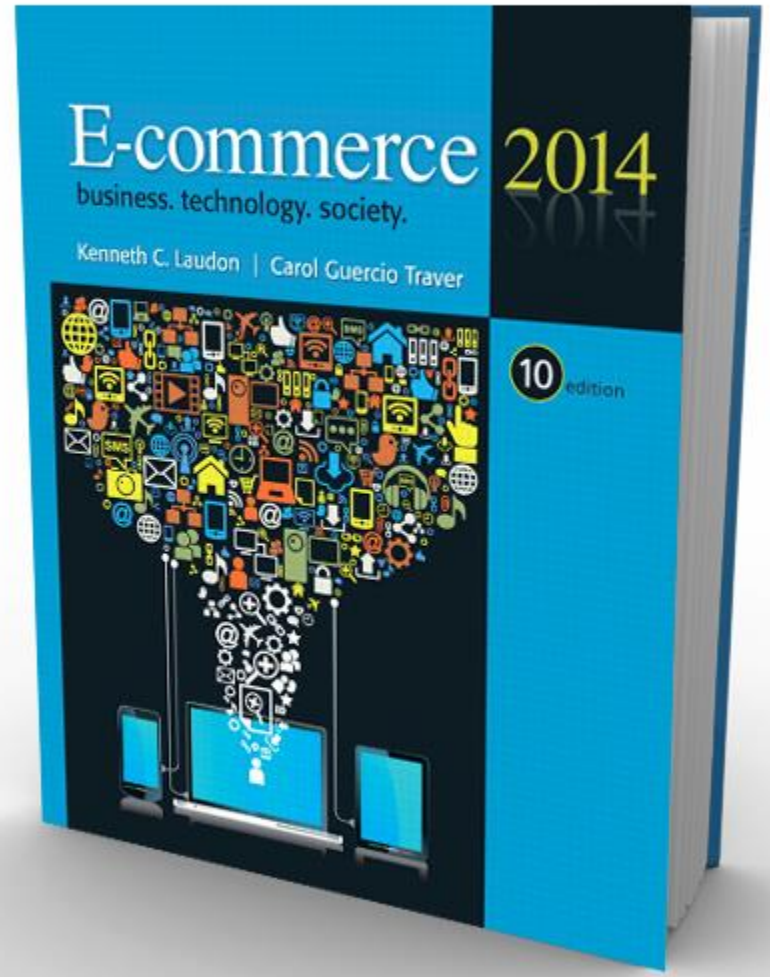


E-commerce 2014

business. technology. society.

tenth edition

Kenneth C. Laudon

Carol Guercio Traver

Chapter 5

E-commerce Security and Payment Systems

Definitions Of Risk

International Organization for Standardization (ISO):

"The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat."

Risk Reduction Methods

- Terminate the Risk,
- Minimize Probability of Occurrence,
- Minimize Impact,
- Transfer/Insurance

What Is Good E-commerce Security?

- **To achieve highest degree of security**
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws
- **Other factors**
  - Time value of money
  - Cost of security vs. potential loss
  - Security often breaks at weakest link

The E-commerce Security Environment

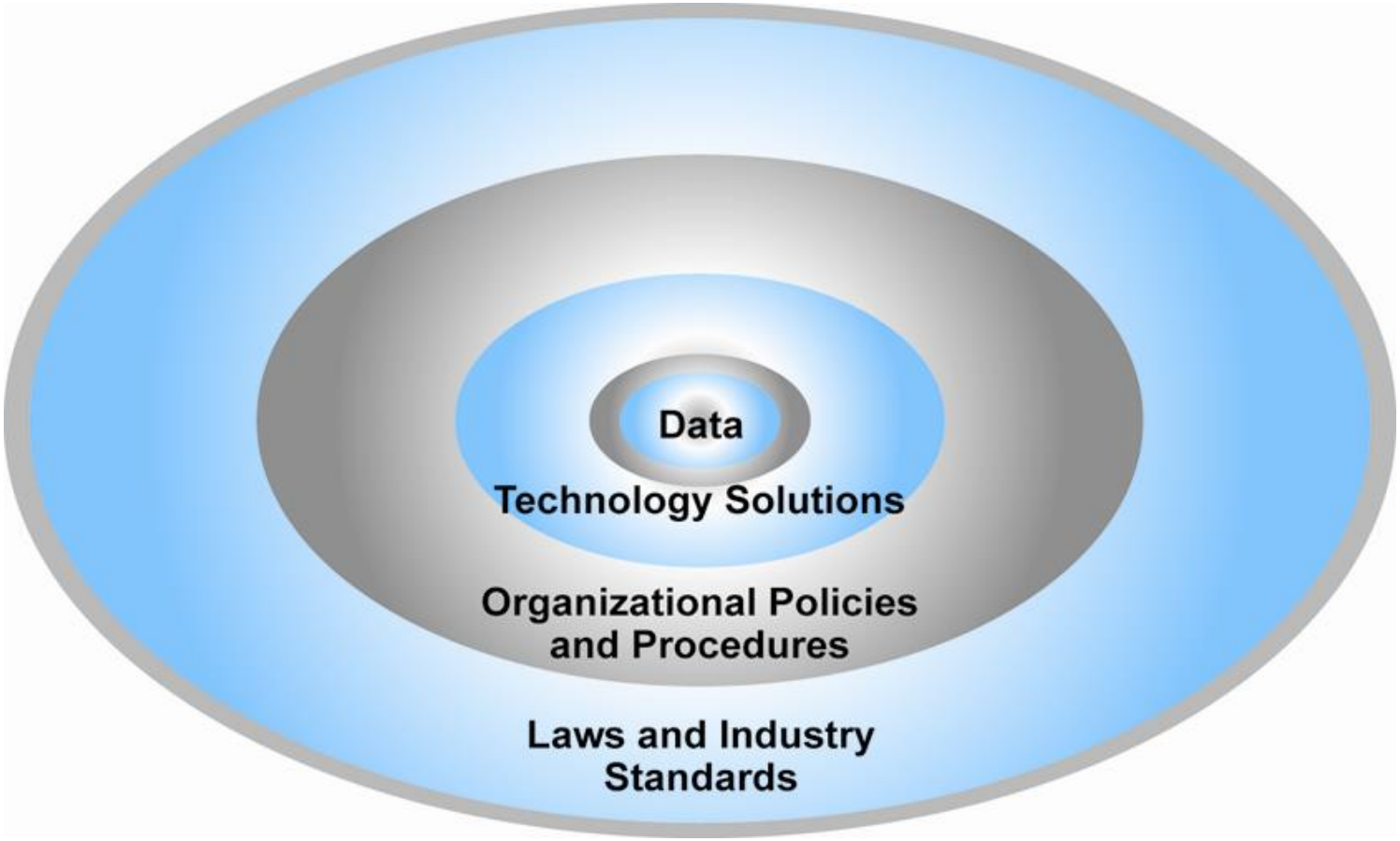


Figure 5.1, Page 252

TABLE 5.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Table 5.3, Page 254

The Tension Between Security and Other Values

- **Ease of use**
  - The more security measures added, the more difficult a site is to use, and the slower it becomes
- **Public safety and criminal uses of the Internet**
  - Use of technology by criminals to plan crimes or threaten nation-state

Security Threats in the E-commerce Environment

- **Three key points of vulnerability in e-commerce environment:**
  1. Client
  2. Server
  3. Communications pipeline (Internet communications channels)

Most Common Security Threats in the E-commerce Environment

- **Malicious code (malware, exploits)**
  - Drive-by downloads
  - Viruses
  - Worms
  - Ransomware
  - Trojan horses
  - Backdoors
  - Bots, botnets
  - Threats at both client and server levels

Most Common Security Threats (cont.)

