SECURITY IN COMPUTING, FIFTH EDITION

Chapter 2: Toolbox: Authentication, Access Control, and Cryptography

Objectives for Chapter 2

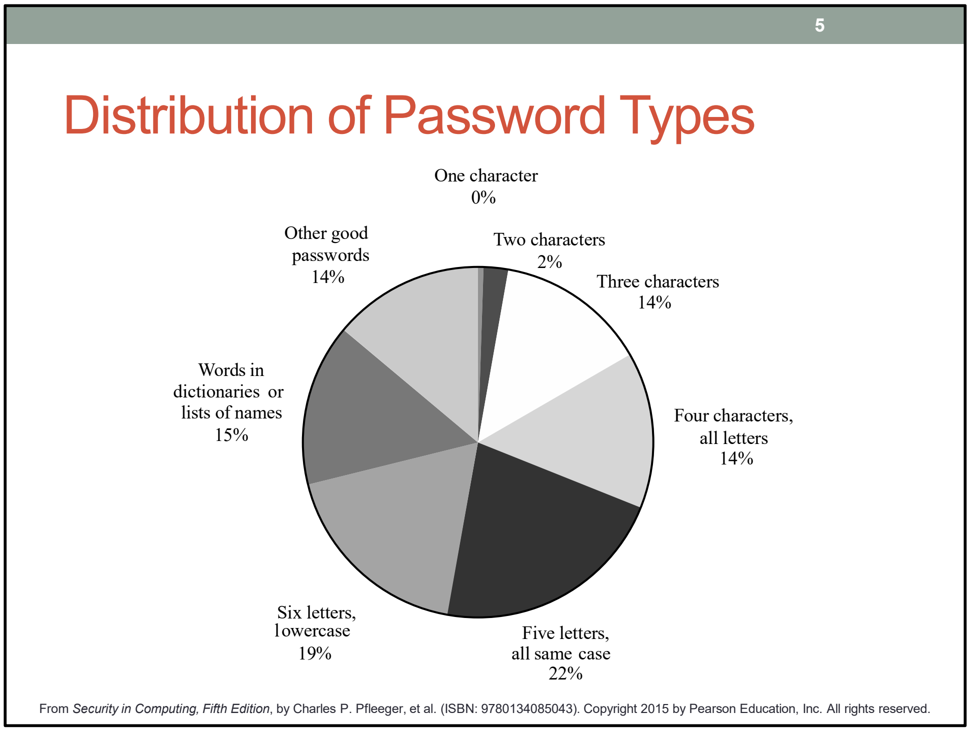
- Survey authentication mechanisms
- List available access control implementation options
- Explain the problems encryption is designed to solve
- Understand the various categories of encryption tools as well as the strengths, weaknesses, and applications of each
- Learn about certificates and certificate authorities

Authentication

- The act of proving that a user is who she says she is
- Methods:
  - Something the user *knows*
  - Something the user *is*
  - Something user *has*

Something You Know

- Passwords
- Security questions
- Attacks on “something you know”:
  - Dictionary attacks
  - Inferring likely passwords/answers
  - Guessing
  - Defeating concealment
  - Exhaustive or brute-force attack
  - Rainbow tables



Alhough this data is from an old study, more recent studies have reaffirmed the results. The vast majority of passwords used on the Internet are extremely easy to crack.

Password Storage

Plaintext

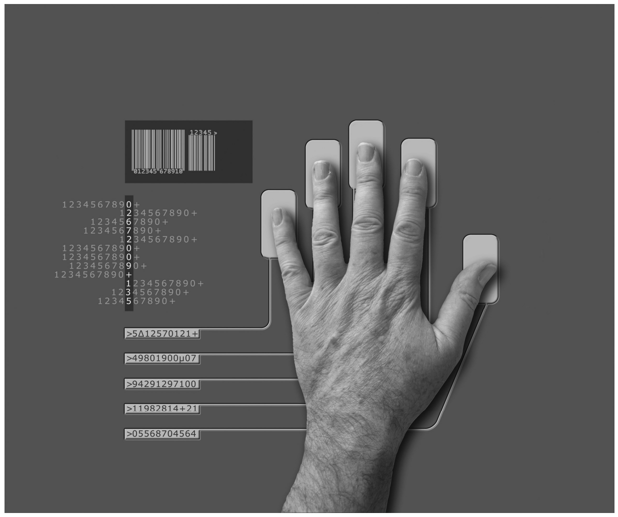
Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm$oto!4

Concealed

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

Passwords should never be stored in plaintext but rather should always be concealed. We talk more about proper password storage later.

