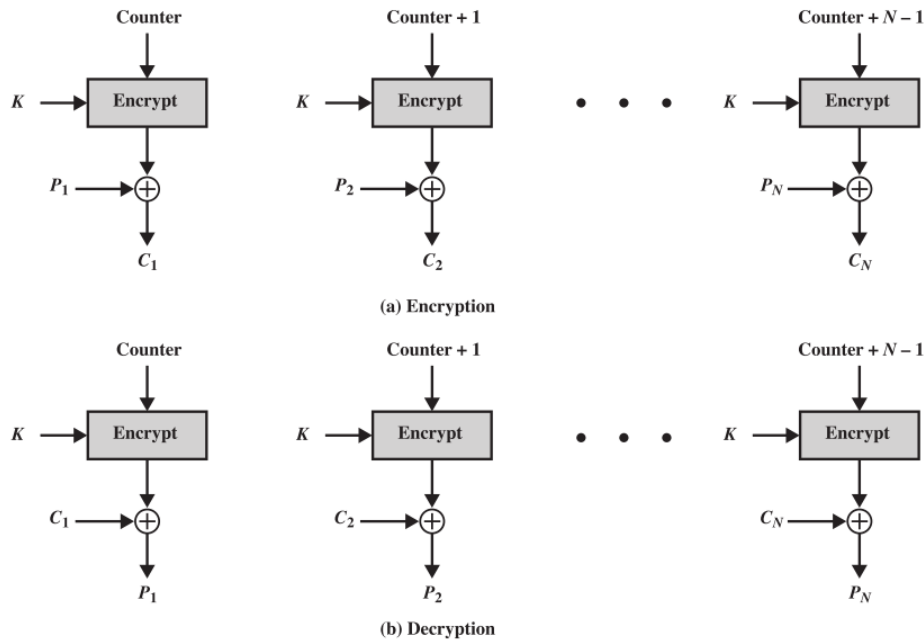


Figure 20.8 Counter (CTR) Mode

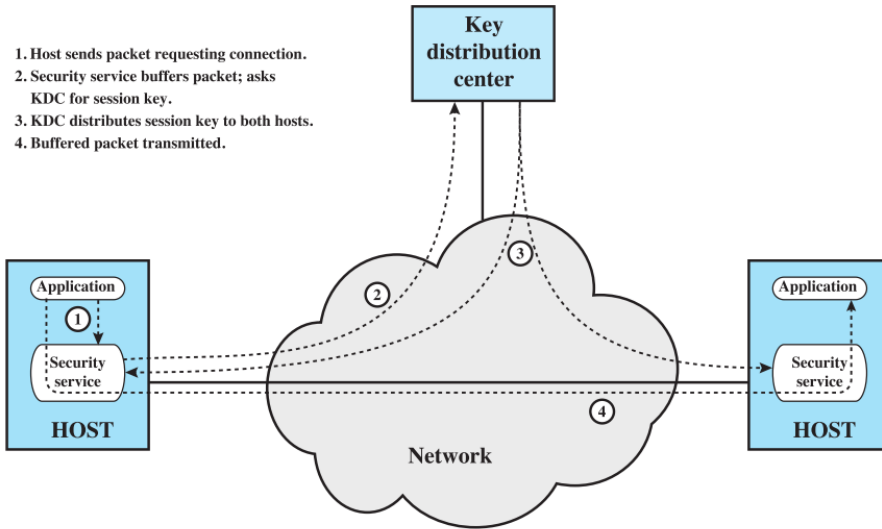


Figure 20.10 Automatic Key Distribution for Connection-Oriented Protocol

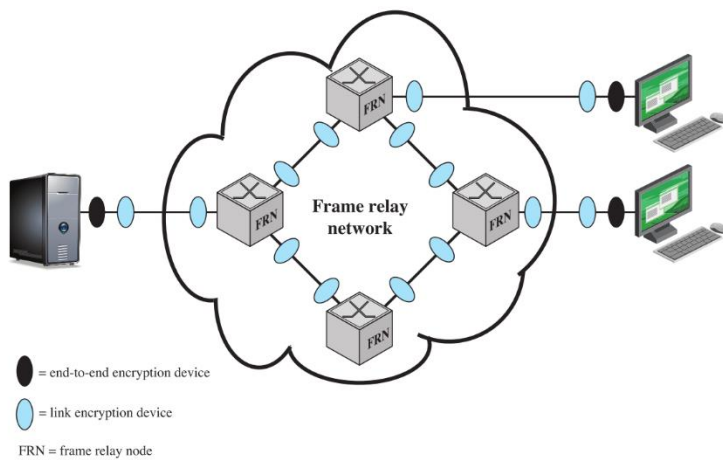
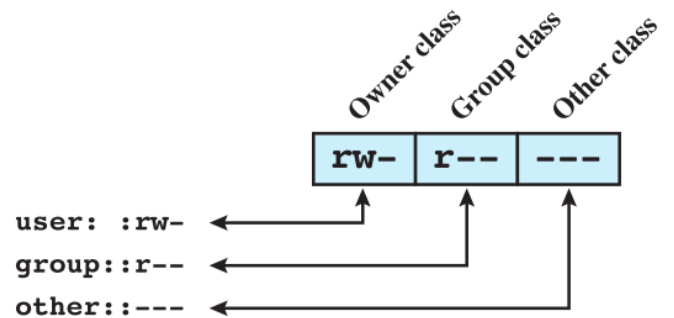


Figure 20.9 Encryption Across a Frame Relay Network



(a) Traditional UNIX approach (minimal access control list)