- **Potentially unwanted programs (PUPs)**
  - Browser parasites
  - Adware
  - Spyware
- **Phishing**
  - Social engineering
  - E-mail scams
  - Spear-phishing
  - Identity fraud/theft

Most Common Security Threats (cont.)

- **Hacking**
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats
  - Hacktivism
- **Cybervandalism:**
  - Disrupting, defacing, destroying Web site
- **Data breach**
  - Losing control over corporate information to outsiders

Most Common Security Threats (cont.)

- Credit card fraud/theft
- Spoofing and pharming
- Spam (junk) Web sites (link farms)
- Identity fraud/theft
- Denial of service (DoS) attack
  - Hackers flood site with useless traffic to overwhelm network
- Distributed denial of service (DDoS) attack

Most Common Security Threats (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider attacks**
- **Poorly designed server and client software**
- **Social network security issues**
- **Mobile platform security issues**
  - Vishing, smishing, madware
- **Cloud security issues**

Technology Solutions

- **Protecting Internet communications**
  - Encryption
- **Securing channels of communication**
  - SSL (Secure Sockets Layer), VPNs
- **Protecting networks**
  - Firewalls
- **Protecting servers and clients**

Tools Available to Achieve Site Security

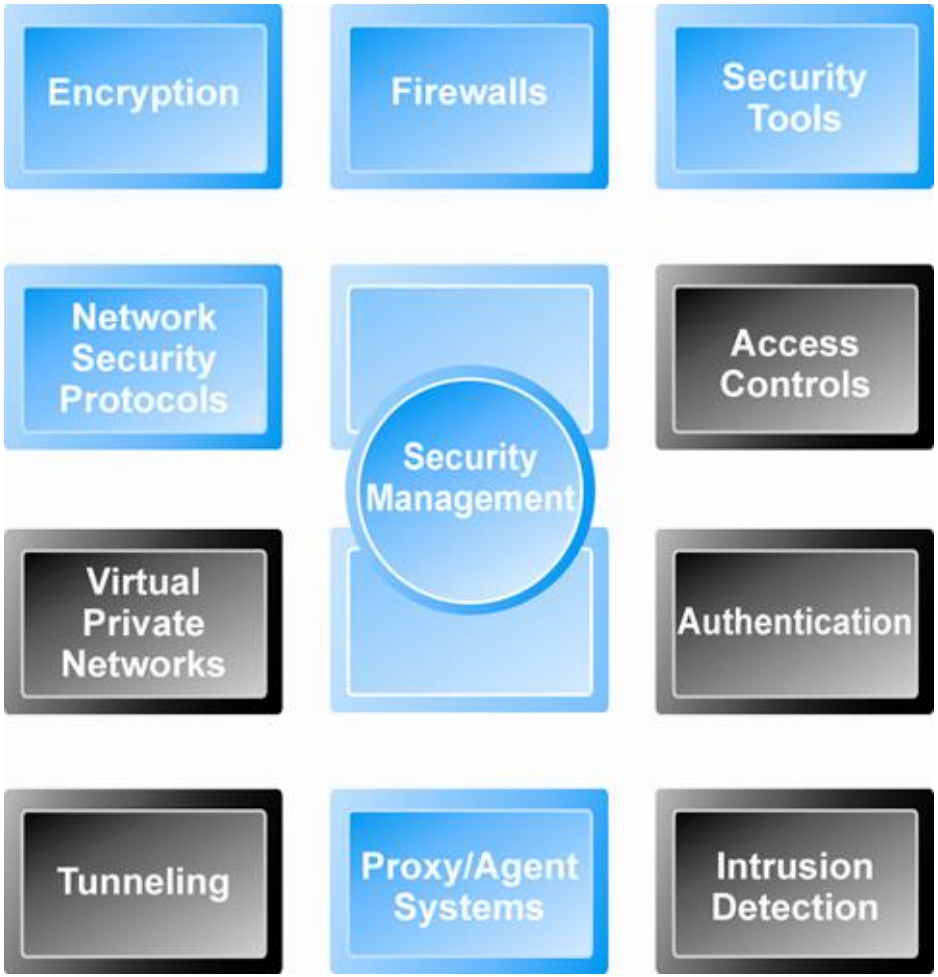


Figure 5.5, Page 276

Limits to Encryption Solutions

- **Doesn't protect storage of private key**
  - PKI not effective against insiders, employees
  - Protection of private keys by individuals may be haphazard
- **No guarantee that verifying computer of merchant is secure**
- **CAs are unregulated, self-selecting organizations**

Securing Channels of Communication

- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)**
  - Establishes secure, negotiated client–server session
- **Virtual Private Network (VPN)**
  - Allows remote users to securely access internal network via the Internet
- **Wireless (Wi-Fi) networks**
  - WPA2

Protecting Networks

- **Firewall**
  - Hardware or software
  - Uses security policy to filter packets
  - Two main methods:
    - Packet filters
    - Application gateways
- **Proxy servers (proxies)**
  - Software servers that handle all communications from or sent to the Internet
- **Intrusion detection systems**
- **Intrusion prevention systems**

