SOLUTIONS MANUAL

COMPUTER SECURITY
THIRD EDITION

CHAPTERS 13–24

WILLIAM STALLINGS
LAWRIE BROWN

NOTICE

This manual contains solutions to the review questions and homework problems in *Computer Security, Third Edition*. If you spot an error in a solution or in the wording of a problem, I would greatly appreciate it if you would forward the information via email to wllmst@me.net. An errata sheet for this manual, if needed, is available at http://www.box.net/shared/ds8lygu0tjljokf98k85 . File name is S-CompSec2e-mmyy.

TABLE OF CONTENTS

CHAPTER 13 TRUSTED COMPUTING AND MULTILEVEL SECURITY

ANSWERS TO QUESTIONS

13.1 In most security models, each subject and each object is assigned a **security class**. In the simplest formulation, security classes form a strict hierarchy and are referred to as **security levels.** A subject is said to have a **security clearance** of a given level; an object is said to have a **security classification** of a given level.

13.2 **no read up:** A subject can only read an object of less or equal security level. This is referred to in the literature as the simple security property (ss-property).
no write down: A subject can only write into an object of greater or equal security level. This is referred to in the literature as the *-property.
ds-property: An individual (or role) may grant to another individual (or role) access to a document based on the owner's discretion, constrained by the MAC rules. Thus, a subject can exercise only accesses for which it has the necessary authorization and which satisfy the MAC rules.

13.3 The ds-property.

13.4 The BLP model deals with confidentiality and is concerned with unauthorized disclosure of information. The Biba models deals with integrity and is concerned with the unauthorized modification of data.

13.5 **Simple integrity:** A subject can modify an object only if the integrity level of the subject dominates the integrity level of the object: $I(S) \geq I(O)$.
Integrity confinement: A subject can read on object only if the integrity level of the subject is dominated by the integrity level of the object: $I(S) \leq I(O)$.
Invocation property: A subject can invoke another subject only if the integrity level of the first subject dominates the integrity level of the second subject: $I(S1) \geq I(S2)$.

13.6 **Certification rules** are security policy restrictions on the behavior of Integrity Verification Procedures and Transformation Procedures. **Enforcement rules** are built-in system security mechanisms that achieve the objectives of the certification rules.

13.7 The Chinese wall is a logical barrier that prevents a subject that accesses data from one side of the wall from accessing data on the other side.

13.8 **No read up:** A subject can only read an object of less or equal security level. **No write down:** A subject can only write into an object of greater or equal security level.

13.9 **Complete mediation:** The security rules are enforced on every access, not just, for example, when a file is opened. **Isolation:** The reference monitor and database are protected from unauthorized modification. **Verifiability:** The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation.

13.10 Roles can be defined by type of access and clearance level.

13.11 **Entire database:** This simple approach is easily accomplished on an MLS platform. An entire database, such as a financial or personnel database, could be classified as confidential or restricted and maintained on a server with other files.

Individual tables (relations): For some applications, it is appropriate to assign classification at the table level. In the example of Figure 13.10a, two levels of classification are defined: unrestricted (U) and restricted (R). The Employee table contains sensitive salary information and is classified restricted, while the Department table is unrestricted. This level of granularity is relatively easy to implement and enforce.

Individual columns (attributes): A security administrator may choose to determine classification on the basis of attributes, so that selected columns are classified. In the example of Figure 13.10b, the administrator determines that salary information and the identity of department managers is restricted information.

Individual rows (tuples): In other circumstances, it may make sense to assign classification levels on the basis of individual rows that match certain properties. In the example of Figure 13.10c, all rows in the Department table that contain information relating to the Accounts Department (Dept. ID = 4), and all rows in the Employee Table for which the Salary is greater than 50K are restricted.

Individual elements: The most difficult scheme to implement and manage is one in which individual elements may be selectively classified. In the example of Figure 13.10d, salary information and the identity of the manager of the Accounts Department are restricted.

13.12 In a database, insert a new row at the lower level without modifying the existing row at the higher level. This is known as **polyinstantiation**. This avoids the inference and data integrity problems but creates a database with conflicting entries

13.13 **Authenticated boot service:** The authenticated boot service is responsible for booting the entire operating system in stages and assuring that each portion of the OS, as it is loaded, is a version that is approved for use.
Certification service: Once a configuration is achieved and logged by the TPM, the TPM can certify the configuration to other parties. The TPM can produce a digital certificate by signing a formatted description of the configuration information using the TPM's private key. Thus, another user, either a local user or a remote system, can have confidence that an unaltered configuration is in use.
Encryption service: The encryption service enables the encryption of data in such a way that the data can be decrypted only by a certain machine and only if that machine is in a certain configuration.

13.14 The aim of these standards is to provide greater confidence in the security of IT products as a result of formal actions taken during the process of developing, evaluating, and operating these products.

13.15 One of the security assurance requirements is that security functionality is not compromised during product delivery. Thus, security functionality is one of the concerns of security assurance.

13.16 •Sponsor: Usually either the customer or the vendor of a product for which evaluation is required. Sponsors determine the security target that the product has to satisfy.
•Developer: Has to provide suitable evidence on the processes used to design, implement, and test the product to enable its evaluation.
•Evaluator: Performs the technical evaluation work, using the evidence supplied by the developers, and additional testing of the product, to confirm that it satisfies the functional and assurance requirements specified in the security target. In many countries, the task of evaluating products against a trusted computing standard is delegated to one or more endorsed commercial suppliers.
•Certifier: The government agency that monitors the evaluation process and subsequently certifies that a product as been

successfully evaluated. Cookies generally manage a register of evaluated products, which can be consulted by customers.

13.17 **1.** Preparation: Involves the initial contact between the sponsor and developers of a product, and the evaluators who will assess it. It will confirm that the sponsor and developers are adequately prepared to conduct the evaluation and will include a review of the security target and possibly other evaluation deliverables. It concludes with a list of evaluation deliverables and acceptance of the overall project costing and schedule.
2. Conduct of evaluation: A structured and formal process in which the evaluators conduct a series of activities specified by the CC. These include reviewing the deliverables provided by the sponsor and developers, and other tests of the product, to confirm it satisfies the security target. During this process, problems may be identified in the product, which are reported back to the developers for correction.
3. Conclusion: The evaluators provide the final evaluation technical report to the certifiers for acceptance. The certifiers use this report, which may contain confidential information, to validate the evaluation process and to prepare a public certification report. The certification report is then listed on the relevant register of evaluated products.

ANSWERS TO PROBLEMS

13.1 The purpose of the "no write down" rule, or *-property is to address the problem of Trojan horse software. With the *-property, information cannot be compromised through the use of a Trojan horse. Under this property, a program operating on behalf of one user cannot be used to pass information to any user having a lower or disjoint access class.

13.2 An append function only requires the ability to update the object without observing (reading) the object. The write function requires the ability to read as well.

13.3 **a.** The set b defines the current accesses. As long as these accesses satisfy the model properties, security is enforced. That is all that is strictly required.
b. The current accesses are determined in part by the permissions defined in the access matrix M. It would be difficult to properly implement the security policy without enforcing the restrictions on M.

13.4 Figure 13.2a: Rule 7 (create object), used by both Dirk and Carla.
Figure 13.2b: Dirk reads f2 (Rule 1). Dirk creates file (Rule 7).
Figure 13.2.c: Dirk creates file (Rule 7)
Figure 13.2d: Dirk downgrades a classification. This is done by a security administrator, outside the scope of the rules.
Figure 13.2e: Carla creates a file (Rule 7) and writes to the file (Rule 1).

13.5 They reflect the role ability to read down and write up.

13.6 a. *allow* (s, *repository, browse*(s)) iff label (s) ≥ class (repository)
allow (s, *repository, insert*(s)) iff label (s) ≤ class (repository)

b. In the initial state, subjects cannot browse information unless their label is MAX which is equal to class (repository) and hence no read up (NRU) is satisfied (first condition of 13.6a). Also, in the initial state, all subjects can insert information but since class (repository) is MAX, subject labels will always be less than or equal to the repository label and hence no write down (NWD) is satisfied (second condition of 13.6b).
Assuming NRU and NWD are met in the current state, it is trivial to argue that neither *browse* nor *insert* will cause the label of any subject or the label of the repository to change. As a result the NRU and NWD rules must be satisfied in any state that results from either of these actions occurring from a reachable state.

13.7 a. For all s ∈ *subjects;*
allow (s, repository, browse(s)) iff label (s) ≤ class (repository)
allow (s, repository, insert(s)) iff label (s) ≥ class (repository)

b. The argument is similar to 13.6b. The first condition of 13.7a corresponds to no read down and the second condition of 13.7a corresponds to no write up.

13.8 **a.** Rules C1, C2, E1 **b.** Rules E2, C3 **c.** Rule E3
d. Rule C4 **e.** Rule C5 **f.** Rule E4

13.9 Drake is not authorized to read the string directly, so the no-read-up rule will prevent this. Similarly, Drake is not authorized to assign a security level of sensitive to the back-pocket file, so that is prevented as well.

13.10 Suppose the role is for top secret users. The user has the potential to read some objects at the top secret level (rts) but could then write them down to the secret level (ws), violating the *-property.
Suppose the role is for secret users. Then the rts access capability violates the simple security property.

13.11 **1.** Notify the user that a row with that primary key already exists and reject the insertion.
2. Replace the existing row at the lower level with the new row being inserted at the high level.
3. Insert the new row at the high level without modifying the existing row at the lower level (i.e., polyinstantiate the entity).

13.12 Few products are evaluated against the higher EAL 6 and EAL 7 Common Criteria assurance levels because the evaluation requirements of these levels require either semiformal or formal verification that the implementation conforms to a formal model of the security design requirements. The need to develop such a formal model and to prove implementation compliance seriously limits the type and complexity of products that can be so evaluated. Such products general only perform extremely limited functions (such as an optical keyboard/mouse/monitor switch, or a data diode to allow one-way data flow from a lower to higher classified network). Given the stringent model, design and verification requirements, it is unlikely that a general-purpose operating system, or database management system, could be evaluated to these levels.

CHAPTER 14 IT SECURITY MANAGEMENT AND RISK ASSESSMENT

ANSWERS TO QUESTIONS

14.1 IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include: determining organizational IT security objectives, strategies and policies; determining organizational IT security requirements; identifying and analyzing security threats to IT assets within the organization; identifying and analyzing risks; specifying appropriate safeguards; monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization; developing and implementing a security awareness program; detecting and reacting to incidents.

14.2 The three fundamental questions IT security management tries to address are:

1. What assets do we need to protect?
2. How are those assets threatened?
3. What can we do to counter those threats?

14.3 IT security management consists of a process that starts by first determining a clear view of an organization's IT security objectives and general risk profile. Next an IT security risk assessment is needed for each asset in the organization that requires protection to answer the three key questions The process continues by selecting suitable controls, and then writing plans and procedures to ensure these necessary controls are effectively implemented. That implementation needs to be monitored, to determine if the security objectives are met. The whole process must be iterated, and the plans and procedures kept up-to-date, because of the rapid rate of change in both the technology and the risk environment.

14.4 Key national and international standards that provide guidance on IT security management and risk assessment include: the ISO27000 series including ISO27001, ISO27002 (previously ISO17799), & ISO27005; ISO31000; ISO13335; NIST Special Publications including SP800-30 & SP800-53.

14.5 The four steps in the iterative security management process are to:
Plan – to establish security policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do – is to implement and operate the security policy, controls, processes and procedures.
Check – is to assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review**.**
Act – to take corrective and preventive actions, based on the results of the internal security audit and management review or other relevant information, to achieve continual improvement of the security management process.

14.6 Organizational security objectives identify what IT security outcomes are desired. Some questions that help clarify these issues are:

- What key aspects of the organization require IT support in order to function efficiently?
- What tasks can only be performed with IT support?
- Which essential decisions depend on the accuracy, currency, integrity or availability of data managed by the IT systems?
- What data created, managed, processed and stored by the IT systems needs protection?
- What are the consequences to the organization of a security failure in their IT systems?

14.7 The four approaches to identifying and mitigating IT risks are the:

- **baseline** approach, which implements a basic general level of security controls on systems using baseline documents, codes of practice, and "industry best practice".
- **informal** approach, which involves conducting some form of informal, pragmatic risk analysis for the organization's IT systems.
- **detailed risk analysis** process, which involves a detailed risk assessment of the organization's IT systems, using a formal structured process, providing the greatest degree of assurance that all significant risks are identified and their implications considered.
- **combined** approach, which combines elements of the baseline, informal, and detailed risk analysis approaches.