Biometrics: Something You Are

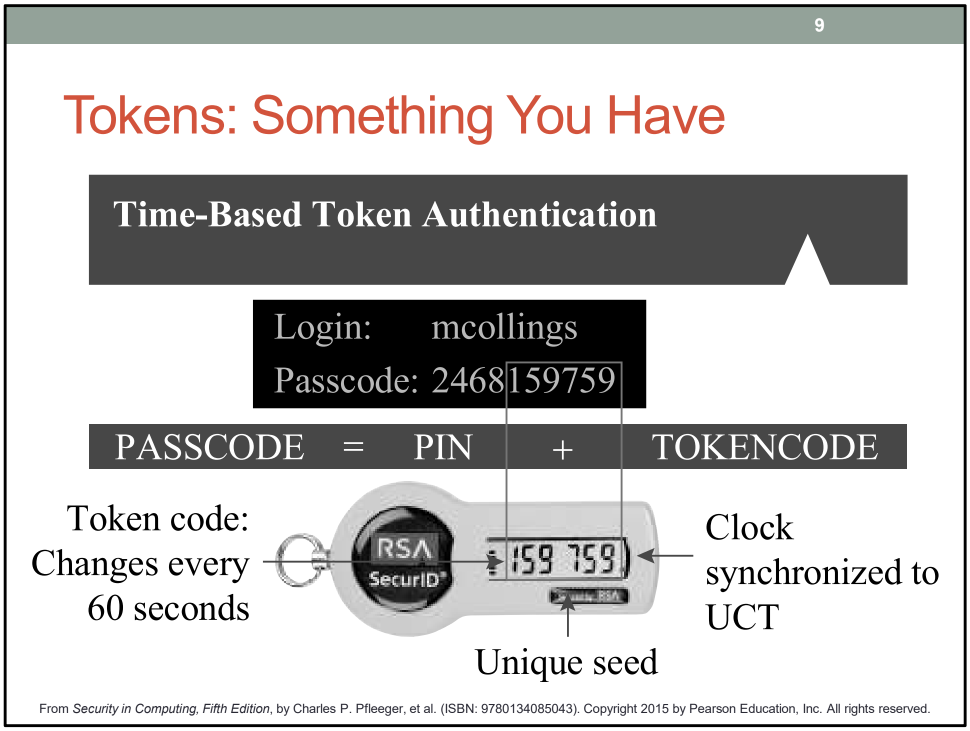


Handprints and fingerprints are two among many examples of biometrics.