Firewalls and Proxy Servers

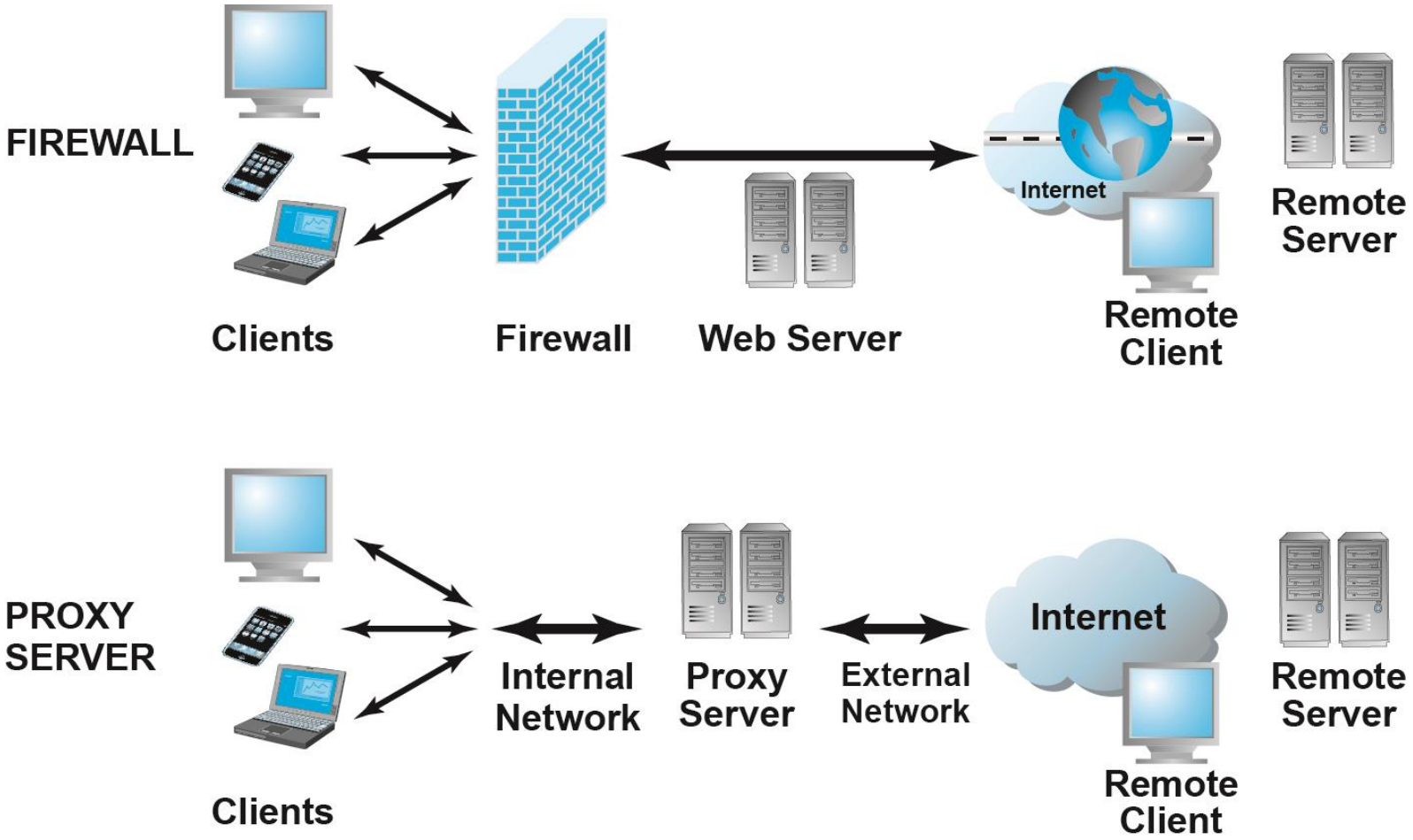


Figure 5.11, Page 289

Protecting Servers and Clients

- **Operating system security enhancements**
  - Upgrades, patches
- **Anti-virus software**
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

Management Policies, Business Procedures, and Public Laws

- **Worldwide, companies spend more than $65 billion on security hardware, software, services**
- **Managing risk includes:**
  - Technology
  - Effective management policies
  - Public laws and active enforcement

A Security Plan: Management Policies

- **Risk assessment**
- **Security policy**
- **Implementation plan**
  - Security organization
  - Access controls
  - Authentication procedures, including biometrics
  - Authorization policies, authorization management systems
- **Security audit**

Developing an E-commerce Security Plan

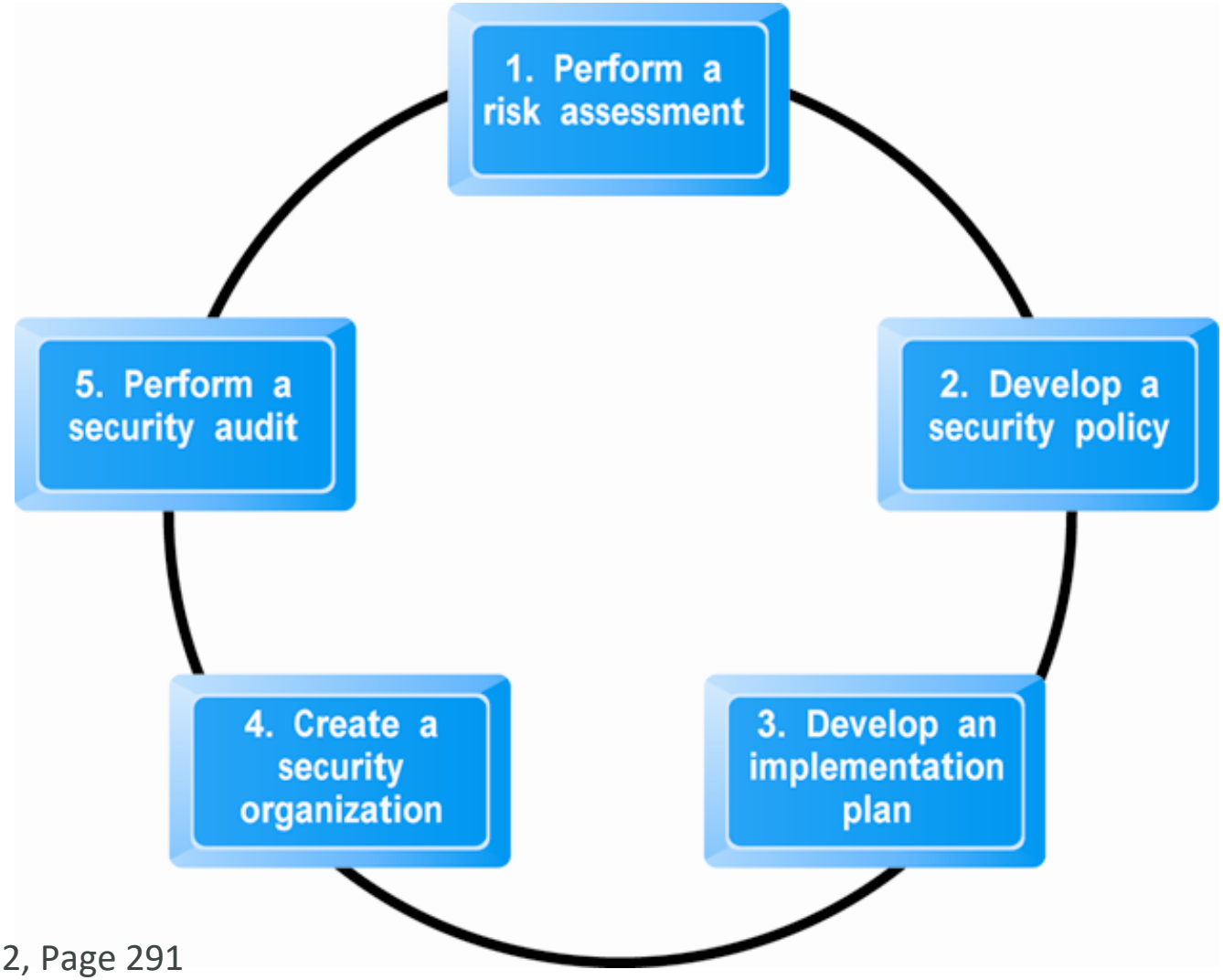


Figure 5.12, Page 291

The Role of Laws and Public Policy

- **Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:**
  - National Information Infrastructure Protection Act of 1996
  - USA Patriot Act
  - Homeland Security Act
- **Private and private-public cooperation**
  - CERT Coordination Center
  - US-CERT
- **Government policies and controls on encryption software**
  - OECD, G7/G8, Council of Europe, Wassener Arrangement

Types of Payment Systems

- **Cash**
  - Most common form of payment
  - Instantly convertible into other forms of value
  - No float
- **Checking transfer**
  - Second most common payment form in United States
- **Credit card**
  - Credit card associations
  - Issuing banks
  - Processing centers

Types of Payment Systems (cont.)