14.8 ISO13335 suggest that for most organizations, in most circumstances, the combined approach for identifying and mitigating IT risks is the most cost effective.

14.9 The steps in the detailed security risk analysis process include:

1. Prepare for assessment
2. Conduct risk analysis (which includes Identify threat sources and events, Identify vulnerabilities and predisposing conditions, Determine likelihood of occurrence, Determine magnitude of impact, Determine risk)
3. Communicate results
4. Maintain assessment

14.10 Possible definitions are:

Asset: A system resource or capability of value to its owner that requires protection.

Control: Management, operational and technical processes and procedures that act to reduce the exposure of the organization to some risks.

Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.

Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.

Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

14.11 Key information on determining what are key assets requires the expertise of people in the relevant areas of the organization. In contrast, identifying possible threats and threat sources requires the use of a variety of sources, along with the experience of the risk analyst. The risk analyst takes the descriptive asset and threat/vulnerability details, and in the light of the organizations overall risk environment and existing controls, decides the appropriate likelihood rating. The determination of the consequence, should any asset be compromised, relies upon the judgment of the asset's owners, and the organization's management, rather than the opinion of the risk analyst.

14.12 Two key questions which help identify threats and risks for an asset are: 1 - Who or what could cause it harm? and 2 - How could this occur? Answering the first of these questions involves identifying

potential threats to assets, which can be natural or man-made, accidental or deliberate. Answering the second of these questions involves identifying flaws or weaknesses in the organization's IT systems or processes, which could be exploited by a threat source to cause harm.

14.13 **consequence**: indicates the impact on the organization should some particular threat actually eventuate.
likelihood: the probability that an identified threat could occur and cause harm to some asset.

14.14 The simple equation for determining risk is:

$$\text{Risk} = \text{Probability that threat occurs} \times \text{Cost to organization}$$

It is not commonly used in practice because it is often extremely hard to determine accurate probabilities, realistic cost consequences, or both. Hence most risk analyses use qualitative, rather than quantitative, ratings for both these items.

14.15 The items typically specified in the risk register for each asset/threat identified are: Asset, Threat/Vulnerability, Existing Controls, Likelihood, Consequence, Level of Risk, and Risk Priority

14.16 Five alternatives for managing identified risks are:

- **risk acceptance**: choosing to accept a risk level greater than normal for business reasons, typically due to excessive cost or time needed to treat the risk. Management must then accept responsibility for the consequences to the organization should the risk eventuate.
- **risk avoidance**: not proceeding with the activity or system that creates this risk. This usually results in loss of convenience or ability to perform some function that is useful to the organization. The loss of this capability is traded off against the reduced risk profile.
- **risk transferal**: sharing responsibility for the risk with a third-party. This is typically achieved by taking out insurance against the risk occurring, by entering into a contract with another organization, or by using partnership or joint venture structures to share the risks and costs should it eventuate.
- **reduce consequence**: by modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur. This could be achieved by implementing controls to enable the organization to quickly recover should the risk occur.
- **reduce likelihood**: by implementing suitable controls to lower the chance of the vulnerability being exploited. These could include technical or administrative controls that aim to improve the security

of the asset, making it harder for an attack to succeed by reducing the vulnerability of the asset.

ANSWERS TO PROBLEMS

14.1 There is no simple answer to this problem, as it depends on the relevant organization's IT Security Policy. However any answer should consider all the topics listed in section 14.2, and should explicitly refer to any relevant privacy or corporate governance legislation.

14.2 Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
integrity of /customer and financial data files on desktop systems	corruption of these files due to import of a worm/virus onto system	anti-virus program	Almost Certain	Major	Extreme

Given limited IT support, it is likely that the systems and A/V programs are not current, hence given the high rate of worm/virus incidents, infection is almost certain. Similarly, it is likely that such an organization does not regularly backup their data, hence such an infection could cause loss of critical customer/financial data, with serious impact on the organizations functions. Clearly changing these assumptions will change the ratings.

14.3 Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
integrity of the accounting records on the server	financial fraud by employee, disguised by altering the accounting records	monthly account audit	Possible	Moderate	High

The chance of insider fraud can be very hard to predict, but is clearly possible. Depending on how long it takes for the fraud to be identified, there could be significant impact on the organizations finances. Assuming there is a regular monthly audit check of the firm's cashflow,

it is likely the fraud will be detected relatively quickly, which suggests a moderate consequence rating. Again changing these assumptions will change the ratings.

14.4 Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
integrity of the organizatio n's web server	hacking and defacement of the web server	-	Possible	Minor	Medium

Assuming that their website uses common CGI programs such as guestbook or blog software, then given the rate of remotely exploitable bugs found in such program, exploit is possible (and is very dependent on both how carefully their IT support tracks reports of such bugs and patches when found, and bad luck in being identified and targeted by an attacker). However whilst defacement of their site may well cause embarrassment and adverse publicity, it ought not affect the actual production work. It is also fairly easy to correct. Hence assume a minor consequence. Changing these assumptions will change the ratings.

14.5 Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
confidentiality of techniques used to conduct penetration tests on customers, and the results of conducting such tests for clients, which are stored on the server	theft/breach of this confidential and sensitive information by either an external or internal source	risk assessed, hardened O/S, automated patching, IDS	Unlikely	Catastrophic	Extreme

Given that the main file server belongs to an IT security consultancy firm it is reasonable to assume that it is managed according to current best practice, having undergone a risk assessment, and using a hardened O/S with automated patching and an IDS. Nonetheless, given that zero-day exploits continue to be found, successful external exploit is conceivable, if unlikely. As noted in the answer to problem 14.3, insider attack is also conceivable, if very hard to predict. Should this attack occur, the damage to the firm is likely to be serious, as it attacks

the core of their reputation and intellectual property. Hence assume a catastrophic consequence. Changing these assumptions will change the ratings.

14.6 Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
confidentiality of personnel information in a copy of a database stored unencrypted on the laptop	theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop	insurance	Possible	Major	Extreme

Given the very high report rate of laptop theft (e.g. the 2006 CSI/FBI survey shows 47% of respondents suffered from this), if the data stored on the laptop is not encrypted (as is still common), then the chances of it being accessed and used in identity theft is possible – depending on the motivations and skills of the thief. Hence assume a rating of possible for this specific threat. A number of large government departments and agencies have been embarrassed, and suffered significant financial penalties, as a result of such a theft in recent years. Hence assume a consequence of major. Changing these assumptions will change the ratings.

14.7 Some threats that a small public service agency is exposed to can include: [NIST12] Table D-2 lists possible threat sources grouped as Adversarial (Individual, Group, Organization, Nation-State), Accidental, Structural (IT Equipment, Controls, Software), and Environmental (Natural Or Man-Made Disaster, Unusual Natural Event, Infrastructure Failure/Outage). Also many of the threats listed [HB231] Appendix A are applicable.

14.8 NIST SP 800-30 (2002) Tables 3-4 to 3-7 use a 3 level scale of high/medium/low for each of likelihood, consequence and risk, while our Tables 14.2 to 14.4 use 5, 6, and 4 levels respectively. This means that assessments using our ratings can use a finer level of granularity, and potentially better separate different asset/threat items, than assessments done using the NIST tables. However having a greater number of levels means that it can be harder to determine the most appropriate rating (although some small changes do not alter the final resultant risk level). The recent version of this standard [NIST12] now proposes 5 level tables, likely to provide a finer level of granularity.

CHAPTER 15 IT SECURITY CONTROLS, PLANS, AND PROCEDURES

ANSWERS TO QUESTIONS

15.1 **Security controls** or **safeguards** are practices, procedures or mechanisms that may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, or detect unwanted incidents and facilitate recovery.

15.2 The three broad classes of controls are:

- **management control:** focus on security policies, planning, guidelines and standards which then influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission.
- **operational control:** address the correct implementation and use of security policies and standards, ensuring consistency in security operations, and correcting identified operational deficiencies.
- **technical controls:** involve the correct use of hardware and software security capabilities in systems.

In turn, each of these control classes may include:

- **supportive controls:** pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by many other controls.
- **preventative controls:** focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability.
- **detection and recovery controls:** focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability, and by providing means to restore the resulting lost computing resources.

15.3 To list a specific example of each of three broad classes of controls from those given in Table 15.3, first use Table 15.1 which classifies the control families into the relevant class, then select any suitable entry from a suitable control family in Table 15.3 for each. If further details are wanted, consult [NIST09] for detailed information on each item.

15.4 The steps we discuss for selecting and implementing controls are shown in Figure 15.1:

1. Prioritize risks (management review of risk register)
2. Respond to risks (determine risk response, evaluate recommended control options, select controls, develop implementation plan and implement selected controls)
3. Monitor risks

15.5 Implementing a new or enhanced control can reduce the residual level of risk as a result of the reduction in threat likelihood from either reducing vulnerabilities/flaws/weaknesses in the system, or by reducing the capability and motivation of the threat source; or from a reduction in consequence by reducing the magnitude of the adverse impact of the threat occurring on the organization.

15.6 The items that should be included in an IT Security Implementation Plan include: risks (asset/threat/vulnerability combinations); recommended controls (from the risk assessment); action priority for each risk; selected controls (on the basis of the cost-benefit analysis); required resources for implementing the selected controls; responsible personnel; target start and end dates for implementation; maintenance requirements and other comments.

15.7 The elements that form the "Implementation of Controls" phase of IT security management include:

- implementation of the security plan (where the identified personnel undertake the tasks needed to implement the new or enhanced controls).
- security training (of the personnel responsible for the development, operation and administration of the system being installed or enhanced)
- security awareness (training for all personnel in an organization to assist it in meeting the security objectives).

15.8 The organizational security officer checks that

- The implementation costs and resources used stay within identified bounds.
- The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved.
- The controls are operated and administered as needed.

15.9 The elements that form the "Implementation Follow-up" phase of IT security management are:

- maintenance of security controls (to ensure their continued correct functioning and appropriateness)

- security compliance checking (an audit process to review the organization's security processes to verify compliance with the security plan)
- change and configuration management (the process used to review proposed changes to systems for implications of both security related and wider operational aspects, on the organization's systems and use)
- incident handling (procedures used to respond to a security incident).

15.10 Because changes can affect security, the general process of change and configuration management overlaps IT security management and must interact with it.

ANSWERS TO PROBLEMS

15.1 To manage the risk to "integrity of customer and financial data files on system" from "corruption of these files due to import of a worm/virus onto system (exercise 14.2), some suitable specific controls from Table 15.3 could include: Security Awareness training, Access Restrictions for Change, Periodic and Timely Systems Maintenance, Malicious Code Protection, Intrusion Detection Tools and Techniques, Spam and Spyware Protection. The most cost-effective controls are likely to include Malicious Code Protection and Spam and Spyware Protection to identify and block infections, along with Periodic and Timely Systems Maintenance to keep the system patched.

15.2 To manage the risk to "integrity of the accounting records on the server" from "financial fraud by an employee, disguised by altering the accounting records " (exercise 14.3), some suitable specific controls from Table 15.3 could include: Separation of Duties, Access Control Supervision and Review, Audit Monitoring, Analysis, and Reporting, Audit Reduction and Report Generation, User Identification and Authentication, Personnel Screening. The most cost-effective controls are likely to include Separation of Duties to ensure that significant financial transactions must be authorized by multiple staff, along with Access Control Supervision and Review to help detect fraud should it occur.

15.3 To manage the risk to "integrity of the organization's web server" from "hacking and defacement of the web server" (exercise 14.4), some suitable specific controls from Table 15.3 could include: Access Restrictions for Change, Periodic and Timely Systems Maintenance, Flaw Remediation, Incident Handling, Vulnerability Scanning, Intrusion Detection Tools and Techniques, Security Alerts and Advisories. The

most cost-effective controls are likely to include Periodic and Timely Systems Maintenance and Flaw Remediation to try and reduce the likelihood of the web server running buggy software, along with good Incident Handling processes to react and correct the system should the threat occur.

15.4 To manage the risk to "confidentiality of techniques for conducting penetration tests on customers, and the results of these tests, which are stored on the server" from "theft/breach of this confidential and sensitive information" (exercise 14.5), some suitable specific controls from Table 15.3 could include: Account Management, Access Enforcement, Separation of Duties, Least Privilege, Audit Monitoring, Analysis, and Reporting, Audit Reduction and Report Generation, User Identification and Authentication, Periodic and Timely Systems Maintenance, Flaw Remediation, Personnel Screening, Personnel Sanctions, Intrusion Detection Tools and Techniques. Given the seriousness of the consequences, controls should focus on reducing the likelihood of this threat occurring, hence the most cost-effective controls are likely to include Personnel Screening, Personnel Sanctions, User Identification and Authentication, Access Enforcement, and Separation of Duties to help manage insider threats; and Periodic and Timely Systems Maintenance, Flaw Remediation, and Intrusion Detection Tools and Techniques to help manage external threats.