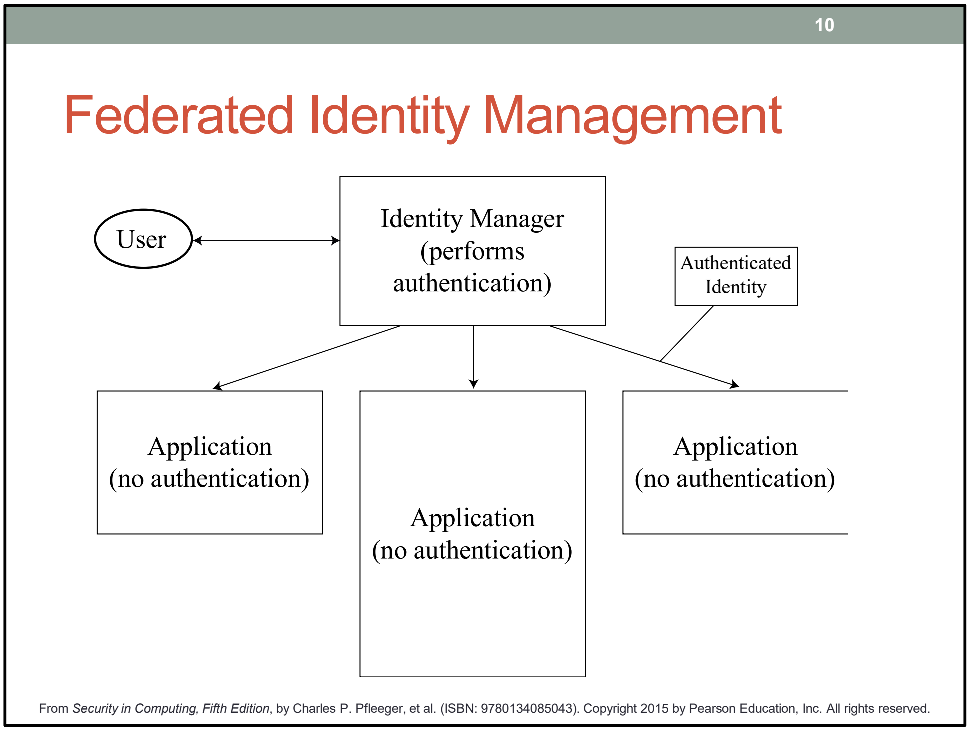
Problems with Biometrics

- Intrusive
- Expensive
- Single point of failure
- Sampling error
- False readings
- Speed
- Forgery

Recent advances in smartphones have begun to make biometrics cheaper and easier to use. Biometrics are still inadequate for extremely sensitive applications, but their convenience makes them a great alternative to weak passwords.

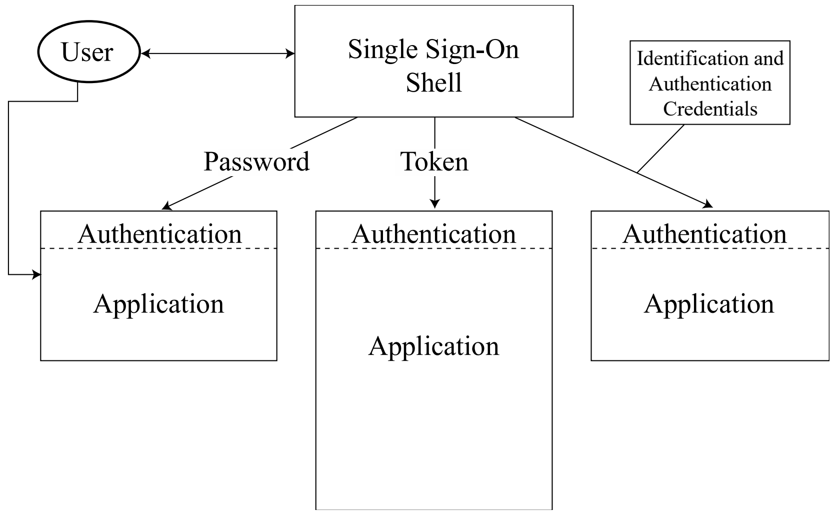


An RSA SecurID with a code that changes every 60 seconds. Physical possession of the token should be necessary for successful authentication.



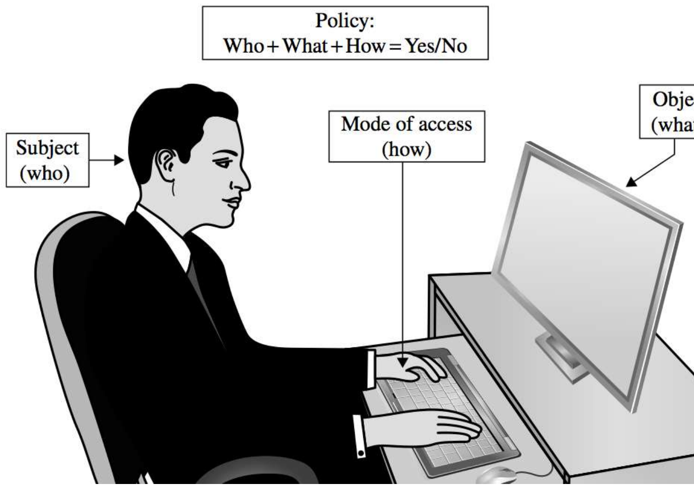
A federated identity management scheme is a union of separate identification and authentication systems. Authentication is performed in one place, and separate processes and systems determine that an already authenticated user is to be activated. Federated identity management is discussed in much greater detail in Chapter 8.

Single Sign-On



Single sign-on lets a user log on once per session but access many different applications/systems. It often works in conjunction with federated identity management, with the federated identity provider acting as the source of authentication for all the applications.