- **Stored value**
  - Funds deposited into account, from which funds are paid out or withdrawn as needed
  - Debit cards, gift certificates
  - Peer-to-peer payment systems
- **Accumulating balance**
  - Accounts that accumulate expenditures and to which consumers make period payments
  - Utility, phone, American Express accounts

Payment System Stakeholders

- **Consumers**
  - Low-risk, low-cost, refutable, convenience, reliability
- **Merchants**
  - Low-risk, low-cost, irrefutable, secure, reliable
- **Financial intermediaries**
  - Secure, low-risk, maximizing profit
- **Government regulators**
  - Security, trust, protecting participants and enforcing reporting

E-commerce Payment Systems

- **Credit cards**
  - 42% of online payments in 2013 (United States)
- **Debit cards**
  - 29% online payments in 2013 (United States)
- **Limitations of online credit card payment**
  - Security, merchant risk
  - Cost
  - Social equity

How an Online Credit Transaction Works

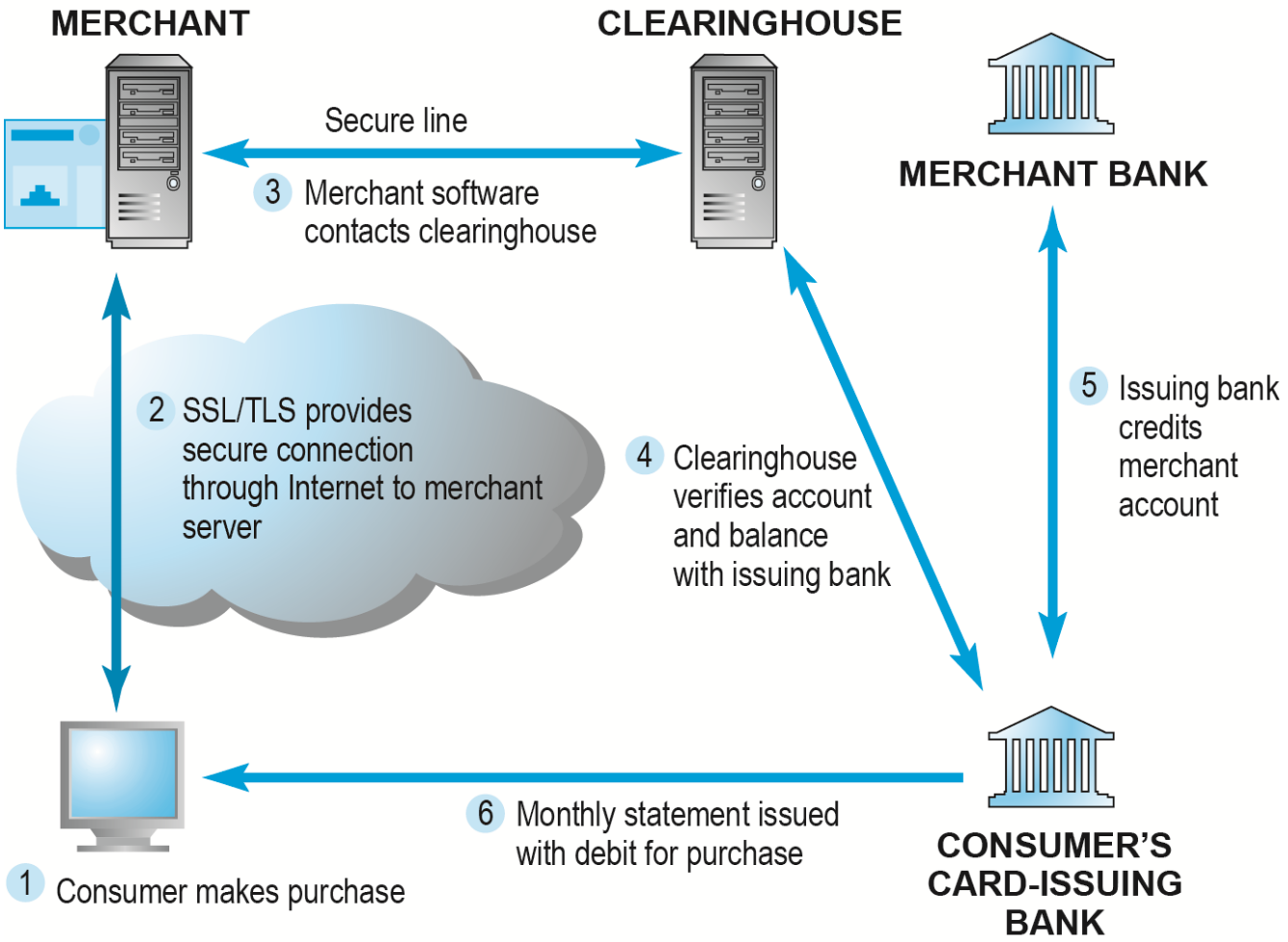


Figure 5.15, Page 302

Alternative Online Payment Systems

- **Online stored value systems:**
  - Based on value stored in a consumer's bank, checking, or credit card account
  - Example: PayPal
- **Other alternatives:**
  - Amazon Payments
  - Google Checkout
  - Bill Me Later
  - WUPay, Dwolla, Stripe

Mobile Payment Systems

- **Use of mobile phones as payment devices established in Europe, Japan, South Korea**
- **Near field communication (NFC)**
  - Short-range (2”) wireless for sharing data between devices
- **Expanding in United States**
  - Google Wallet
    - Mobile app designed to work with NFC chips
  - PayPal
  - Square

Digital Cash and Virtual Currencies

- **Digital cash**
  - Based on algorithm that generates unique tokens that can be used in "real" world
  - Example: Bitcoin
- **Virtual currencies**
  - Circulate within internal virtual world
  - Example: Linden Dollars in Second Life, Facebook Credits

Electronic Billing Presentment and Payment (EBPP)

- **Online payment systems for monthly bills**
- **50% of all bill payments**
- **Two competing EBPP business models:**
  - Biller-direct (dominant model)
  - Consolidator
- **Both models are supported by EBPP infrastructure providers**

Cryptography

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

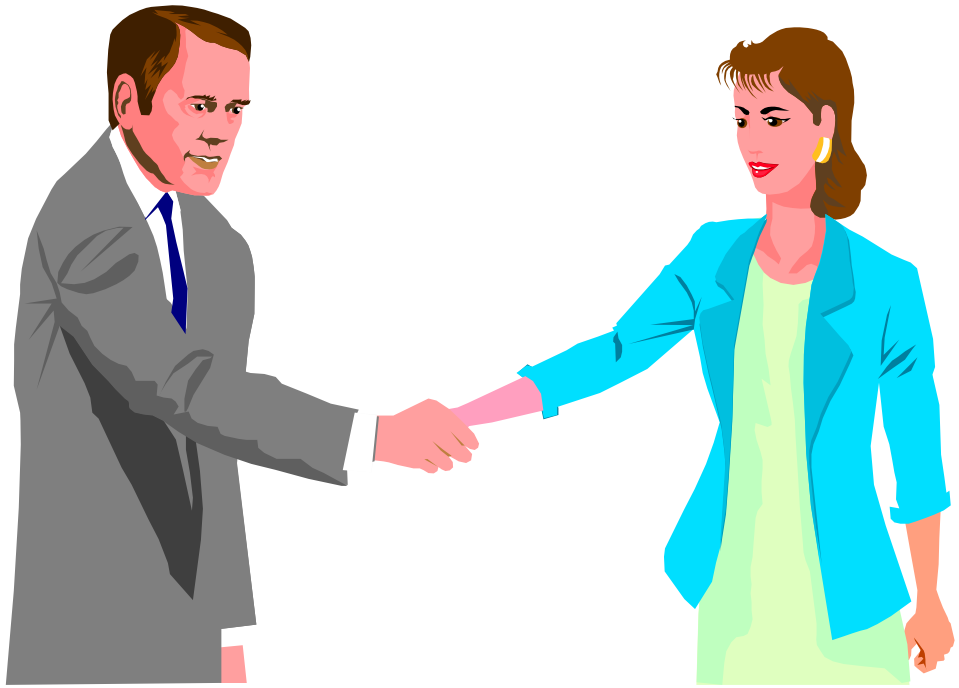
- I AM SPARTA
- 42 11 23 34 53 11 24 44 11

Do you agree that trust is the basis of all business / commercial transactions?

What are the elements of trust which you would look for in a business relationship?