15.5 To manage the risk to "confidentiality of personnel information in a copy of a database stored unencrypted on the laptop" from "theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop" (exercise 14.6), some suitable specific controls from Table 15.3 could include: Access Control for Portable and Mobile Systems, Security Awareness Training, Physical Access Control, Personnel Sanctions, Use of Validated Cryptography. The most cost-effective controls are likely to include the Use of Validated Cryptography and Access Control for Portable and Mobile Systems to ensure any sensitive information is encrypted and hence cannot be accessed as a result of the theft, along with Security Awareness Training and Personnel Sanctions to help limit the transfer of sensitive information to such devices, and to adjust behavior to reduce the chance of such thefts occurring.

15.6 In managing the risks identified in the assessment of a small public service agency (exercise 14.7), clearly a very wide range of controls are applicable. Depending on assumptions made and the current environment, what are considered the most critical risks can vary considerably. However these would likely include the common natural environmental threats (fire, flood, failure of power/water/air conditioning). Against these, suitable contingency planning and

physical and environmental protection controls should be chosen. Critical risks would also include those due to accidental insider actions such as operational errors, and the input of invalid information. Against these controls from the awareness and training and audit and accountability sections should be chosen. In the case of deliberate insider threats (fraud, sale of information etc), audit and accountability and personnel controls could be used. Lastly for external attacks, controls relating to access controls, configuration management, contingency planning and incident response can be used.

CHAPTER 16 PHYSICAL AND INFRASTRUCTURE SECURITY

ANSWERS TO QUESTIONS

16.1 (1) Room temperature too hot or too cold for equipment. (2) Internal equipment temperature too hot. (3) Humidity too high or too low.

16.2 The direct threat is the damage caused by the fire itself. The indirect threats are from heat, release of toxic fumes, water damage from fire suppression, and smoke damage.

16.3 Undervoltage, overvoltage, and noise.

16.4 Dealing with this problem is primarily a matter of having environmental-control equipment of appropriate capacity and appropriate sensors to warn of thresholds being exceeded. Beyond that, the principal requirement is the maintenance of a power supply.

16.5
1. Choice of site to minimize likelihood of disaster. Few disastrous fires originate in a well-protected computer room or IS facility. The IS area should be chosen to minimize fire, water, and smoke hazards from adjoining areas. Common walls with other activities should have at least a one-hour fire-protection rating.
2. Air conditioning and other ducts designed so as not to spread fire. There are standard guidelines and specifications for such designs.
3. Positioning of equipment to minimize damage.
4. Good housekeeping. Records and flammables must not be stored in the IS area. Tidy installation if IS equipment is crucial.
5. Hand-operated fire extinguishers readily available, clearly marked, and regularly tested.
6. Automatic fire extinguishers installed. Installation should be such that the extinguishers are unlikely to cause damage to equipment or danger to personnel.
7. Fire detectors. The detectors sound alarms inside the IS room and with external authorities, and start automatic fire extinguishers after a delay to permit human intervention.

8. Equipment power-off switch. This switch must be clearly marked and unobstructed. All personnel must be familiar with power-off procedures.
9. Emergency procedures posted.
10. Personnel safety. Safety must be considered in designing the building layout and emergency procedures.
11. Important records stored in fireproof cabinets or vaults.
12. Records needed for file reconstruction stored off the premises.
13. Up-to-date duplicate of all programs stored off the premises.
14. Contingency plan for use of equipment elsewhere should the computers be destroyed.
15. Insurance company and local fire department should inspect the facility.

16.6 Prevention and mitigation measures for water threats must encompass the range of such threats. For plumbing leaks, the cost of relocating threatening lines is generally difficult to justify. With knowledge of the exact layout of water supply lines, measures can be taken to locate equipment sensibly. The location of all shutoff valves should be clearly visible or at least clearly documented, and responsible personnel should know the procedures to follow in case of emergency. To deal with both plumbing leaks and other sources of water, sensors are vital. Water sensors should be located on the floor of computer rooms, as well as under raised floors, and should cut off power automatically in the event of a flood.

16.7 To deal with brief power interruptions, an uninterruptible power supply (UPS) should be employed for each piece of critical equipment. The UPS is a battery backup unit that can maintain power to processors, monitors, and other equipment for a period of minutes. UPS units can also function as surge protectors, power noise filters, and automatic shutdown devices when the battery runs low. For longer blackouts or brownouts, critical equipment should be connected to an emergency power source, such as a generator. For reliable service, a range of issues need to be addressed by management, including product selection, generator placement, personnel training, testing and maintenance schedules, and so forth.

ANSWERS TO PROBLEMS

16.1 The World Bank checklist specifically mentions the following items not covered by the Security Policy: biometric and smart card access control techniques; checking audit trails; storage of backup data securely; unused ports turned off; use of surveillance cameras; fire suppression equipment; humidity controls; ceiling reinforcement. The

Security Policy is general but goes into more detail than the checklist on procedures and general areas of concern. It is interesting to note that in fact there are quite a few areas covered in each document that are not covered in the other. Both are meant as guidelines but clearly neither is exhaustive.

16.2 The chapter generally covers all of the areas mentioned in the two documents.

16.3 The Security Policy covers in general terms the areas that are covered in more detail in Sections 16.1 through 16.3 of this chapter. It does not cover the material in Sections 16.4, 16.5, and 16.7. The scope of this chapter is broader.

16.4 There is no unique set of answers to this question. The following is from [FORR06].

	IT Security	Physical Security
Boundary type (what constitutes the perimeter)	Complex boundaries that combine hardware, software and networks (VPN, Web browsing, database, wireless)	Discrete, well-defined boundaries (vaults, building walls, containers)
Standards	Customers demand interoperability; equal mix of standards-based and proprietary systems	Some infrastructure uses commodity parts, but systems are generally proprietary and not interoperable
Maturity	Rapid evolution of products	Industry has 100-plus years of processes and response system; longer product cycles
Frequency of attacks	High: attacks often scale quickly, with active communities discussing well-known attacks	Low: attacks tend to be localized and repeated less often
Attack responses (types of responses)	Effective patch management and update mechanisms	Security fixes and firmware updates applied in nonuniform fashion
Risk to attackers	Few: hard to trace sophisticated attacks	High: adversary risks physical arrest/capture
Evidence of compromise	Varies, hard to tell if data were copied	Stolen items are noticed missing.

CHAPTER 17 HUMAN RESOURCES SECURITY

ANSWERS TO QUESTIONS

17.1 • Improving employee behavior
• Increasing the ability to hold employees accountable for their actions
• Mitigating liability of the organization for an employee's behavior
• Complying with regulations and contractual obligations

17.2 In general, a **security awareness** program seeks to inform and focus an employee's attention on issues related to security within the organization. A **security training** program is designed to teach people the skills to perform their IS-related tasks more securely.

17.3 An organizational security policy is a formal statement of the rules by which people that are given access to an organization's technology and information assets must abide.

17.4 • Site security administrator
• Information technology technical staff (e.g., staff from computing center)
• Supervisors of large user groups within the organization (e.g., business divisions, computer science department within a university, etc.)
• Security incident response team
• Representatives of the user groups affected by the security policy
• Responsible management
• Legal counsel (if appropriate)

17.5 ISO 27002 is a comprehensive set of controls comprising best practices in information security. It is essentially an internationally recognized generic information security standard.

17.6 • Least privilege: Give each person the minimum access necessary to do his or her job. This restricted access is both logical (access to accounts, networks, programs) and physical (access to computers, backup tapes, and other peripherals). If every user has accounts on

every system and has physical access to everything, then all users are roughly equivalent in their level of threat.

• Separation of duties: Carefully separate duties so that people involved in checking for inappropriate use are not also capable of making such inappropriate use. Thus, having all the security functions and audit responsibilities reside in the same person is dangerous. This practice can lead to a case in which the person may violate security policy and commit prohibited acts, yet in which no other person sees the audit trail to be alerted to the problem.

• Limited reliance on key employees: No one in an organization should be irreplaceable. If your organization depends on the ongoing performance of a key employee, then your organization is at risk. Organizations cannot help but have key employees. To be secure, organizations should have written policies and plans established for unexpected illness or departure. As with systems, redundancy should be built into the employee structure. There should be no single employee with unique knowledge or skills.

17.7

1. Significant employee work time may be consumed in non-work-related activities, such as surfing the Web, playing games on the Web, shopping on the Web, chatting on the Web, and sending and reading personal e-mail.
2. Significant computer and communications resources may be consumed by such non-work-related activity, compromising the mission that the IS resources are designed to support.
3. Excessive and casual use of the Internet and e-mail unnecessarily increases the risk of introduction of malicious software into the organization's IS environment.
4. The non-work-related employee activity could result in harm to other organizations or individuals outside the organization, thus creating a liability for the organization.
5. E-mail and the Internet may be used as tools of harassment by one employee against another.
6. Inappropriate online conduct by an employee may damage the reputation of the organization.

17.8 The benefits of developing an incident response capability include: responding to incidents systematically so that the appropriate steps are taken; helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information, and disruption of services; using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data; and dealing properly with legal issues that may arise during incidents.

17.9 The broad categories of security incidents include various forms of unauthorized access to a system, and various forms of unauthorized modification of information on the system.

17.10 Some types of tools used to detect and respond to incidents are: system integrity verification tools, log analysis tools, network and host intrusion detection systems, and intrusion prevention systems.

17.11 Following the immediate response to an incident, there is a need to identify what vulnerability led to its occurrence, and how this might be addressed to prevent it occurring in future. Details of the incident, and the response taken are recorded for future reference. The impact on the organization's systems, and their risk profile must also be reconsidered as a result of the incident.

ANSWERS TO PROBLEMS

17.1 Awareness deals with what the security threats are. Training deals with how to counter those threats.

17.2 **a.** Taking pictures of or in the worksite should be forbidden in the policy. [often overlooked these days]. The janitor should be fired. If the policy did not include this, fire the janitor for goofing off.
b. Rewrite the policy to state that taking pictures is forbidden at the worksite.

17.3 Any jpgs can be modified to include hidden messages. Security should run a debugger or disassembler to find out if this is so. Screensaver pictures are actually no longer necessary so dump them totally. Forbid the use of work computers to save or send pictures for that reason.

17.4 USB port drives should be addressed in the policy and forbidden on work grounds because people can use them to download unauthorized software, boot to an outside line in order to use a messenger service, or upload trojans, viruses, and bots into the system. additionally, security personnel should look into USB blocking. USB drive should be left with security until Lynsay goes home that day with clear instructions NOT to bring one to work.

17.5 Find out what the game is and where it originated (in this case it may be a freebie download from yahoo or a modified download from yahoo that was paid). Dump the game. Inform Harriet that games are not allowed. Write her up or fire her if the policy says no downloading of outside stuff. If not, add it to the policy and warn her.

17.6 All security administrators should check search engines on a regular basis for the words MyCompanySucks or My Company Sucks. The policy should also address blogs as they are becoming popular. All employees should sign agreement to notify company of any pre-existing blogs or future blogs and must agree not to discuss company stuff in a general or specific way in the blog. Security personnel should be reading the blogs of every employee who has one to ensure that the blogs are in line with confidentiality and security procedures. If the company has company blogs, only specific employees would be allowed to post to them and those posts must be preapproved. Phil must agree to remove the offending link, is not entitled to keep a blog during work time (even if it is during his breaks) on a work computer. Phil's willingness to link to a CompanySucks blog points to a larger problem of employee morale. Could be that he is either immature or resentful and he should be given an older man mentor (who is not his boss) to develop a relationship with to further his career growth, and maybe will be a role model to him also.

17.7 In the incident response policy for the small accounting firm (exercises 14.2 and 15.1), in response to the detection of an email worm infecting some of the company systems and producing large volumes of email spreading the propagation, if the indications are that the infection is seriously compromising the external network connections, and the risk of further infection is high, then disconnecting the firm's systems from the Internet to limit further spread is a reasonable policy. Whilst recognizing this will impact email/web communications and hence the firm's operations, it is still likely the better option than contributing to the further spread of the infection. The policy would most likely also recommend reporting the incident to the appropriate Computer Emergency Response Team (CERT), but not as a matter of urgency (if it is large enough, they will know about it). It would not recommend reporting it to law enforcement authorities, since its unlikely that legal action in response is possible.