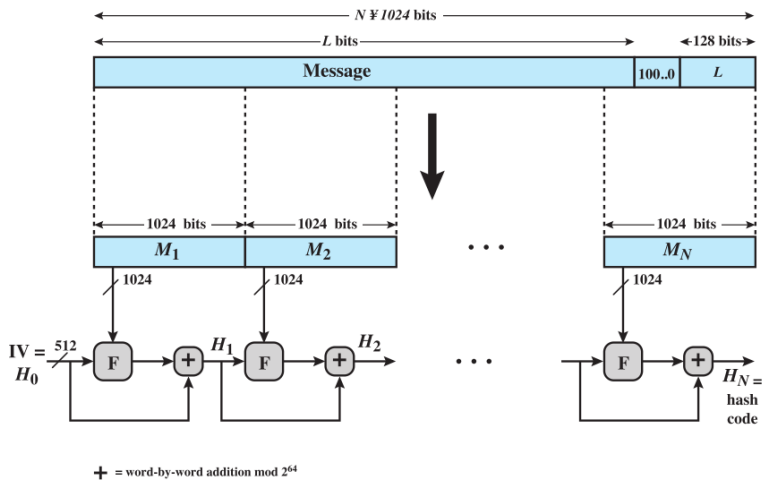


Figure 21.2 Message Digest Generation Using SHA-512

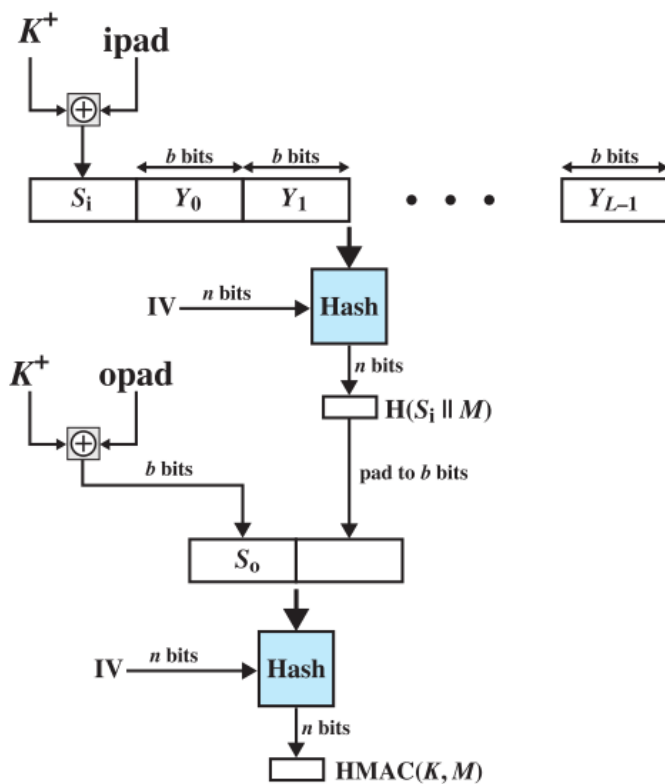


Figure 21.4 HMAC Structure

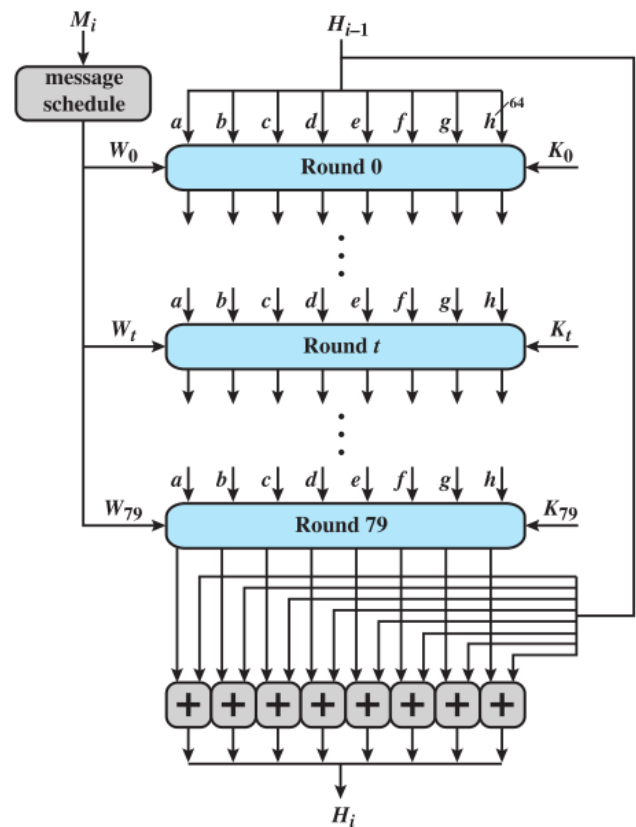


Figure 21.8 Diffie-Hellman Key Exchange