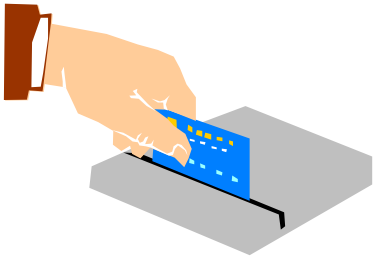
A MATTER OF TRUST

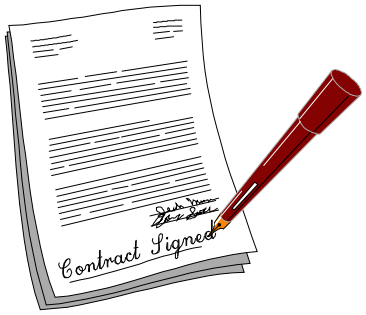
- Building Trust: Direct trust relationship



Some every day transactions:

Credit Card

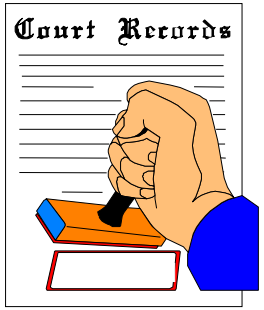




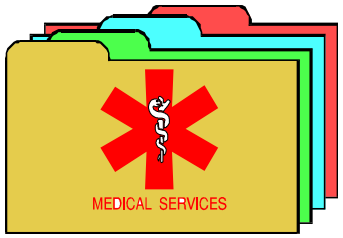
Contract

Why do we place trust in these transactions?

- Authentication
- Access control
- Confidentiality
- Integrity
- Non-repudiation



Notarized Document



Medical Records

So, why PKI?

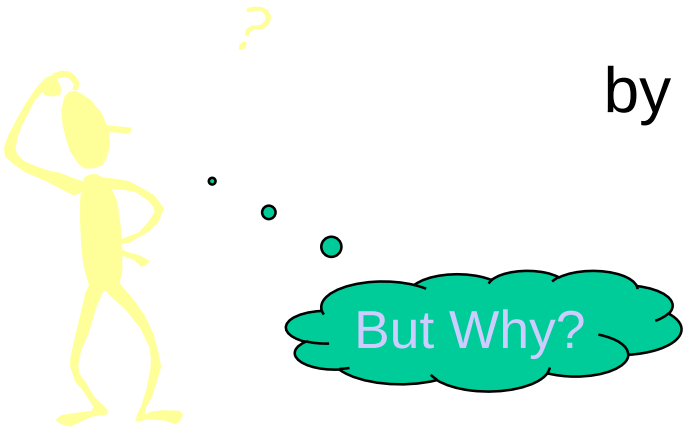
- PKI technology provides all of the elements we expect from a secure transaction
  - Authentication
  - Access control
  - Confidentiality
  - Integrity
  - Non-repudiation

What is Public Key Infrastructure?

"...a system for establishing the identity of people who hold cryptographic keys."

---Web Security & Commerce

by Simson Garfinkel & Gene Spafford



What is a PKI? Another definition.

- A system that establishes and maintains trustworthy e-business environments through the generation and distribution of keys and certificates.

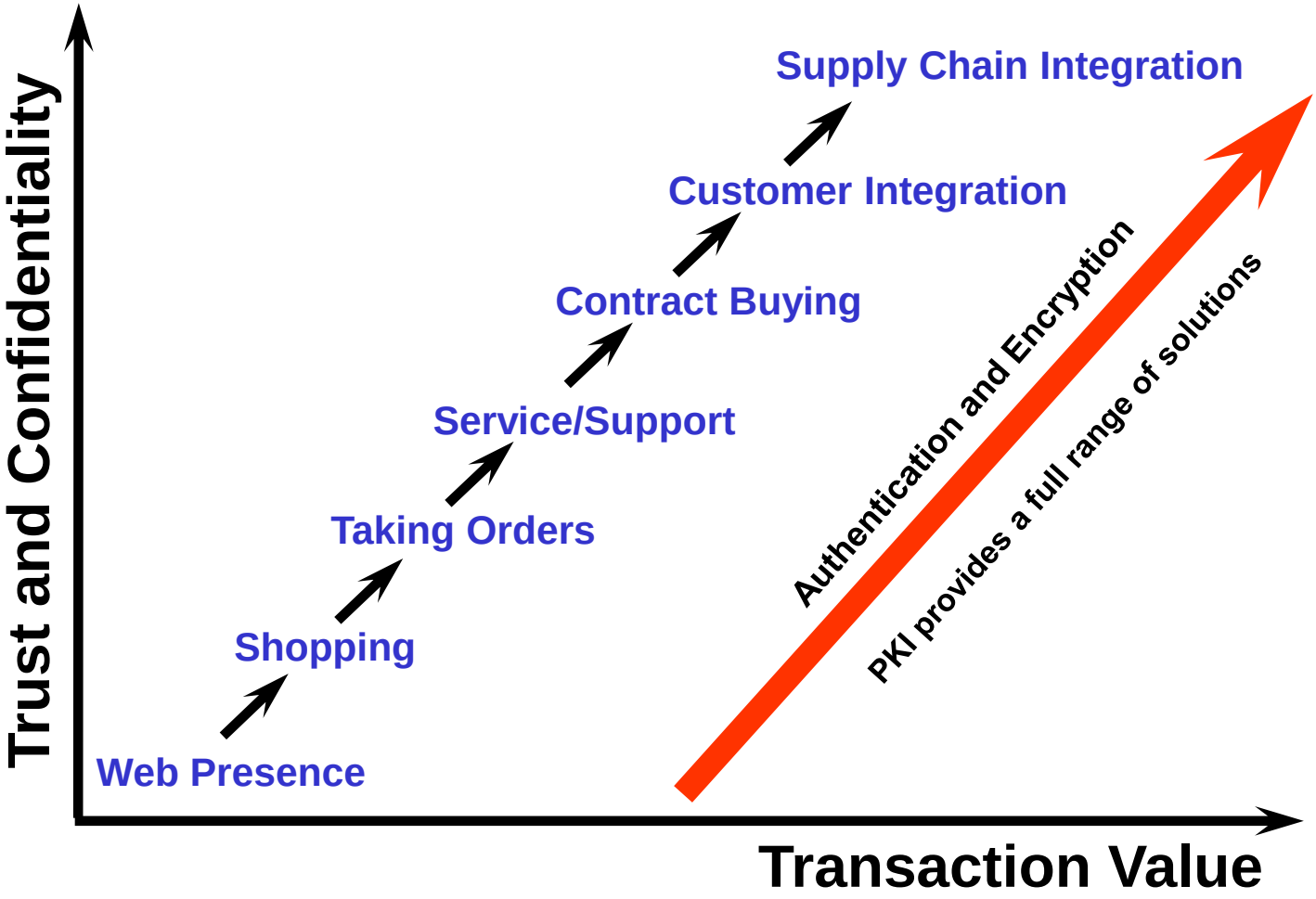
What is a PKI? Yet, another definition.

Public Key Infrastructure (*abbr. PKI*) a comprehensive system that provides public-key encryption and digital signature services to ensure confidentiality, access control, data integrity, authentication and non-repudiation.