17.8 In the incident response policy for the small legal firm (exercises 14.3 and 15.2), in response to the detection of significant financial fraud by an employee, initial actions should include isolating the suspected staff member from any access to the firm's systems, and arranging for a forensic copy to be made of all relevant data, especially audit records of actions taken on the system, in the event of future legal action. This incident should be reported to the relevant law enforcement authorities to allow them to respond and collect evidence needed. Ideally it should also be reported in general terms to the relevant Computer Emergency Response Team (CERT) to allow them to compile accurate statistics of computer crime incidents.

17.9 In the incident response policy for the web design company (exercises 14.4 and 15.3), in response to the detection of hacking and defacement of their web server, it would most likely NOT recommend disconnecting the system from the Internet to limit damaging publicity, but rather immediately restoring the defaced pages from backups, and initiating action to identify the vulnerability exploited to allow the attack, and taking immediate steps to block access to it (which may involve removing some functionality from the system pending further analysis and corrective action). This is more likely an appropriate response than complete disconnection, as the web site is needed to promote the company's operations. The policy would most likely also recommend immediately reporting the incident to the appropriate Computer Emergency Response Team (CERT), as they may be able to advise whether it is part of a larger coordinated attack, and perhaps supply additional information on countering it. It would not recommend reporting it to law enforcement authorities unless there is evidence identifying the attacker, since otherwise it is unlikely that legal action in response is possible.

17.10 In the incident response policy for the large government department (exercises 14.6 and 15.5), in response to the report of theft of a laptop containing a large number of sensitive personnel records, the policy will likely be bound by legal requirements which increasingly mandate contacting the personnel whose records have been stolen, and most likely requiring the government to provide monitoring of their credit records for some period. Assuming the department has policies concerning the circumstances under which sensitive information can be transferred to laptops, if these were not followed then the relevant sanctions should be imposed against the employee whose laptop was stolen. If the department does not have such policies, this lack should be highlighted as a consequence of the development of this policy, and management warned that serious adverse publicity and financial costs are possible should this risk occur. Legal requirements increasingly mandate that the incident should be reported to the relevant law enforcement authorities, and/or government security agency, to allow them to respond appropriately. Ideally it should also be reported in general terms to the relevant Computer Emergency Response Team (CERT) to allow them to compile accurate statistics of computer crime incidents.

CHAPTER 18 SECURITY AUDITING

ANSWERS TO QUESTIONS

18.1 An event discriminator is a logical module that detects security-relate event. Each such event triggers a **security audit message** to an audit recorder. Thus the message simply causes the detected event to be recorded. If the event requires some defensive action, the event discriminator sends a **security alarm** on this even to an alarm processor to trigger the action. Thus a security alarm results in an action.

18.2 • Event discriminator: The is logic embedded into the software of the system that monitors system activity and detects security-related events that it has been configured to detect.
• Audit recorder: For each detected event, the event discriminator transmits the information to an audit recorder. The model depicts this transmission as being in the form of a message. The audit could also be done by recording the event in a shared memory area.
• Alarm processor: Some of the events detected by the event discriminator are defined to be alarm events. For such events an alarm is issued to an alarm processor. The alarm processor takes some action based on the alarm. This action is itself an auditable event and so is transmitted to the audit recorder.
• Security audit trail: The audit recorder creates a formatted record of each event and stores it in the security audit trail.
• Audit analyzer: The security audit trail is available to the audit analyzer, which, based on a pattern of activity, may define a new auditable event that is sent to the audit recorder and may generate an alarm.
• Audit archiver: This is a software module that periodically extracts records from the audit trail to create a permanent archive of auditable events.
• Archives: The audit archives are a permanent store of security-related events on this system.
• Audit provider: The audit provider is an application and/or user interface to the audit trail.
• Audit trail examiner: The audit trail examiner is an application or user who examines the audit trail and the audit archives for historical trends, for computer forensic purposes, and for other analysis.

• Security reports: The audit trail examiner prepares human-readable security reports.

18.3 • Data generation: Identifies the level of auditing, enumerates the types of auditable events, and identifies the minimum set of audit-related information provided. This function must also deal with the conflict between security and privacy and specify for which events the identity of the user associated with an action is included in the data generated for an event.
• Event selection: Inclusion or exclusion of events from the auditable set. This allows the system to be configured at different levels of granularity to avoid the creation of an unwieldy audit trail.
• Event storage: Creation and maintenance of the secure audit trail. The storage function includes measures to provide availability and to prevent loss of data from the audit trail.
• Automatic response: Defines reactions taken following detection of events that are indicative of a potential security violation.
• Audit analysis: Provided via automated mechanisms to analyze system activity and audit data in search of security violations. This component identifies the set of auditable events whose occurrence or accumulated occurrence indicates a potential security violation. For such events, an analysis is done to determine if a security violation has occurred; this analysis uses anomaly detection and attack heuristics.
• Audit review: As available to authorized users to assist in audit data review. The audit review component may include a selectable review function that provides the ability to perform searches based on a single criterion or multiple criteria with logical (i.e. and/or) relations, sort audit data, and filter audit data before audit data are reviewed. Audit review may be restricted to authorized users.

18.4 • Introduction of objects within the security-related portion of the software into a subject's address space
• Deletion of objects
• Distribution or revocation of access rights or capabilities
• Changes to subject or object security attributes
• Policy checks performed by the security software as a result of a request by a subject
• The use of access rights to bypass a policy check
• Use of identification and authentication functions
• Security-related actions taken by an operator and/or authorized user (e.g., suppression of a protection mechanism)
• Import/export of data from/to removable media (e.g., printed output, tapes, disks)

18.5 **System-level audit trails:** captures data such as login attempts, both successful and unsuccessful, devices used, and OS functions performed
Application-level audit trails: may be used to detect security violations within an application or to detect flaws in the application's interaction with the system.
User-level audit trails: traces the activity of individual users over time.
Physical access audit trails: generated by equipment that controls physical access and then transmitted to a central host for subsequent storage and analysis.

18.6 • syslog(): An application program interface (API) referenced by several standard system utilities and available to application programs
• logger: A UNIX command used to add single-line entries to the system log
• /etc/syslog.conf: The configuration file used to control the logging and routing of system log events
• syslogd: The system daemon used to receive and route system log events from syslog() calls and logger commands.

18.7 This technique described provides for application-level auditing by creating new procedures that intercept calls to shared library functions in order to instrument the activity.

18.8 • Audit analysis: Provided via automated mechanisms to analyze system activity and audit data in search of security violations. This component identifies the set of auditable events whose occurrence or accumulated occurrence indicates a potential security violation. For such events, an analysis is done to determine if a security violation has occurred; this analysis uses anomaly detection and attack heuristics.
• Audit review: As available to authorized users to assist in audit data review. The audit review component may include a selectable review function that provides the ability to perform searches based on a single criterion or multiple criteria with logical (i.e. and/or) relations, sort audit data, and filter audit data before audit data are reviewed. Audit review may be restricted to authorized users.

18.9 SIEM software is a centralized logging software package similar to, but much more complex than, syslog. SIEM systems provide a centralized, uniform audit trail storage facility and a suite of audit data analysis programs.

ANSWERS TO PROBLEMS

18.1 a. The X.800 series is specifically concerned with networking and telecommunications, so you would expect a more network-based orientation than ISO 27002, which is focused on information and computer security. This is reflected in Tables 18.2 and 18.3. For example, X.816 refers to connection-related security events, and ISO 27002 does not.

b. An example of the ISO 27002 focus on computer security is the set of events related to privileged operations. X.816 has not comparable events.

18.2 a. X.816, with its orientation to the OSI model, refers to events related to the layers of that model in a way that Table 18.6 does not. The items in ISO 27002 are fairly well covered in Table 18.6.

b. Table 18.6 is a lengthier and more detailed list. As such, it provides perhaps more useful guidance in developing a specific list of events.

18.3 From SP-800-92: There are advantages and disadvantages to each method. The primary advantage of the agentless approach is that agents do not need to be installed, configured, and maintained on each logging host. The primary disadvantage is the lack of filtering and aggregation at the individual host level, which can cause significantly larger amounts of data to be transferred over networks and increase the amount of time it takes to filter and analyze the logs. Another potential disadvantage of the agentless method is that the SIEM server may need credentials for authenticating to each logging host. In some cases, only one of the two methods is feasible; for example, there might be no way to remotely collect logs from a particular host without installing an agent onto it.

CHAPTER 19 LEGAL AND ETHICAL ASPECTS

ANSWERS TO QUESTIONS

19.1 • Computers as targets: This form of crime targets a computer system, to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server. Using the terminology of Chapter 1, this form of crime involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability.
• Computers as storage devices: Computers can be used to further unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer can be used to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software).
• Computers as communications tools: Many of the crimes falling within this category are simply traditional crimes that are committed online. Examples include the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography.

19.2 • Real property: Land and things permanently attached to the land, such as trees, buildings, and stationary mobile homes.
• Personal property: Personal effects, moveable property and goods, such as cars, bank accounts, wages, securities, a small business, furniture, insurance policies, jewelry, patents, pets, and season baseball tickets.
• Intellectual property: Any intangible asset that consists of human knowledge and ideas. Examples include software, data, novels, sound recordings, the design of a new type of mousetrap, or a cure for a disease.

19.3 • Copyrights: Copyright law protects the tangible or fixed expression of an idea, not the idea itself.

• Trademarks: A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.
• Patents: A patent for an invention is the grant of a property right to the inventor.

19.4 (1) The proposed work is original. (2) The creator has put this original idea into a concrete form, such as hard copy (paper), software, or multimedia form.

19.5 • Reproduction right: Lets the owner make copies of a work
• Modification right: Also known as the derivative-works right, concerns modifying a work to create a new or derivative work
• Distribution right: Lets the owner publicly sell, rent, lease, or lend copies of the work.
• Public-performance right: Applies mainly to live performances
• Public-display right: Lets the owner publicly show a copy of the work directly or by means of a film, slide, or television image

19.6 The DMCA, signed into law in 1998, is designed to implement World Intellectual Property Organization (WIPO) treaties, signed in 1996. In essence, DMCA strengthens the protection of copyrighted materials in digital format.

19.7 Digital Rights Management (DRM) refers to systems and procedures that ensure that holders of digital rights are clearly identified and receive the stipulated payment for their works.

19.8 • Content provider: Holds the digital rights of the content and wants to protect these rights. Examples are a music record label and a movie studio.
• Distributor: Provides distribution channels, such as an online shop or a Web retailer. For example, an online distributor receives the digital content from the content provider and creates a Web catalog presenting the content and rights metadata for the content promotion.
• Consumer: Uses the system to access the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license. The player/viewer application used by the consumer takes charge of initiating license request to the clearinghouse and enforcing the content usage rights.
• Clearinghouse: Handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly. The clearinghouse is also responsible for logging license consumptions for every consumer.

19.9 • Notice: Organizations must notify individuals what personal information they are collecting, the uses of that information, and what choices the individual may have.
• Consent: Individuals must be able to choose whether and how their personal information is used by, or disclosed to, third parties. They have the right not to have any sensitive information collected or used without express permission, including race, religion, health, union membership, beliefs, and sex life.
• Consistency: Organizations may use personal information only in accordance with the terms of the notice given the data subject and any choices with respect to its use exercised by the subject.
• Access: Individuals must have the right and ability to access their information and correct, modify, or delete any portion of it.
• Security: Organizations must provide adequate security, using technical and other means, to protect the integrity and confidentiality of personal information.
• Onward transfer: Third parties receiving personal information must provide the same level of privacy protection as the organization from whom the information is obtained.
• Enforcement: The Directive grants a private right of action to data subjects when organizations do not follow the law. In addition, each EU member has a regulatory enforcement agency concerned with privacy rights enforcement.

19.10 The Common Criteria specification is primarily concerned with the privacy of an individual with respect to that individual's use of computer resources, rather than the privacy of personal information concerning that individual.

19.11
1. A code can serve two inspirational functions: as a positive stimulus for ethical conduct on the part of the professional, and to instill confidence in the customer or user of an IS product or service. However, a code that stops at just providing inspirational language is likely to be vague and open to an abundance of interpretations.
2. A code can be educational. It informs professionals about what should be their commitment to undertake a certain level of quality of work and their responsibility for the well being of users of their product and the public, to the extent the product may affect nonusers. The code also serves to educate managers on their responsibility to encourage and support employee ethical behavior and on their own ethical responsibilities.
3. A code provides a measure of support for a professional whose decision to act ethically in a situation may create conflict with an employer or customer.