Access Control



Access Policies

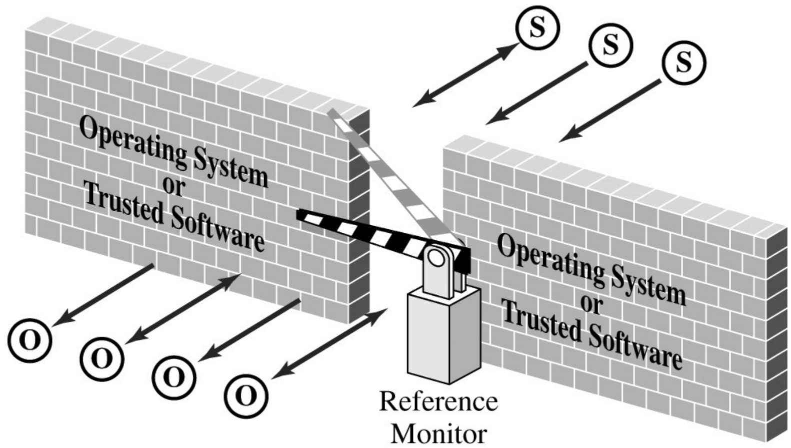
- Goals:
  - Check every access
  - Enforce least privilege
  - Verify acceptable usage
- Track users' access
- Enforce at appropriate granularity
- Use audit logging to track accesses

Implementing Access Control

- Reference monitor
- Access control directory
- Access control matrix
- Access control list
- Privilege list
- Capability
- Procedure-oriented access control
- Role-based access control

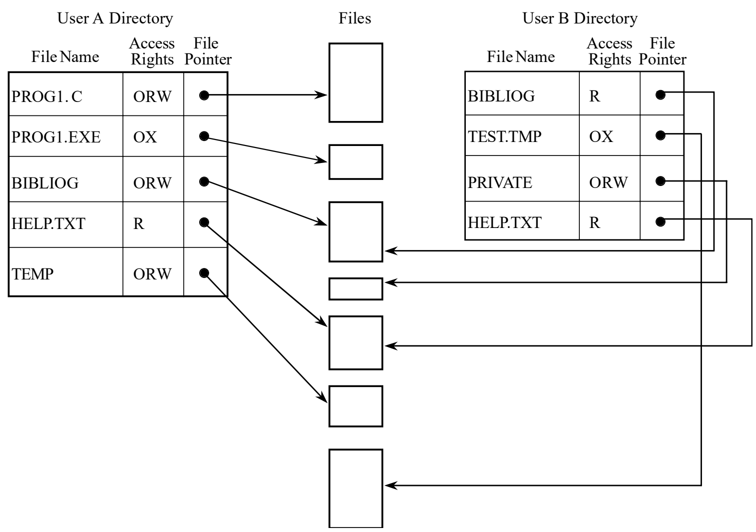
Many of these items are shown in more detail in the following slides. Access control directories, matrixes, and lists are shown in self-explanatory visual representations.

Reference Monitor



A reference monitor is the primary access control enforcement mechanism of the operating system. It is discussed in more detail in Chapter 5.

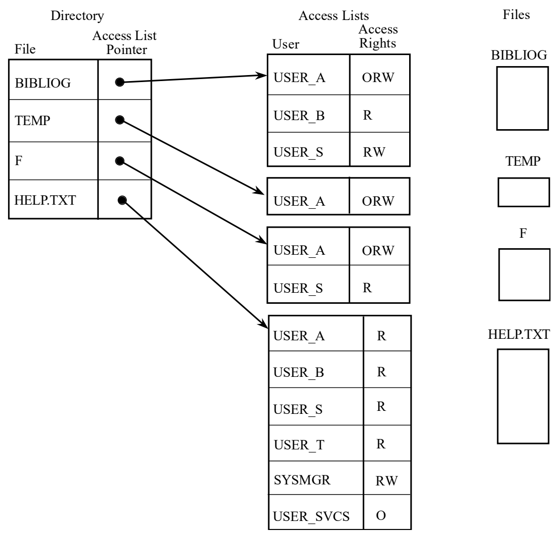
Access Control Directory



Access Control Matrix

	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	-	-	R	X	X	R	W
USER S	RW	-	R	R	X	X	R	W
USER T	-	-	-	R	X	X	R	W
SYS_MGR	-	-	-	RW	OX	OX	ORW	O
USER_SVCS	-	-	-	O	X	X	R	W