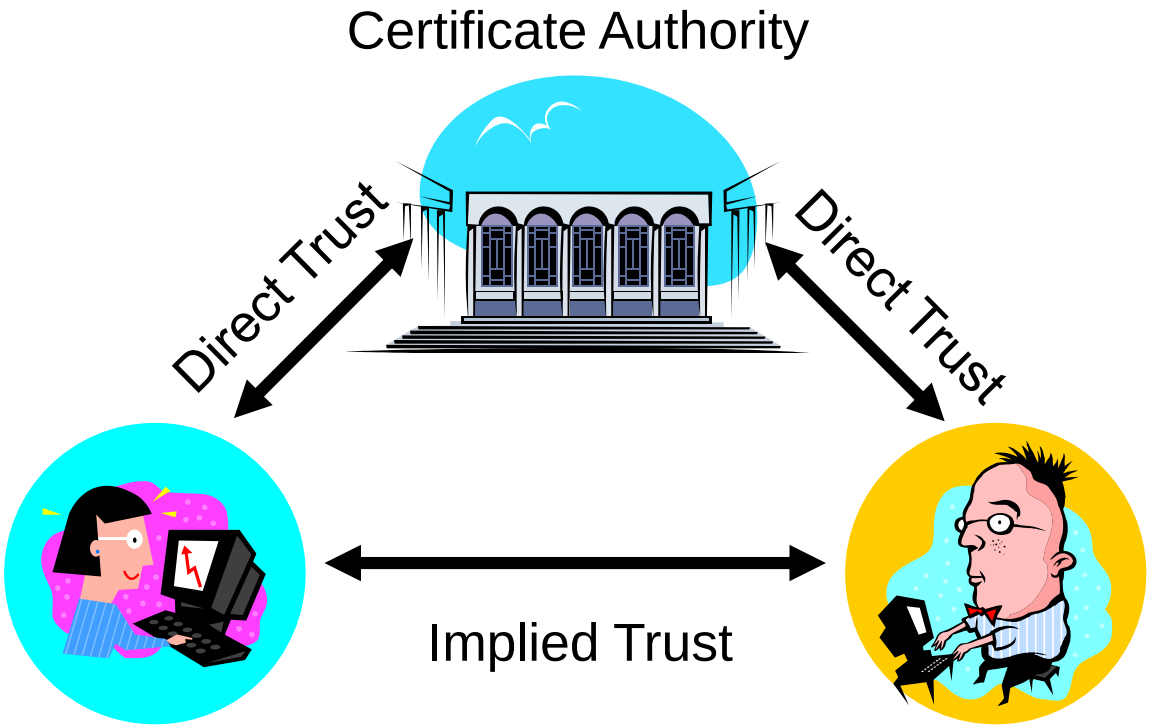
Why the need for PKI?

- Internet-enabled E-Commerce
  - -- identify users accessing sensitive information? (Authentication)
  - – control who accesses information (Access Control)
  - – be sure communication is private but carried over the Internet? (Privacy)
  - – ensure data has not been tampered with? (Integrity)
  - – provide a digital method of signing information and transactions? (Non-repudiation)

What Level of Trust (or Security)?



- Building Trust: Third party trust relationship



PKI Components

- Public/private key pair

- Digital certificate

- Certificate authority

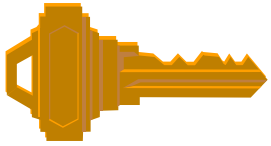
- LDAP directory

- Authentication device

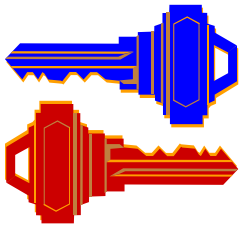
LDAP: Lightweight Directory Access Protocol