4. A code can be a means of deterrence and discipline. A professional society can use a code as a justification for revoking membership or even a professional license. An employee can use a code as a basis for a disciplinary action.
5. A code can enhance the profession's public image, if it is seen to be widely honored.

Answers to Problems

19.1 **Article 2 Illegal access**: This is a general threat the could fall into any of the three categories, depending on what use is made of the access.
Article 3 Illegal interception: Computer as target, attack on data confidentiality.
Article 4 Data interference: Computer as target, attack on data integrity.
Article 5 System interference: Computer as target, various attack types.
Article 6 Misuse of devices: Primarily computer as communications tool.
Article 7 Computer-related forgery: Computer as target, data integrity or privacy.
Article 8 Computer-related fraud: Computer as communications tool
Article 9 Offenses related to child pornography: Computer as communications tool.
Article 10 Infringements of copyright and related rights: Computer as communications tool.
Article 11 Attempt and aiding or abetting: Computer as communications tool.

19.2 **Theft of intellectual property:** Computer as target, attack on data confidentiality.
Theft of other (proprietary) info including customer records, financial records, etc.: Computer as target, attack on privacy.
Denial of service attacks: Computer as target, attack on availability.
Virus, worms or other malicious code: This is a general threat the could fall into any of the three categories, depending on what use is made of the attack.
Fraud (credit card fraud, etc.): Computer as communications tool.
Identity theft of customer: Computer as communications tool.
Illegal generation of spam e-mail. Computer as communications tool.
Phishing: Computer as target, attack on privacy.

Unauthorized access to/use of information, systems or networks: This is a general threat the could fall into any of the three categories, depending on what use is made of the attack.
Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks: Computer as target, attack on availability.
Extortion: Computer as communications tool.
Web site defacement: Computer as target, attack on data integrity.
Zombie machines on organization's network/bots/use of network by BotNets: Computer as communications tool.
Intentional exposure of private or sensitive information: Computer as target, attack on privacy.
Spyware (not including adware): Computer as communications tool.

19.3 There is no simple answer to this problem, as it depends on which survey is reviewed, given that the details do change from year to year and region to region. Any answer should note significant changes in the types of crime reported, and differences between the survey results and those shown in Table 19.2.

19.4 There is no single answer to this problem. However a web search on 'DeCSS' should be done. Two key current sites are the Gallery of CSS Descramblers at CMU (http://www.cs.cmu.edu/~dst/DeCSS/Gallery/) and the Wikipedia DeCSS page which both provide many details and further links on the case. Given the very large number of items in the Gallery of CSS Descramblers (http://www.cs.cmu.edu/~dst/DeCSS/Gallery/) it is fair to conclude that the MPAA failed to suppressing details of the DeCSS descrambling algorithm.

19.5 If a person purchases a track from the iTunes store, protected by Apple's FairPlay DRM, by an EMI artist, then the DRM component roles shown in Figure 19.3 in this case are: Content Provider is EMI, Distributor and Clearinghouse are both handled by the iTunes Store, and the Consumer is the person purchasing the track.

19.6 EU calls out the need for notice. This proactive measure is worthwhile. OECD mentions collection limitation, not explicitly called out in the EU list. Again, a worthwhile principle.

19.7 There is no simple answer to this problem, as it depends on the relevant organization's Privacy Policy. However any answer should consider all the principles listed in section 19.3, and should also refer to any relevant privacy legislation that applies to the chosen organization.

19.8 There is considerable overlap in spirit. The guidelines in the problem are perhaps more oriented to specific management action. They serve as a useful supplement to the standardized checklist of items in the Standard of Good Practice.

19.9 In this scenario, the administrator has very likely broken the law (though it depends on the jurisdiction applying), and breached company policy (provided they actually had one), even if for potentially altruistic reasons. The actions likely violated several of the potential ethical dilemmas listed in Table 19.3 including employee monitoring (in checking their passwords), hacking (in accessing the password files from other sections), and even internal privacy (knowing other user's passwords gives access to their data that you otherwise do not have authorization for). You might defend yourself by arguing that as a systems administrator you were authorized to access the password file. Unfortunately you are not the administrator for the section whose password file was cracked, and it will be difficult to argue that you had authority to do so. You would also have to argue that you had no intent to use that data to break any law, that your motives were not malicious and that they were in the interests of the organization and its employees. You might support these arguments by referring to item 2.5 (analysis of risks) in the ACM code, and item 7 (correct errors) in the IEEE code. The counter argument is that you failed to obey for example item 2.8 (authorized access) in the ACM code. Clearly the outcome would have been more satisfactory if the administrator had raised the issue of password security with senior management, and been granted permission to conduct the survey of current password security in a manner consistent with the law and company policy.

19.10 Assume appropriate section and subsection numbering for AITP.

	ACM	IEEE	AITP
dignity and worth of people	1.2	8, 9	—
personal integrity	Section 2	2, 3, 4	2.1, 3.6
responsibility for work	Section 2	1	1.3
confidentiality of information	1.7, 1.8	—	3.1, 4.5
public safety, health, and welfare	1.1, 1.2	1	3.3
participation in professional societies	—	—	—
knowledge about technology related to social power.	2.7	5	4.8

19.11 **a.** EC1.2, EC2.2, and EC4.1 seem designed more to protect ACM's reputation than to focus on the professionals ethical responsibility and so can reasonably be excluded. EC 2.3 and EC 3.1 are not explicit in the 1997 Code and perhaps should be. They are covered implicitly however.

b. In a number of areas, the 1997 Code is more detailed and more explicit, which provides better guidance to the professional. For example, the 1997 Code includes references to being aware of the legal responsibilities of professionals and managerial obligations.

19.12 **a.** I.3 refers to adequate compensation; this does not seem to be on target for an ethics code. II.b refers to disseminating information. Even though this is qualified with respect to legal and proprietary restraints, it seems better not to include this in the Code. II.e seems designed more for IEEE's benefit than the individual's. Section III, on responsibilities to employers and clients, is not explicit in the 2006 Code and perhaps should be.

b. Nothing new in the 2006 Code not covered in the older Code.

19.13 **a.** ACM Code. The Software Engineering Code (SEC) specifically calls out responsibilities to client and employer. Perhaps ACM Code should as well. In general SEC is more detailed; this has the benefit of covering more ground in more detail but the disadvantage of discouraging professionals from reading the whole code.

b. IEEE Code. SEC specifically calls out responsibilities to client and employer. SEC specifically addresses confidentiality. Both should probably be addressed in IEEE code.

c. AITP Code. SEC refers to the quality of the products of the professional. AITP does not specifically call this out.

CHAPTER 20 SYMMETRIC ENCRYPTION & MESSAGE CONFIDENTIALITY

ANSWERS TO QUESTIONS

20.1 Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

20.2 Permutation and substitution.

20.3 One secret key.

20.4 A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

20.5 Cryptanalysis and brute force.

20.6 In some modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

20.7 With triple encryption, a plaintext block is encrypted by passing it through an encryption algorithm; the result is then passed through the same encryption algorithm again; the result of the second encryption is passed through the same encryption algorithm a third time. Typically, the second stage uses the decryption algorithm rather than the encryption algorithm.

20.8 There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

20.9 With **link encryption**, each vulnerable communications link is equipped on both ends with an encryption device. With **end-to-end encryption**, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data; the data in encrypted form are then transmitted unaltered across the network to the destination terminal or host.

20.10 For two parties A and B, key distribution can be achieved in a number of ways, as follows:

1. A can select a key and physically deliver it to B.
2. A third party can select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

20.11 A **session key** is a temporary encryption key used between two principals. A **master key** is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys. Typically, the master keys are distributed by noncryptographic means.

20.12 A key distribution center is a system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal.

ANSWERS TO PROBLEMS

20.1 To see that the same algorithm with a reversed key order produces the correct result, consider the figure following this discussion, which shows the encryption process going down the left-hand side and the decryption process going up the right-hand side for a 16-round algorithm (the result would be the same for any number of rounds). For clarity, we use the notation LE_i and RE_i for data traveling through the encryption algorithm and LD_i and RD_i for data traveling through the decryption algorithm. The diagram indicates that, at every round, the intermediate value of the decryption process is equal to the corresponding value of the encryption process with the two halves of the value swapped. To put this another way, let the output of the ith encryption round be $LE_i||RE_i$ (L_i concatenated with R_i). Then the corresponding input to the (16 – i)th decryption round is $RD_i||LD_i$.

Let us walk through the figure to demonstrate the validity of the preceding assertions. To simplify the diagram, it is unwrapped, not showing the swap that occurs at the end of each iteration. But note that the intermediate result at the end of the ith stage of the encryption process is the 2w-bit quantity formed by concatenating LE_i and RE_i, and that the intermediate result at the end of the ith stage of the decryption process is the 2w-bit quantity formed by concatenating LD_i and RD_i. After the last iteration of the encryption process, the two halves of the output are swapped, so that the ciphertext is $RE_{16}||LE_{16}$. The output of that round is the ciphertext. Now take that ciphertext and use it as input to the same algorithm. The input to the first round is $RE_{16}||LE_{16}$, which is equal to the 32-bit swap of the output of the sixteenth round of the encryption process.

Now we would like to show that the output of the first round of the decryption process is equal to a 32-bit swap of the input to the sixteenth round of the encryption process. First, consider the encryption process. We see that:

$$LE_{16} = RE_{15}$$
$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

On the decryption side:

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$
$$RD_1 = LD_0 \oplus F(RD_0, K_{16})$$
$$= RE_{16} \oplus F(RE_{15}, K_{16})$$
$$= [LE_{15} \oplus F(RE_{15},K_{16})] \oplus F(RE_{15}, K_{16})$$

The XOR has the following properties:

$$[A \oplus B] \oplus C = A \oplus [B \oplus C]$$
$$D \oplus D = 0$$
$$E \oplus 0 = E$$

Thus, we have $LD_1 = RE_{15}$ and $RD_1 = LE_{15}$. Therefore, the output of the first round of the decryption process is $LE_{15}||RE_{15}$, which is the 32-bit swap of the input to the sixteenth round of the encryption. This correspondence holds all the way through the 16 iterations, as is easily shown. We can cast this process in general terms. For the ith iteration of the encryption algorithm:

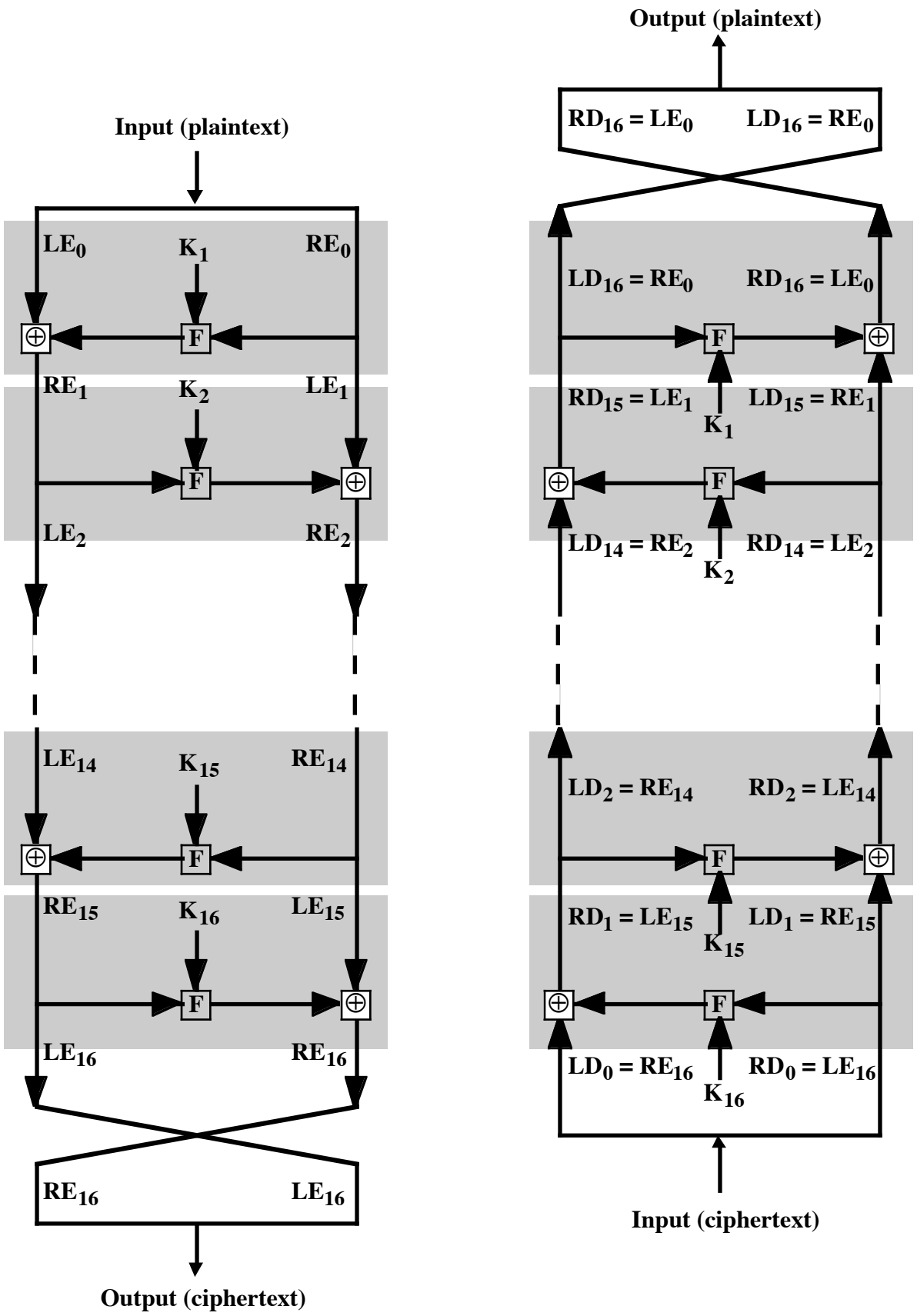
$$LE_i = RE_{i-1}$$
$$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$$