Access Control List



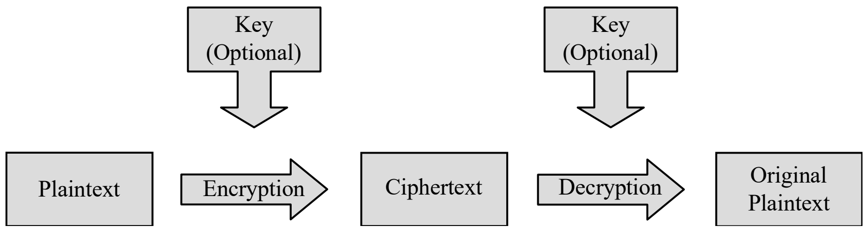
Problems Addressed by Encryption

- Suppose a sender wants to send a message to a recipient. An attacker may attempt to
  - Block the message
  - Intercept the message
  - Modify the message
  - Fabricate an authentic-looking alternate message

Encryption Terminology

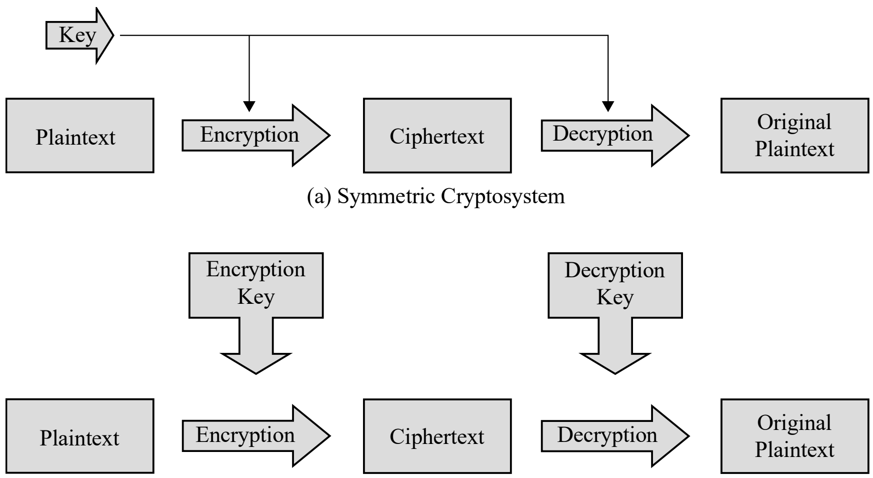
- Sender
- Recipient
- Transmission medium
- Interceptor/intruder
- Encrypt, encode, or encipher
- Decrypt, decode, or decipher
- Cryptosystem
- Plaintext
- Ciphertext

Encryption/Decryption Process



The basic process of encrypting and then decrypting data.