Cryptography

Symmetric Key Encryption

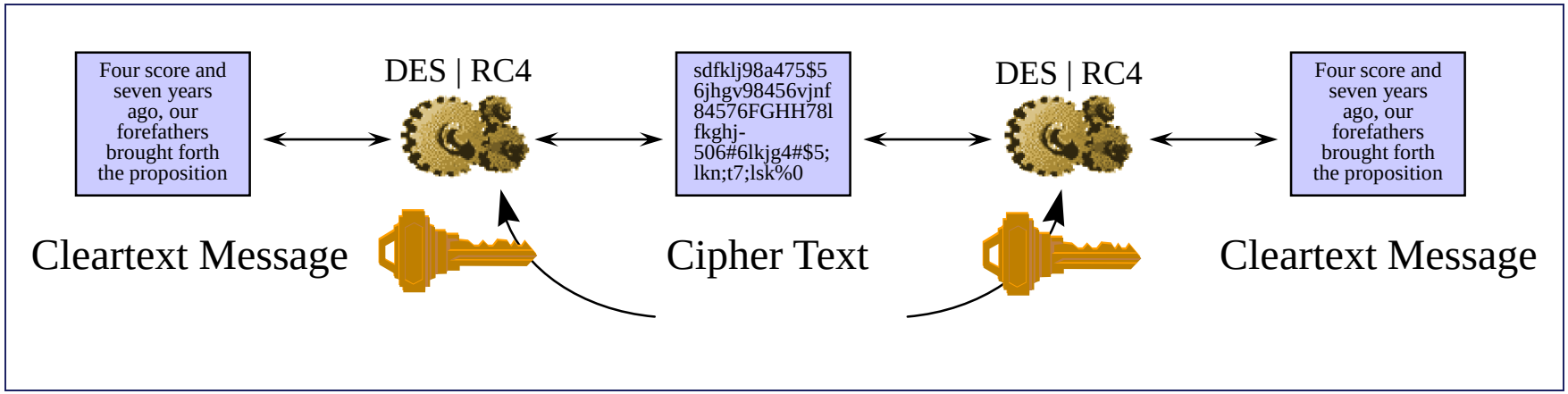


Public Key Encryption



Message Digest

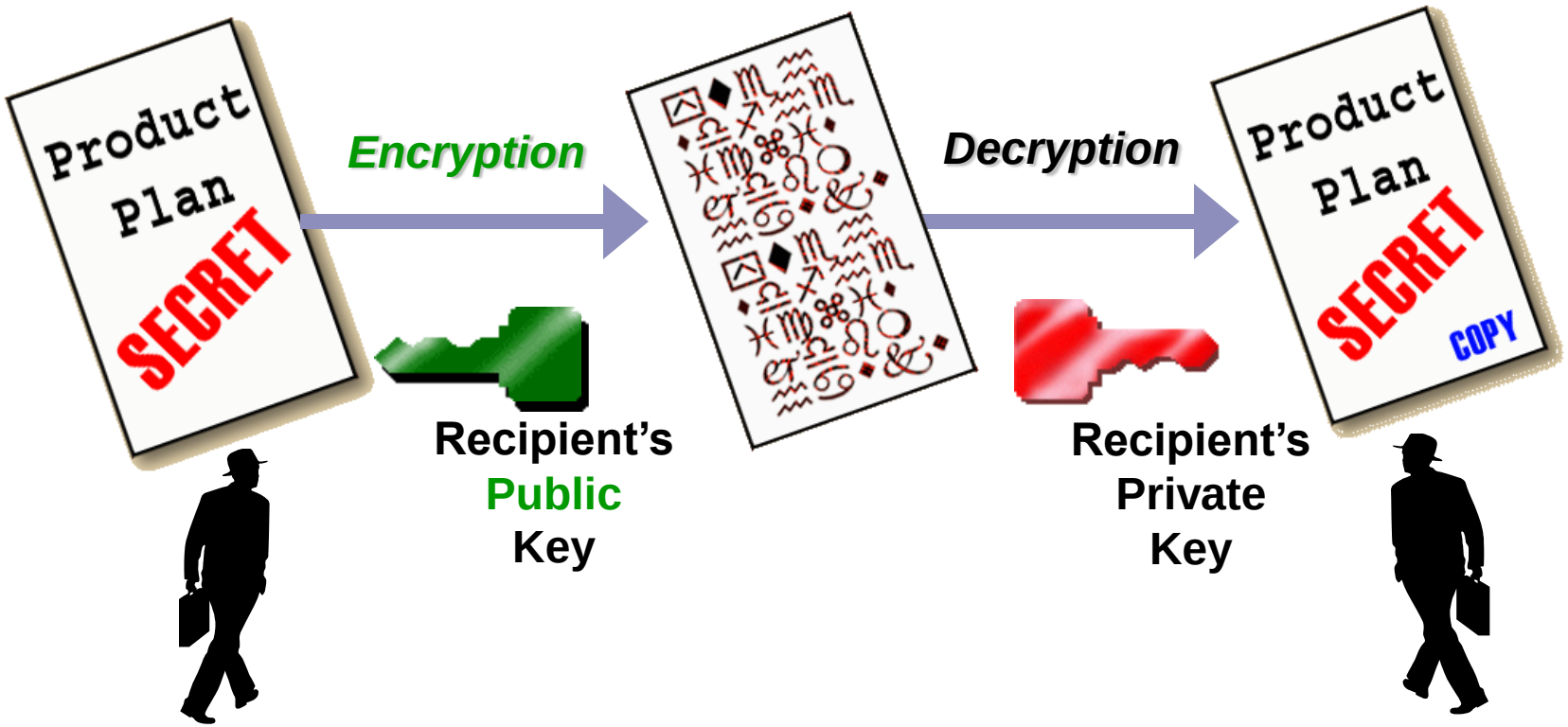
Symmetric Key Encryption



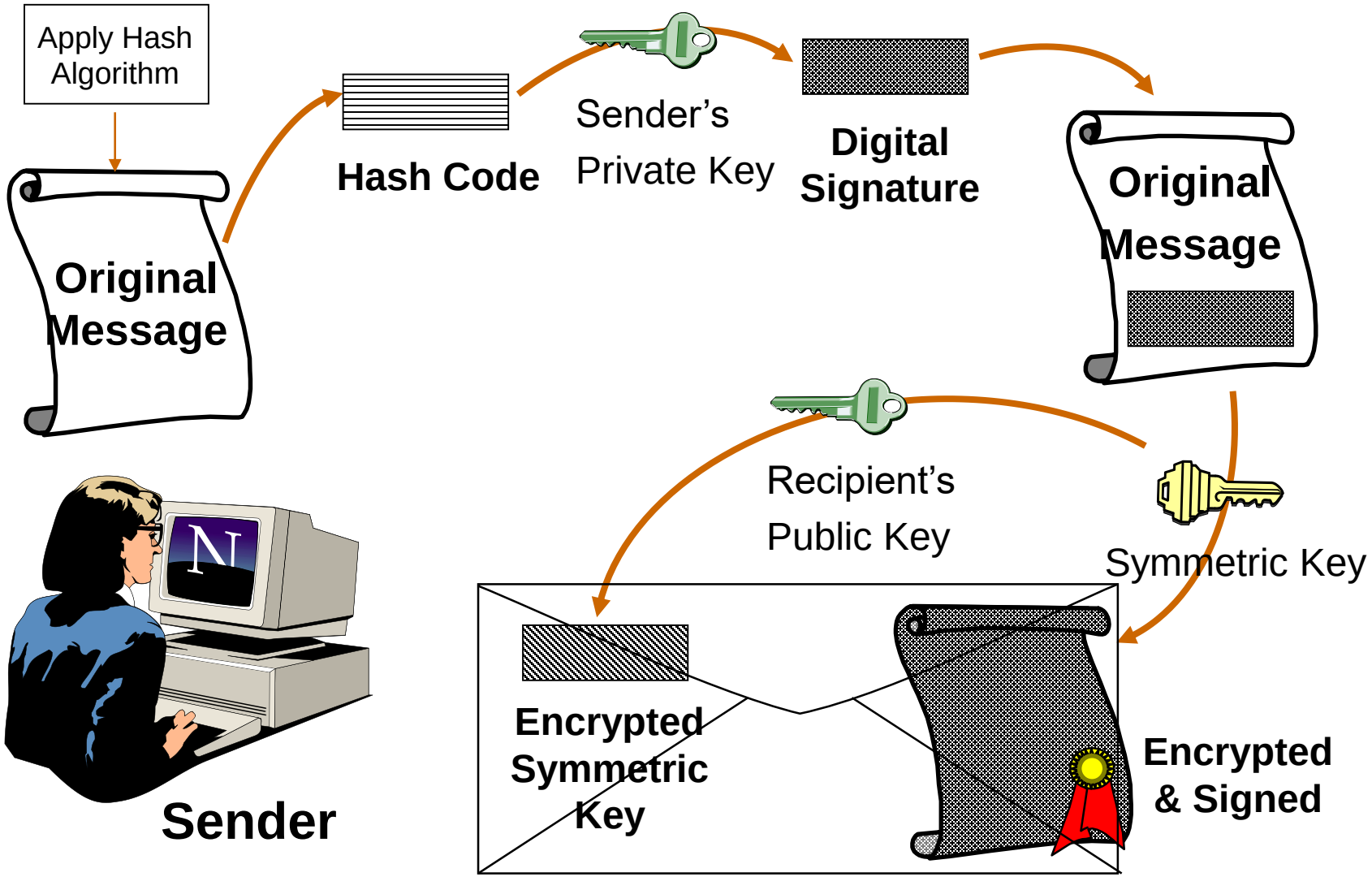
DEC: digital electronic control

Public/Private Key

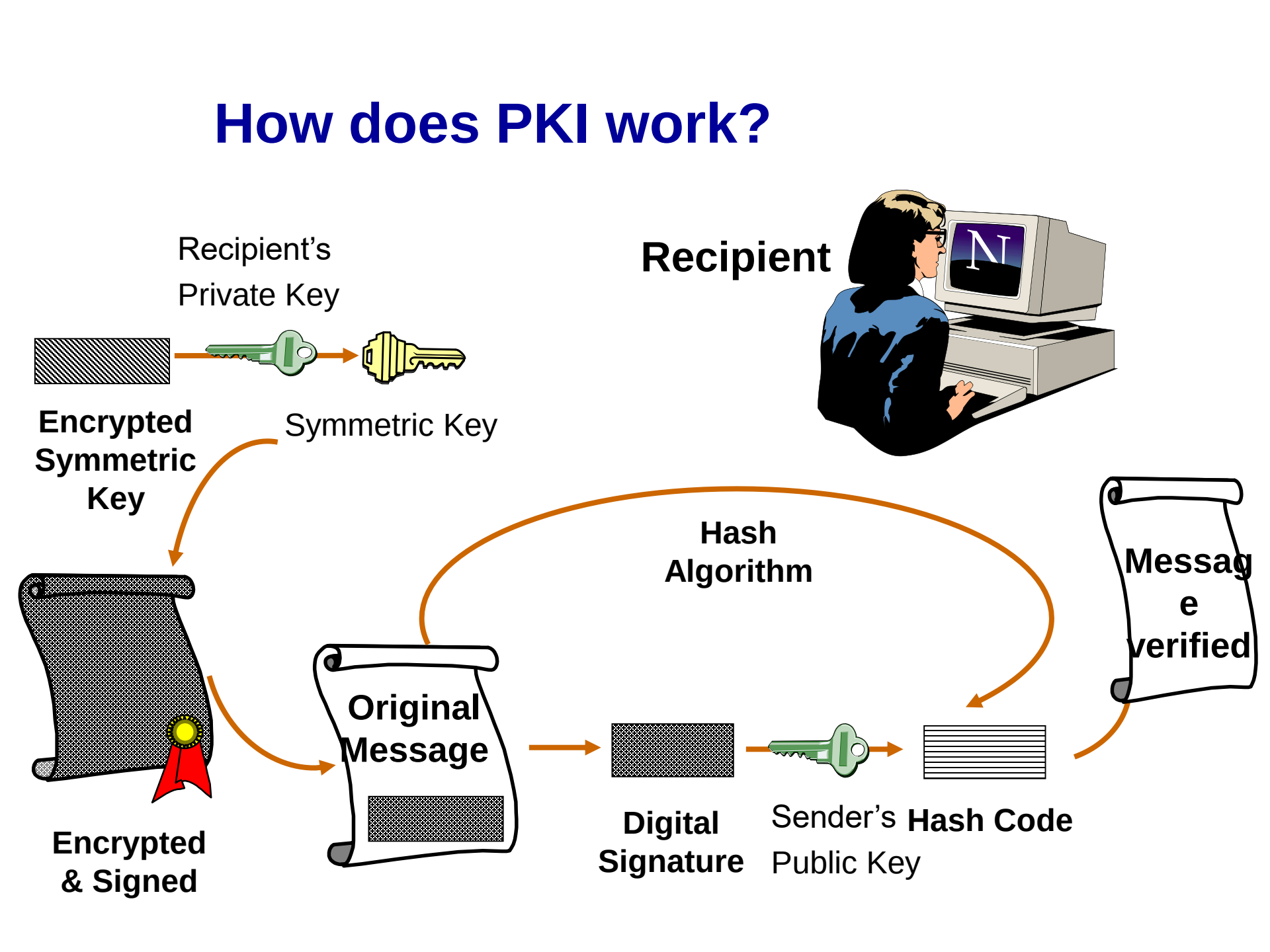
One half of a key pair is used to encrypt, the other half is used to decrypt.