Rearranging terms:

$$RE_{i-1} = LE_i$$
$$LE_{i-1} = RE_i \oplus F(RE_{i-1}, K_i) = RE_i \oplus F(LE_i, K_i)$$

Thus, we have described the inputs to the ith iteration as a function of the outputs, and these equations confirm the assignments shown in the right-hand side of the following figure.

Finally, we see that the output of the last round of the decryption process is $RE_0||LE_0$. A 32-bit swap recovers the original plaintext, demonstrating the validity of the Feistel decryption process.


Input (plaintext)
LE0
K1
RE0
F
RE1
K2
LE1
F
LE2
RE2
LE14
K15
RE14
F
RE15
K16
LE15
F
LE16
RE16
RE16
LE16
Output (ciphertext)
Output (plaintext)
RD16 = LE0
LD16 = RE0
LD16 = RE0
RD16 = LE0
F
RD15 = LE1
LD15 = RE1
K1
F
LD14 = RE2
RD14 = LE2
K2
LD2 = RE14
RD2 = LE14
F
RD1 = LE15
LD1 = RE15
K15
F
LD0 = RE16
RD0 = LE16
K16
Input (ciphertext)

20.2 Because of the key schedule, the round functions used in rounds 9 through 16 are mirror images of the round functions used in rounds 1 through 8. From this fact we see that encryption and decryption are identical. We are given a ciphertext *c*. Let *m*' = *c*. Ask the encryption oracle to encrypt *m*'. The ciphertext returned by the oracle will be the decryption of *c*.

20.3 For $1 \le i \le 128$, take $c_i \in \{0, 1\}^{128}$ to be the string containing a 1 in position i and then zeros elsewhere. Obtain the decryption of these 128 ciphertexts. Let $m_1, m_2, \ldots, m_{128}$ be the corresponding plaintexts. Now, given any ciphertext c which does not consist of all zeros, there is a unique nonempty subset of the c_i's which we can XOR together to obtain c. Let $I(c) \subseteq \{1, 2, \ldots, 128\}$ denote this subset. Observe

$$c = \bigoplus_{i \in I(c)} c_i = \bigoplus_{i \in I(c)} E(m_i) = E\left(\bigoplus_{i \in I(c)} m_i \right)$$

Thus, we obtain the plaintext of c by computing $\bigoplus_{i \in I(c)} m_i$. Let **0** be the all-zero string. Note that **0** = **0** ⊕ **0**. From this we obtain E(**0**) = E(**0** ⊕ **0**) = E(**0**) ⊕ E(**0**) = **0**. Thus, the plaintext of c = **0** is m = **0**. Hence we can decrypt every $c \in \{0, 1\}^{128}$.

20.4 Use a key of length 255 bytes. The first two bytes are zero; that is K[0] = K[1] = 0. Thereafter, we have: K[2] = 255; K[3] = 254; … K[255]= 2.

20.5 **a.** Simply store i, j, and S, which requires $8 + 8 + (256 \times 8) = 2064$ bits

b. The number of states is $[256! \times 256^2] \approx 2^{1700}$. Therefore, 1700 bits are required.

20.6 **a.** No. For example, suppose C_1 is corrupted. The output block P_3 depends only on the input blocks C_2 and C_3.

b. An error in P_1 affects C_1. But since C_1 is input to the calculation of C_2, C_2 is affected. This effect carries through indefinitely, so that all ciphertext blocks are affected. However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. You can show this by writing out the equations for the decryption. Therefore, the error only effects the corresponding decrypted plaintext block.

20.7 If an error occurs in transmission of ciphertext block C_i, then this error propagates to the recovered plaintext blocks P_i and P_{i+1}.

20.8 **a.** If the IVs are kept secret, the 3-loop case has more bits to be determined and is therefore more secure than 1-loop for brute force attacks.

b. For software implementations, the performance is equivalent for most measurements. One-loop has two fewer XORs per block. three-loop might benefit from the ability to do a large set of blocks with a single key before switching. The performance difference from choice of mode can be expected to be smaller than the differences induced by normal variation in programming style.

For hardware implementations, three-loop is three times faster than one-loop, because of pipelining. That is: Let P_i be the stream of input plaintext blocks, X_i the output of the first DES, Y_i the output of the second DES and C_i the output of the final DES and therefore the whole system's ciphertext.

In the 1-loop case, we have:

X_i = DES(XOR(P_i, C_{i-1}))
Y_i = DES(X_i)
C_i = DES(Y_i)

[where C_0 is the single IV]

If P_1 is presented at t=0 (where time is measured in units of DES operations), X_1 will be available at t=1, Y_1 at t=2 and C_1 at t=3. At t=1, the first DES is free to do more work, but that work will be:

X_2 = DES(XOR(P_2, C_1))

but C_1 is not available until t=3, therefore X_2 can not be available until t=4, Y_2 at t=5 and C_2 at t=6.

In the 3-loop case, we have:

X_i = DES(XOR(P_i, X_{i-1}))
Y_i = DES(XOR(X_i, Y_{i-1}}))
C_i = DES(XOR(Y_i, C_{i-1}))

[where X_0, Y_0 and C_0 are three independent IVs]

If P_1 is presented at t=0, X_1 is available at t=1. Both X_2 and Y_1 are available at t=4. X_3, Y_2 and C_1 are available at t=3. X_4, Y_3 and C_2 are available at t=4. Therefore, a new ciphertext block is produced every 1 tick, as opposed to every 3 ticks in the single-loop case. This gives the three-loop construct a throughput three times greater than the one-loop construct.

20.9 Instead of CBC [CBC (CBC (X))], use ECB [CBC (CBC (X))]. The final IV was not needed for security. The lack of feedback loop prevents the chosen-ciphertext differential cryptanalysis attack. The extra IVs still become part of a key to be determined during any known plaintext attack.

20.10

Mode	Encrypt	Decrypt
ECB	$C_j = E(K, P_j)$ $j = 1, \ldots, N$	$P_j = D(K, C_j)$ $j = 1, \ldots, N$
CBC	$C_1 = E(K, [P_1 \oplus IV])$ $C_j = E(K, [P_j \oplus C_{j-1}])$ $j = 2, \ldots, N$	$P_1 = D(K, C_1) \oplus IV$ $P_j = D(K, C_j) \oplus C_{j-1}$ $j = 2, \ldots, N$
CFB	$C_1 = P_1 \oplus S_s(E[K, IV])$ $C_j = P_j \oplus S_s(E[K, C_{j-1}])$	$P_1 = C_1 \oplus S_s(E[K, IV])$ $P_j = C_j \oplus S_s(E[K, C_{j-1}])$
OFB	$C_1 = P_1 \oplus S_s(E[K, IV])$ $C_j = P_j \oplus S_s(E(K, [C_{j-1} \oplus P_{j-1}]))$	$P_1 = C_1 \oplus S_s(E[K, IV])$ $P_j = C_j \oplus S_s(E(K, [C_{j-1} \oplus P_{j-1}]))$
CTR	$C_j = P_j \oplus E[K, Counter + j - 1]$	$P_j = C_j \oplus E[K, Counter + j - 1]$

20.11 After decryption, the last byte of the last block is used to determine the amount of padding that must be stripped off. Therefore there must be at least one byte of padding.

20.12 **a.** Assume that the last block of plaintext is only L bytes long, where $L < 2w/8$. The encryption sequence is as follows (The description in RFC 2040 has an error; the description here is correct.):

1. Encrypt the first $(N - 2)$ blocks using the traditional CBC technique.
2. XOR P_{N-1} with previous ciphertext block C_{N-2} to create Y_{N-1}.
3. Encrypt Y_{N-1} to create E_{N-1}.

4. Select the first L bytes of E_{N-1} to create C_N.

5. Pad P_N with zeros at the end and exclusive-OR with E_{N-1} to create Y_N.

6. Encrypt Y_N to create C_{N-1}.

The last two blocks of the ciphertext are C_{N-1} and C_N.

b. $P_{N-1} = C_{N-2} \oplus D(K, [C_N \| X])$

$P_N \| X = (C_N \| 00\ldots0) \oplus D(K, [C_{N-1}])$

P_N = left-hand portion of $(P_N \| X)$

where $\|$ is the concatenation function

20.13 **a.** Assume that the last block (P_N) has j bits. After encrypting the last full block (P_{N-1}), encrypt the ciphertext (C_{N-1}) again, select the leftmost j bits of the encrypted ciphertext, and XOR that with the short block to generate the output ciphertext.

b. While an attacker cannot recover the last plaintext block, he can change it systematically by changing individual bits in the ciphertext. If the last few bits of the plaintext contain essential information, this is a weakness.

20.14 Nine plaintext characters are affected. The plaintext character corresponding to the ciphertext character is obviously altered. In addition, the altered ciphertext character enters the shift register and is not removed until the next eight characters are processed.

20.15 The CBC mode with an IV of 0 and plaintext blocks D1, D2, . . ., Dn and 64-bit CFB mode with IV = D1 and plaintext blocks D2, D3, . . ., Dn yield the same result.

20.16 The central points should be highly fault-tolerant, should be physically secured, and should use trusted hardware/software.

20.17 Yes. The eavesdropper is left with two strings, one sent in each direction, and their XOR is the secret key.

CHAPTER 21 PUBLIC-KEY CRYPTOGRAPHY & MESSAGE AUTHENTICATION

ANSWERS TO QUESTIONS

21.1 The compression function is the fundamental module, or basic building block, of a hash function. The hash function consists of iterated application of the compression function.

21.2 Addition modulo 2^{64}, circular shift, primitive Boolean functions based on AND, OR, NOT, and XOR.

21.3 To replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module.

21.4 For any given code h, it is computationally infeasible to find x such that $H(x) = h$. A hash function with this property is referred to as **one-way**. This definition appeared in Chapter 2.

21.5 Two parties each create a public-key, private-key pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key and the other side's public key.

ANSWERS TO PROBLEMS

21.1 **a.** Yes. The XOR function is simply a vertical parity check. If there is an odd number of errors, then there must be at least one column that contains an odd number of errors, and the parity bit for that column will detect the error. Note that the RXOR function also catches all errors caused by an odd number of error bits. Each RXOR bit is a function of a unique "spiral" of bits in the block of data. If there is an odd number of errors, then there must be at least one spiral that contains an odd number of errors, and the parity bit for that spiral will detect the error.

b. No. The checksum will fail to detect an even number of errors when both the XOR and RXOR functions fail. In order for both to fail, the

pattern of error bits must be at intersection points between parity spirals and parity columns such that there is an even number of error bits in each parity column and an even number of error bits in each spiral.

c. It is too simple to be used as a secure hash function; finding multiple messages with the same hash function would be too easy.