Symmetric vs. Asymmetric

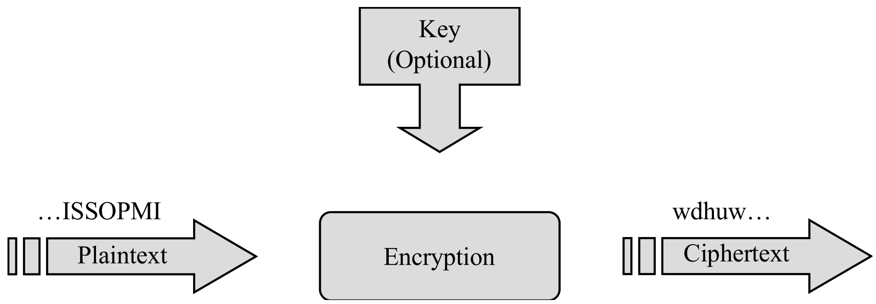


(a) Symmetric Cryptosystem

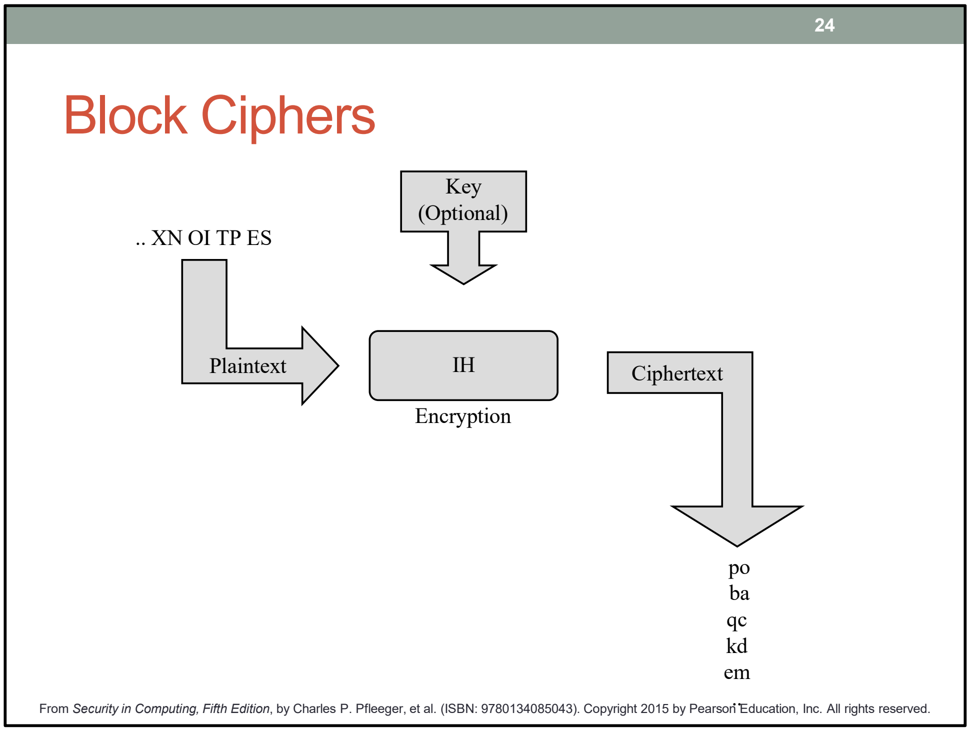
(b) Asymmetric Cryptosystem

The critical difference between symmetric and asymmetric is that symmetric uses a single key for both encryption and decryption, whereas asymmetric uses complementary keys.

Stream Ciphers



In stream ciphers, each byte of the data stream is encrypted separately. This is as opposed to block ciphers, which are shown on the next slide.



Unlike a stream cipher, a block cipher encrypts a group of plaintext symbols as a single block. The pros and cons of each model are discussed on the next slide.

Stream vs. Block

	Stream	Block
Advantages	• Speed of transformation • Low error propagation	• High diffusion • Immunity to insertion of symbol
Disadvantages	• Low diffusion • Susceptibility to malicious insertions and modifications	• Slowness of encryption • Padding • Error propagation

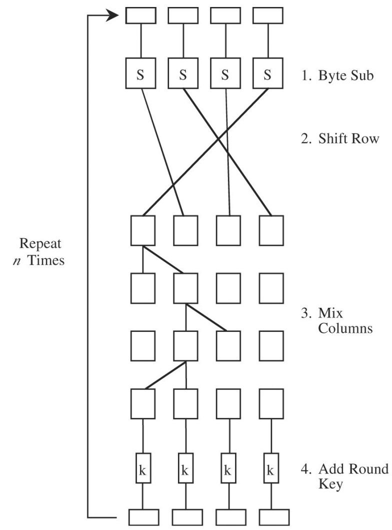
DES: The Data Encryption Standard

- Symmetric block cipher
- Developed in 1976 by IBM for the US National Institute of Standards and Technology (NIST)

Form	Operation	Properties	Strength
DES	Encrypt with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
Double DES	Encrypt with first key; then encrypt result with second key	Two 56-bit keys	Only doubles strength of 56-bit key version
Two-key triple DES	Encrypt with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit keys	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
Three-key triple DES	Encrypt with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit keys	Gives strength equivalent to about 112-bit key about 72 quintillion ($72*10^{15}$) times as strong as 56-bit version

AES: Advanced Encryption System

- Symmetric block cipher
- Developed in 1999 by independent Dutch cryptographers
- Still in common use



DES vs. AES

	DES	AES
Date designed	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length); up to 112 bits with multiple keys	128, 192, 256 (and possibly more) bits
Operations	16 rounds	10, 12, 14 (depending on key length); can be increased
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but open public comments and criticisms invited
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

AES has become the dominant symmetric encryption algorithm in use today. We discuss DES in this book both for historical purposes and because it is a relatively simple algorithm to use to explain how cryptographic primitives work.