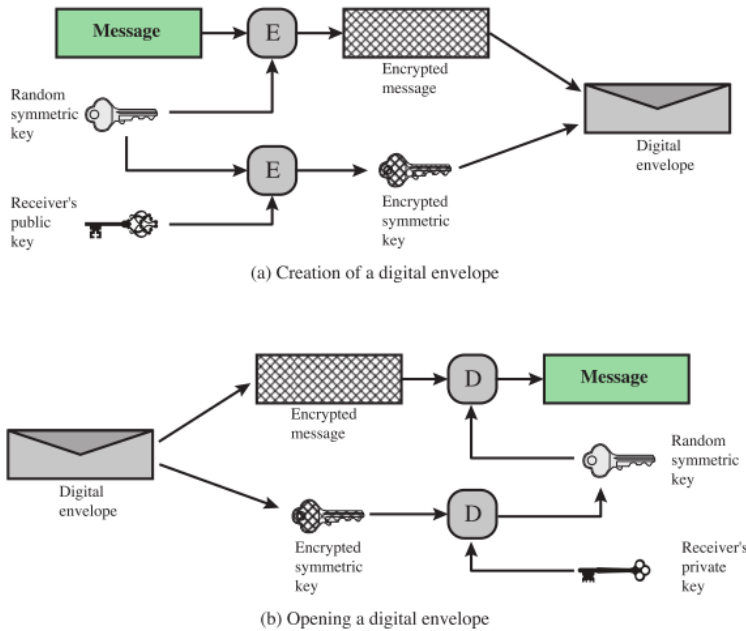


Figure 2.8 Digital Envelopes

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart	Electronic memory and processor inside	Biometric ID card
Contact	Electrical contacts exposed on surface	
Contactless	Radio antenna embedded inside	