21.2 **a.** It satisfies properties 1 through 3 but not the remaining properties. For example, for property 4, a message consisting of the value *h* satisfies H(*h*) = *h*. For property 5, take any message *M* and add the decimal digit 0 to the sequence; it will have the same hash value.

b. It satisfies properties 1 through 3. Property 4 is also satisfied if *n* is a large composite number, because taking square roots modulo such an integer *n* is considered to be infeasible. Properties 5 and 6 are not satisfied because –M will have the same value as M.

c. 955

21.3 If you examine the structure of a single round of DES, you see that the round includes a one-way function, F, and an XOR:

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

For DES, the function F is depicted in Figure 2.4. It maps a 32-bit R and a 48-bit K into a 32-bit output. That is, it maps an 80-bit input into a 32-bit output. This is clearly a one-way function. Any hash function that produces a 32-bit output could be used for F. The demonstration in the text that decryption works is still valid for any one-way function F.

21.4 The opponent has the two-block message B1, B2 and its hash RSAH(B1, B2). The following attack will work. Choose an arbitrary C1 and choose C2 such that:

$$C2 = RSA(C1) \oplus RSA(B1) \oplus B2$$

then

$$RSA(C1) \oplus C2 = RSA(C1) \oplus RSA(C1) \oplus RSA(B1) \oplus B2$$
$$= RSA(B1) \oplus B2$$

so $RSAH(C1, C2) = RSA[RSA(C1) \oplus C2)] = RSA[RSA(B1) \oplus B2]$
$= RSAH(B1, B2)$

21.5 **a.** Two quantities are precomputed:

$f(IV, (K^+ \oplus ipad))$
$f(IV, (K^+ \oplus opad))$

where f(cv, block) is the compression function for the hash function, which takes as arguments a chaining variable of n bits and a block of b bits and produces a chaining variable of n bits. These quantities only need to be computed initially and every time the key changes. In effect, the precomputed quantities substitute for the initial value (IV) in the hash function. With this implementation, only one additional instance of the compression function is added to the processing normally produced by the hash function.

b. This is a more efficient implementation. This more efficient implementation is especially worthwhile if most of the messages for which a MAC is computed are short.

21.6 **a.** $n = 33$; $\phi(n) = 20$; $d = 3$; C = 26.

b. $n = 55$; $\phi(n) = 40$; $d = 27$; C = 14.

c. $n = 77$; $\phi(n) = 60$; $d = 53$; C = 57.

d. $n = 143$; $\phi(n) = 120$; $d = 11$; C = 106.

e. $n = 527$; $\phi(n) = 480$; $d = 343$; C = 128. For decryption, we have

$$128^{343} \bmod 527 = 128^{256} \times 128^{64} \times 128^{16} \times 128^{4} \times 128^{2} \times 128^{1} \bmod 527$$
$$= 35 \times 256 \times 35 \times 101 \times 47 \times 128 = 2 \bmod 527$$
$$= 2 \bmod 257$$

21.7 M = 5

21.8 d = 3031

21.9 Yes. If a plaintext block has a common factor with n modulo n then the encoded block will also have a common factor with n modulo n. Because we encode blocks that are smaller than pq, the factor must be p or q and the plaintext block must be a multiple of p or q. We can test each block for primality. If prime, it is p or q. In this case we divide into n to find the other factor. If not prime, we factor it and try the factors as divisors of n.

21.10 Yes.

21.11 Consider a set of alphabetic characters {A, B, …, Z}. The corresponding integers, representing the position of each alphabetic character in the alphabet, form a set of message block values SM = {0, 1, 2, …, 25}. The set of corresponding ciphertext block values SC = $\{0^e \bmod N, 1^e \bmod N, \ldots, 25^e \bmod N\}$, and can be computed by everybody with the knowledge of the public key of Bob.

Thus, the most efficient attack against the scheme described in the problem is to compute $M^e \bmod N$ for all possible values of M, then create a look-up table with a ciphertext as an index, and the

corresponding plaintext as a value of the appropriate location in the table.

21.12 **a.** $X_A = 6$

b. $K = 3$

CHAPTER 22 INTERNET SECURITY PROTOCOLS & STANDARDS

ANSWERS TO QUESTIONS

22.1 **Enveloped data:** This function consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.
Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

22.2 R64 converts a raw 8-bit binary stream to a stream of printable ASCII characters. Each group of three octets of binary data is mapped into four ASCII characters.

22.3 When S/MIME is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted (with the sender's private key). If the confidentiality service is used, the message plus signature (if present) are encrypted (with a one-time symmetric key). Thus, part or all of the resulting block consists of a stream of arbitrary 8-bit octets. However, many electronic mail systems only permit the use of blocks consisting of ASCII text.

22.4 DomainKeys Identified Mail (DKIM) is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream.

22.5 SSL handshake protocol; SSL change cipher spec protocol; SSL alert protocol; SSL record protocol.

22.6 **Connection:** A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session. **Session:** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

22.7 **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

22.8 HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.

22.9 Access control; connectionless integrity; data origin authentication; rejection of replayed packets (a form of partial sequence integrity); confidentiality (encryption); and limited traffic flow confidentiality

22.10 An IPSec security association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both.

22.11 **1.** an authentication-only function referred to as Authentication Header (AH); **2.** a combined authentication/encryption function called Encapsulating Security Payload (ESP).

ANSWERS TO PROBLEMS

22.1 The change cipher spec protocol exists to signal transitions in ciphering strategies, and can be sent independent of the complete handshake protocol exchange.

22.2 **a. Man-in-the-Middle Attack:** This is prevented by the use of public-key certificates to authenticate the correspondents.
b. Password Sniffing: User data is encrypted.

c. **IP Spoofing:** The spoofer must be in possession of the secret key as well as the forged IP address.
d. **IP Hijacking:** Again, encryption protects against this attack.
e. **SYN Flooding:** SSL provides no protection against this attack.

22.3 SSL relies on an underlying reliable protocol to assure that bytes are not lost or inserted. There was some discussion of reengineering the future TLS protocol to work over datagram protocols such as UDP, however, most people at a recent TLS meeting felt that this was inappropriate layering (from the SSL FAQ).

22.4 Inbound processing proceeds as follows when a packet is received:
1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
3. If the received packet is to the left of the window, or if authentication fails, the packet is discarded; this is an auditable event.

22.5 The first mode is called **transport mode**, which provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Examples include a TCP or UDP segment or an ICMP packet, all of which operate directly above IP in a host protocol stack. Typically, transport mode is used for end-to-end communication between two hosts (e.g., a client and a server, or two workstations). When a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header. For IPv6, the payload is the data that normally follow both the IP header and any IPv6 extensions headers that are present, with the possible exception of the destination options header, which may be included in the protection. ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header. AH in transport mode authenticates the IP payload and selected portions of the IP header.
The second mode is called **tunnel mode**, which provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header. The entire original, or inner, packet travels through a "tunnel" from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security. Tunnel mode is used

when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec. The unprotected packets generated by such hosts are tunneled through external networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at the boundary of the local network.

22.6 It certainly provides more security than a simple monoalphabetic substitution. Because we are treating the plaintext as a string of bits and encrypting 6 bits at a time, we are not encrypting individual characters. Therefore, the frequency information is lost, or at least significantly obscured.

22.7 The **quoted-printable** transfer encoding is useful when the data consist largely of octets that correspond to printable ASCII characters. The **base64 transfer encoding**, also known as radix-64 encoding, is a common one for encoding arbitrary binary data in such a way as to be invulnerable to the processing by mail transport programs. This technique maps arbitrary binary input into printable character output.

CHAPTER 23 INTERNET AUTHENTICATION APPLICATIONS

ANSWERS TO QUESTIONS

23.1 **Client:** wishes to authenticate itself to a server.
Server: requires authentication before granting service to client.
Authentication server: authenticates users to servers and servers to users.
Ticket-granting server: issues tickets to users who have been authenticated to the authentication server; the tickets are used to authenticate user to server.

23.2 A realm is an environment in which: **1.** The Kerberos server must have the user ID (UID) and hashed password of all participating users in its database. All users are registered with the Kerberos server. **2.** The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

23.3 Version 5 overcomes some environmental shortcomings and some technical deficiencies in Version 4, including tagging an encrypted message with an encryption algorithm identifier, support for authentication forwarding, and support for a method for inter-realm authentication that requires fewer secure key exchanges than in version 4.

23.4 The X.509 ITU-T standard, also specified in RFC 5280, is the most widely accepted format for public-key certificates. X.509 certificates are used in most network security applications, including IP security (IPSEC), secure sockets layer (SSL), secure electronic transactions (SET), and S/MIME, as well as in eBusiness applications. Each certificate links a public key with the identity of the key's owner, with the whole block signed by a trusted third party certification authority.

23.5 Key elements in a X.509 certificate include the key owning Subject's X.500 name and public-key information, the Period of validity dates, the CA's Issuer name, and their Signature that binds all this information together. Current X.509 certificates use the version 3

format that includes a general extension mechanism to provide more flexibility and to convey information needed in special circumstances.

23.6 Typically, the trusted third party that signs certificates is a **certificate authority** (CA) that is trusted by the user community, such as a government agency, financial institution, telecommunications company, or other trusted peak organization. A user can present his or her public key to the authority in a secure manner and obtain a certificate. The user can then publish the certificate, or send it to others. Anyone needing this user's public key can obtain the certificate and verify that it is valid by way of the attached trusted signature, provided they can verify the CA's public key.

23.7 X.509 certificate variants include:

- **Conventional (long-lived) certificates**: traditional CA and "end user" certificates, linking an identity with a public key, which are typically issued for validity periods of months to years.
- **Short-lived certificates**: are used to provide authentication for applications such as grid computing, while avoiding some of the overheads and limitations of conventional certificates, with validity periods of just hours to days, which limits the period of misuse if compromised.
- **Proxy certificates**: are widely used to provide authentication for applications such as grid computing, while addressing some of the limitations of short-lived certificates. They are identified by the presence of the "proxy certificate" extension. They allow an "end user" certificate to sign another certificate, which must be an extension of their existing certificate.
- **Attribute certificates**: which use a different certificate format, link a user's identity to a set of attributes that are typically used for authorization and access control.

23.8 The X.509 standard defines a certificate revocation list (CRL), signed by the issuer. When an application receives a certificate, the X.509 standard states it should determine whether it has been revoked, by checking against the current CRL for its issuing CA. However, due to the overheads in retrieving and storing these lists, very few applications actually do this. A more practical alternative is to use the Online Certificate Status Protocol (OCSP) to query the CA as to whether a specific certificate is valid. This lightweight protocol is increasingly used, including in most common web browsers.

23.9 A public-key infrastructure (PKI) is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric

cryptography. The principal objective for developing a PKI is to enable secure, convenient, and efficient acquisition of public keys.

23.10 Current X.509 PKI implementations came with a large list of CAs and their public keys, known as a "trust store." These CAs usually either directly sign "end-user" certificates or sign a small number of Intermediate-CAs that in turn sign "end-user" certificates. Thus all the PKI hierarchies are very small, and all are equally trusted. Users and servers that want an automatically verified certificate must acquire it from one of these CAs. Alternatively they can use either a "self-signed" certificate or a certificate signed by some other CA. However, in both these cases, such certificates will initially be recognized as "untrusted" and the user presented with stark warnings about accepting such certificates, even if they are actually legitimate.

23.11 Some key problems with current public key infrastructure implementations include:

- the reliance on the user to make an informed decision when there is a problem verifying a certificate.
- the assumption that all of the CAs in the "trust store" are equally trusted, equally well managed, and apply equivalent policies.
- that different implementations, in the various web browsers and operating systems, use different "trust stores," and hence present different security views to users.

23.12 PKIX key elements are:

End entity: A generic term used to denote end users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public-key certificate. End entities typically consume and/or support PKI-related services.

Certification authority (CA): The issuer of certificates and (usually) certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more registration authorities.