Public Key (Asymmetric) Cryptography

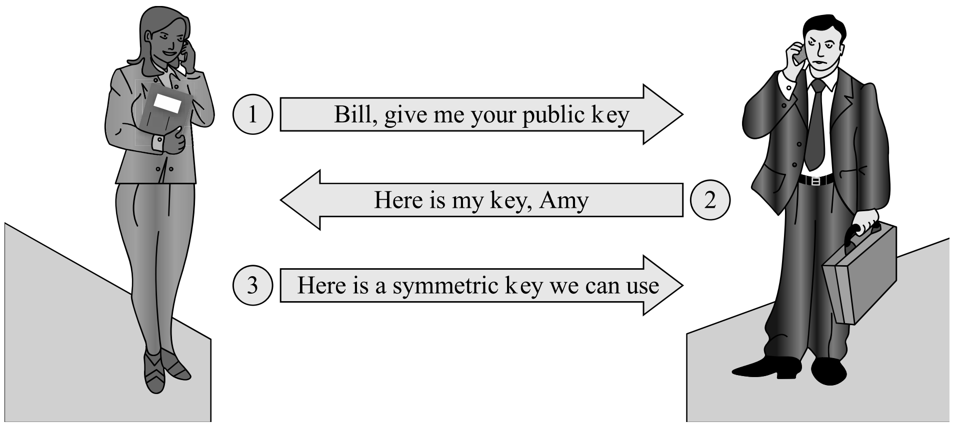
- Instead of two users sharing one secret key, each user has two keys: one public and one private
- Messages encrypted using the user's public key can only be decrypted using the user's private key, and vice versa

Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Unlimited; typically no less than 256; 1000 to 2000 currently considered desirable for most uses
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

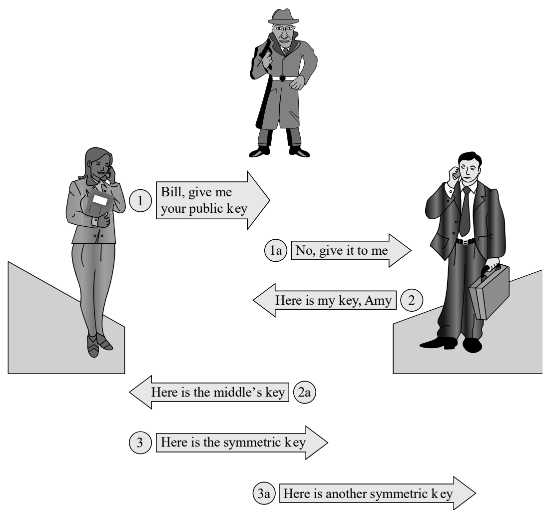
Symmetric and asymmetric algorithms have complementary strengths and weaknesses and are therefore used both for different purposes and in concert with each other.

Public Key to Exchange Secret Keys



This is a great example of asymmetric and symmetric encryption being used together. We need asymmetric to perform the initial exchange securely, but thereafter we can benefit from the speed of a symmetric algorithm.

Key Exchange Man in the Middle



This exchange is the same as on the previous slide, but with an attacker in the middle. This attack can be defeated using the simple tweak described on pp. 107–108 of the textbook. This is an interesting problem to have students brainstorm or work on for homework.

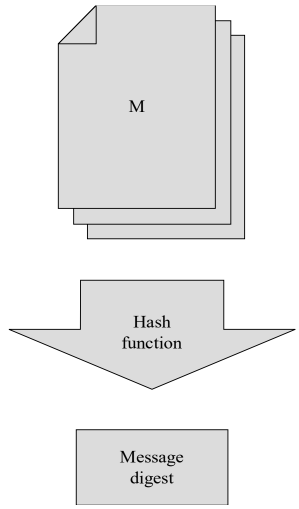
Error Detecting Codes

- Demonstrates that a block of data has been modified
- Simple error detecting codes:
  - Parity checks
  - Cyclic redundancy checks
- Cryptographic error detecting codes:
  - One-way hash functions
  - Cryptographic checksums
  - Digital signatures

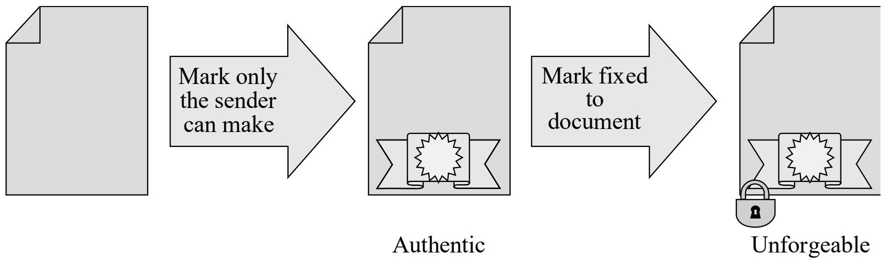
Parity Check

Original Data	Parity Bit	Modified Data	Modification Detected?
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 0 1	Yes
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 0	Yes
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 1	No
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 1 1	No
0 0 0 0 0 0 0 0	1	0 0 0 0 0 1 1 1	Yes
0 0 0 0 0 0 0 0	1	0 0 0 0 1 1 1 1	No
0 0 0 0 0 0 0 0	1	0 1 0 1 0 1 0 1	No
0 0 0 0 0 0 0 0	1	1 1 1 1 1 1 1 1	No