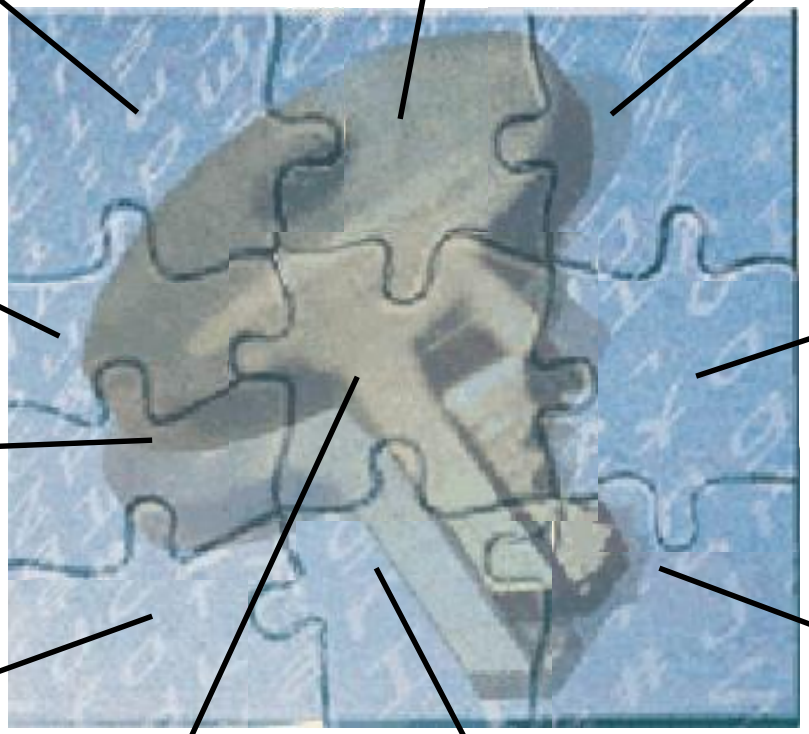
How does PKI work?



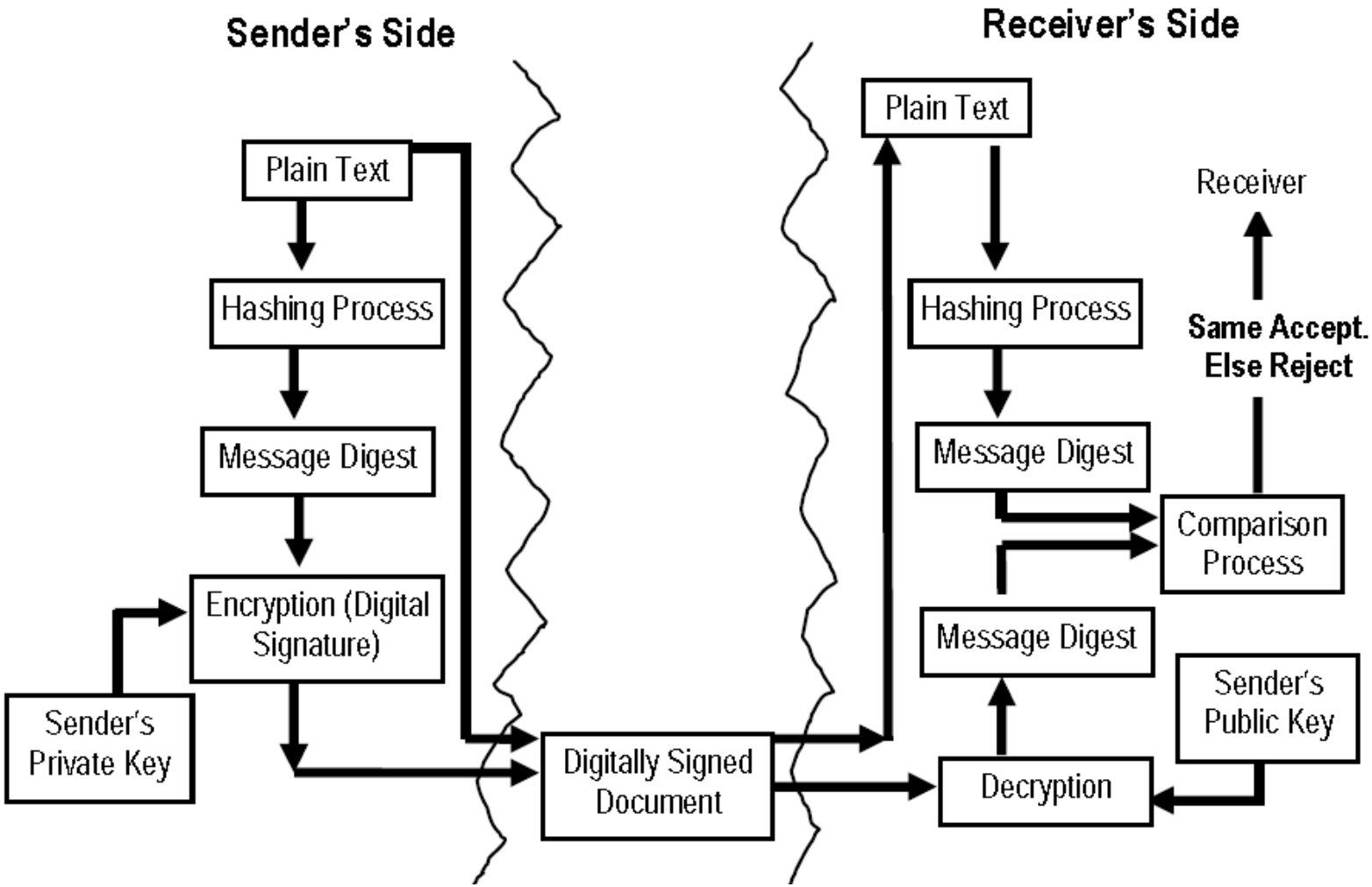
How does PKI work?



General PKI Requirements



Digital Signatures



Working of the Digital Signature by Using Hashing