## Types of Cards Used as Tokens

## Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed $s$ bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

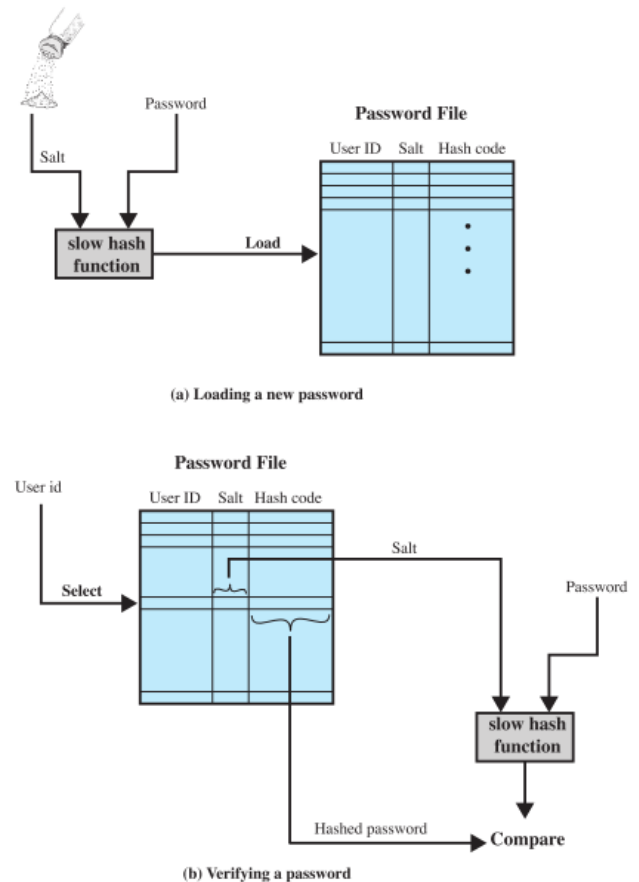


Figure 3.2 UNIX Password Scheme

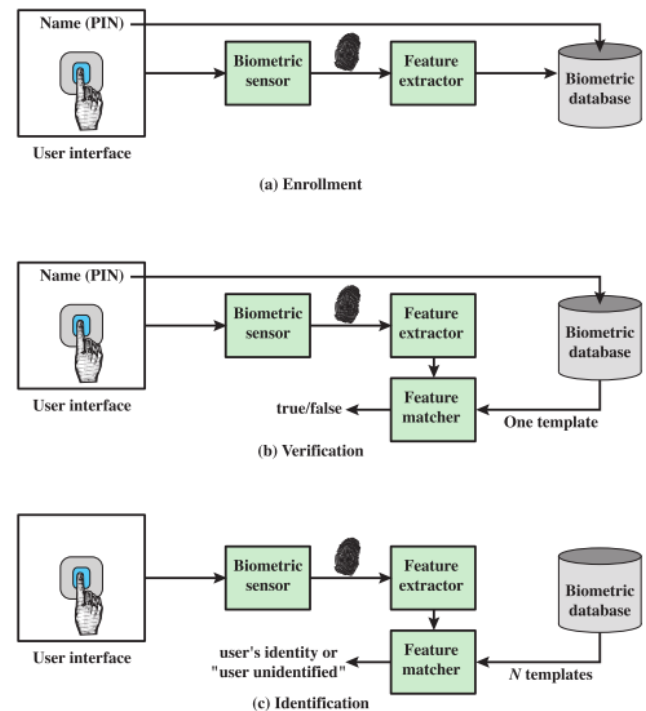


Figure 3.8 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.