One-Way Hash Function

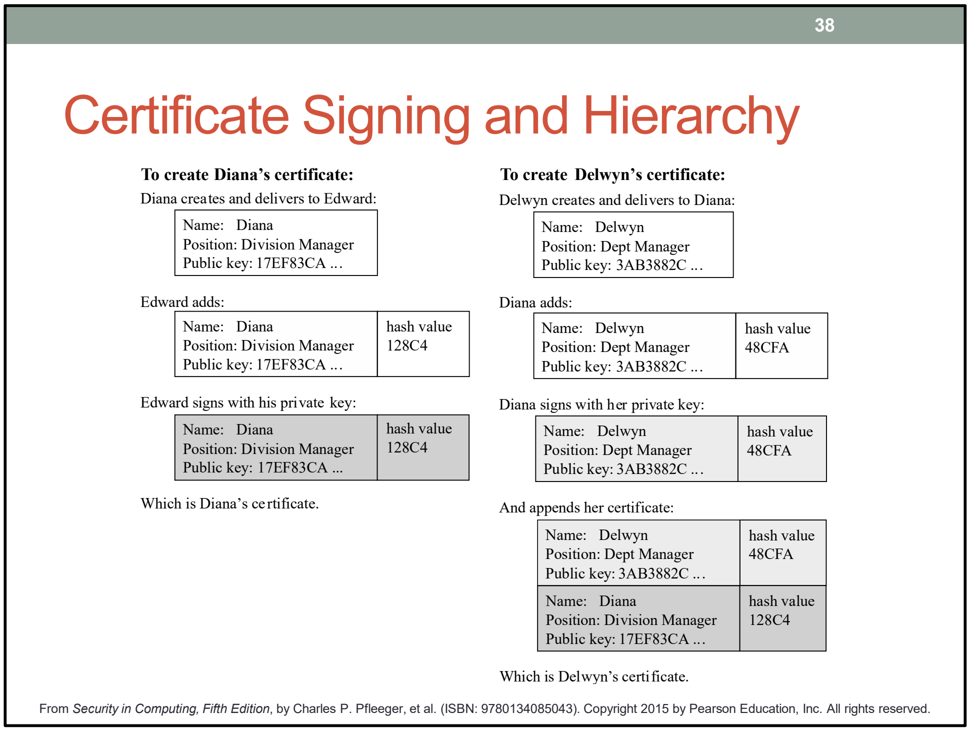


Digital Signature



Certificates: Trustable Identities and Public Keys

- A certificate is a public key and an identity bound together and signed by a certificate authority.
- A certificate authority is an authority that users trust to accurately verify identities before generating certificates that bind those identities to keys.



Diana’s certificate is made using Edward’s signature. Delwyn’s certificate includes Diana’s certificate so that it can effectively be tied back to Edward, creating a chain of trust.

Cryptographic Tool Summary

Tool	Uses
Secret key (symmetric) encryption	Protecting confidentiality and integrity of data at rest or in transit
Public key (asymmetric) encryption	Exchanging (symmetric) encryption keys Signing data to show authenticity and proof of origin
Error detection codes	Detect changes in data
Hash codes and functions (forms of error detection codes)	Detect changes in data
Cryptographic hash functions	Detect changes in data, using a function that only the data owner can compute (so an outsider cannot change both data and the hash code result to conceal the fact of the change)
Error correction codes	Detect and repair errors in data
Digital signatures	Attest to the authenticity of data
Digital certificates	Allow parties to exchange cryptographic keys with confidence of the identities of both parties

Summary

- Users can authenticate using something they know, something they are, or something they have
- Systems may use a variety of mechanisms to implement access control
- Encryption helps prevent attackers from revealing, modifying, or fabricating messages
- Symmetric and asymmetric encryption have complementary strengths and weaknesses
- Certificates bind identities to digital signatures