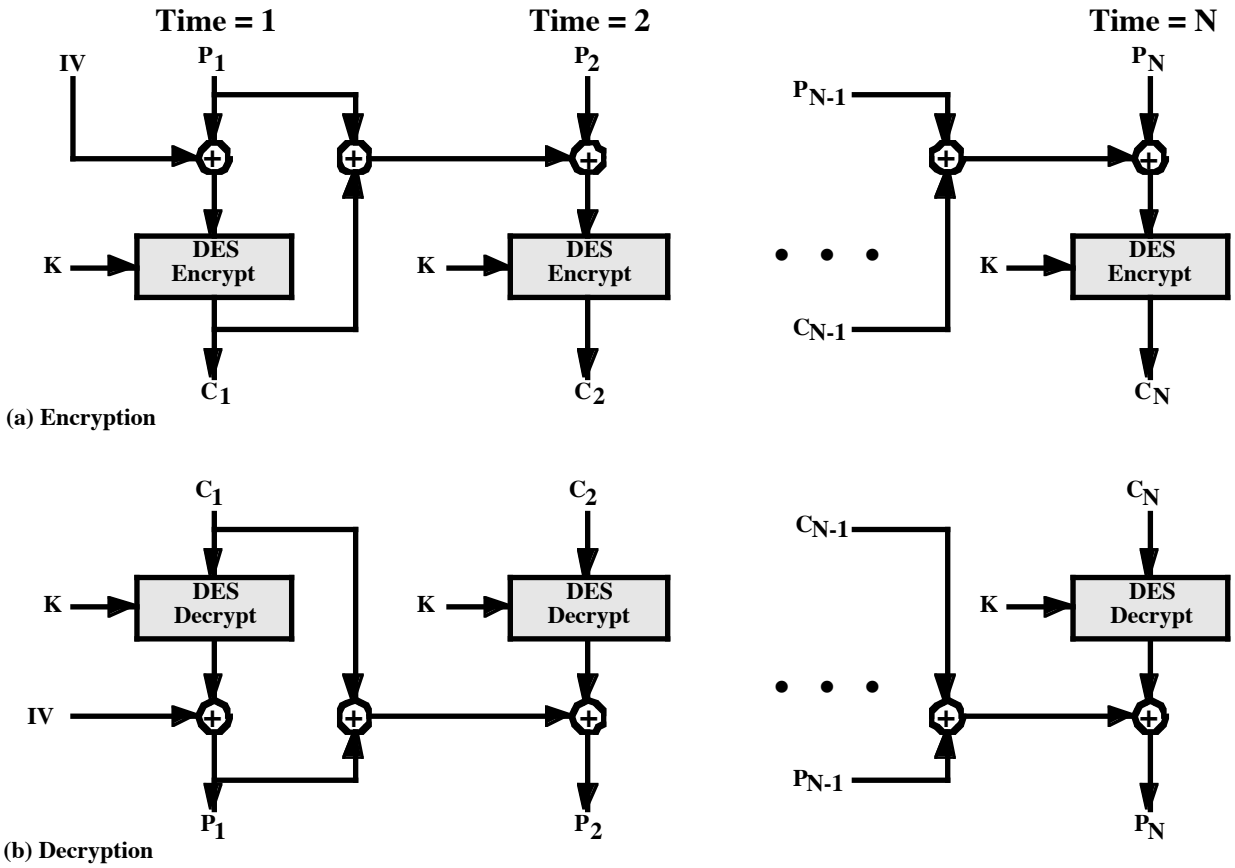
Registration authority (RA): An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the end entity registration process but can assist in a number of other areas as well.

CRL issuer: An optional component that a CA can delegate to publish CRLs.

Repository: A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

ANSWERS TO PROBLEMS

23.1 a.



b. On decryption, each ciphertext block is passed through the decryption algorithm. Then the output is XORed with the preceding ciphertext block and the preceding plaintext block. We can demonstrate that this scheme works, as follows:

$$D(K, C_n) = D(K, E(K, [C_{n-1} \oplus P_{n-1} \oplus P_n]))$$
$$D(K, C_n) = C_{n-1} \oplus P_{n-1} \oplus P_n$$
$$C_{n-1} \oplus P_{n-1} \oplus D(K, C_n) = P_n$$

c. An error in C_1 affects P_1 because the encryption of C_1 is XORed with IV to produce P_1. Both C_1 and P_1 affect P_2, which is the XOR of the encryption of C_2 with the XOR of C_1 and P_1. Beyond that, P_{N-1} is one of the XORed inputs to forming P_N.

23.2 Let us consider the case of the interchange of C_1 and C_2. The argument will be the same for any other adjacent pair of ciphertext blocks. First, if C_1 and C_2 arrive in the proper order:

$P_1 = E[K, C_1] \oplus IV$
$P_2 = E[K, C_2] \oplus C_1 \oplus P_1 = E[K, C_2] \oplus C_1 \oplus E[K, C_1] \oplus IV$

$P_3 = E[K, C_3] \oplus C_2 \oplus P_2 = E[K, C_3] \oplus C_2 \oplus E[K, C_2] \oplus C_1 \oplus E[K, C_1] \oplus IV$

Now suppose that C_1 and C_2 arrive in the reverse order. Let us refer to the decrypted blocks as Q_i.

$Q_1 = E[K, C_2] \oplus IV$
$Q_2 = E[K, C_1] \oplus C_2 \oplus Q_1 = E[K, C_1] \oplus C_2 \oplus E[K, C_2] \oplus IV$
$Q_3 = E[K, C_3] \oplus C_1 \oplus Q_2 = E[K, C_3] \oplus C_1 \oplus E[K, C_1] \oplus C_2 \oplus E[K, C_2] \oplus IV$

The result is that $Q_1 \neq P_1$; $Q_2 \neq P_2$; but $Q_3 = P_3$. Subsequent blocks are clearly unaffected.

23.3 Given the X.509 certificate shown:

a. key elements are:

- owner's name (Subject, Verisign Digital ID class 1 for John Doe):

```
Subject: O=VeriSign, Inc.,
OU=VeriSign Trust Network,
OU=Persona Not Validated,
OU=Digital ID Class 1 - Netscape
CN=John Doe/Email=john.doe@adfa.edu.au
```

- public key (RSA key with 512 bit modulus as shown):

```
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (512 bit)
    Modulus (512 bit):
      00:98:f2:89:c4:48:e1:3b:2c:c5:d1:48:67:80:53:
      d8:eb:4d:4f:ac:31:a9:fd:11:68:94:ba:44:d8:48:
      46:0d:fc:5c:6d:89:47:3f:9f:d0:c0:6d:3e:9a:8e:
      ec:82:21:48:9b:b9:78:cf:aa:09:61:92:f6:d1:cf:
      45:ca:ea:8f:df
    Exponent: 65537 (0x10001)
```

- validity dates (Jan 13 to Mar 13 2000):

```
Validity
  Not Before: Jan 13 00:00:00 2000 GMT
  Not After : Mar 13 23:59:59 2000 GMT
```

- name of the CA that signed it (Issuer, Verisign Inc):

```
Issuer: O=VeriSign, Inc.,
  OU=VeriSign Trust Network,
  CN=VeriSign Class 1 CA Individual - Persona Not Validated
```

- type (MD5 with RSA) and value of signature:

```
Signature Algorithm: md5WithRSAEncryption
    5a:71:77:c2:ce:82:26:02:45:41:a5:11:68:d6:99:f0:4c:ce:
    7a:ce:80:44:f4:a3:1a:72:43:e9:dc:e1:1a:9b:ec:64:f7:ff:
    21:f2:29:89:d6:61:e5:39:bd:04:e7:e5:3d:7b:14:46:d6:eb:
    8e:37:b0:cb:ed:38:35:81:1f:40:57:57:58:a5:c0:64:ef:55:
    59:c0:79:75:7a:54:47:6a:37:b2:6c:23:6b:57:4d:62:2f:94:
    d3:aa:69:9d:3d:64:43:61:a7:a3:e0:b8:09:ac:94:9b:23:38:
    e8:1b:0f:e5:1b:6e:e2:fa:32:86:f0:c4:0b:ed:89:d9:16:e4:
    a7:77
```

b. it is an end-user certificate, as it has:

```
X509v3 Basic Constraints:
```

`CA:FALSE`

this would have to be "`CA:TRUE`" for a CA certificate.

c. the certificate is not valid as it's validity dates are in the past.

d. the other obvious problem with the algorithms used in this certificate is the use of MD5 in the signature, since research advances in creating MD5 collisions has led to the development of several techniques for forging new certificates for different identities that have the same hash, and hence can reuse the same signature, as an existing valid certificate. Any still valid certificates using MD5 should be revoked and replaced as soon as possible.

23.4 There is no single answer for this problem, as it depends on the site, and it's X.509 certificate. To answer the questions as for 23.3, you would view the same elements of the certificate as listed above. Note that this will be an end-user certificate, as in 23.3.

23.5 There is no single answer for this problem, as it depends on the authority selected, and it's X.509 certificate. To answer the questions as for 23.3, you would view the same elements of the certificate as listed above. Note that this will be a CA certificate, i.e. have "`CA:TRUE`".

CHAPTER 24 WIRELESS NETWORK SECURITY

ANSWERS TO QUESTIONS

24.1 Basic service set.

24.2 Two or more basic service sets interconnected by a distribution system.

24.3 **Association:** Establishes an initial association between a station and an AP. **Authentication:** Used to establish the identity of stations to each other. **Deauthentication:** This service is invoked whenever an existing authentication is to be terminated. **Disassociation:** A notification from either a station or an AP that an existing association is terminated. A station should give this notification before leaving an ESS or shutting down. **Distribution:** used by stations to exchange MAC frames when the frame must traverse the DS to get from a station in one BSS to a station in another BSS. **Integration:** enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN. **MSDU delivery:** delivery of MAC service data units. **Privacy:** Used to prevent the contents of messages from being read by other than the intended recipient. **Reassocation:** Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.

24.4 It may or may not be.

24.5 **Mobility** refers to the types of physical transitions that can be made by a mobile node within an 802.11 environment (no transition, movement from one BSS to another within an ESS, movement from one ESS to another). **Association** is a service that allows a mobile node that has made a transition to identify itself to the AP within a BSS so that the node can participate in data exchanges with other mobile nodes.

24.6 **I**EEE 802.11i addresses three main security areas: authentication, key management, and data transfer privacy.

24.7 **Discovery:** An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.

Authentication: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.

Key generation and distribution: The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only

Protected data transfer: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.

Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.

24.8 TKIP is designed to require only software changes to devices that are implemented with the older wireless LAN security approach called Wired Equivalent Privacy (WEP).

ANSWERS TO PROBLEMS

24.1 **a.** This scheme is extremely simple and easy to implement. It does protect against very simple attacks using an off-the-shelf Wi-Fi LAN card, and against accidental connection to the wrong network.

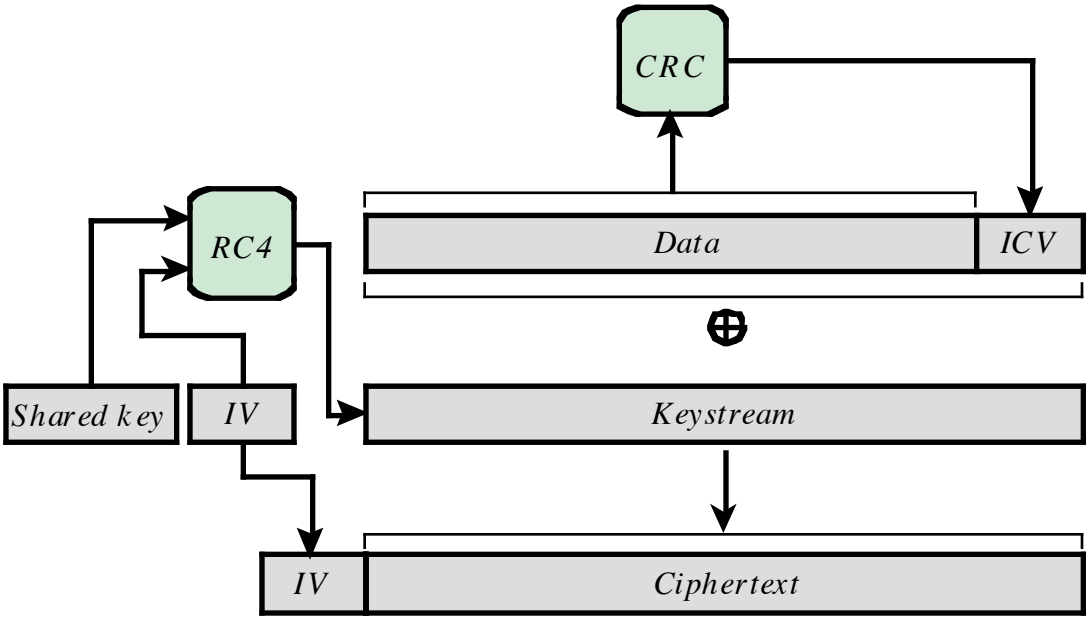
b. This scheme depends on all parties behaving honestly. The scheme does not protect against MAC address forgery.

24.2 **a.** Because the AP remembers the random number previously sent, it can check whether the result sent back was encrypted with the correct key; the STA must know the key in order to encrypt the random value successfully.

b. This scheme does nothing to prove to the STA that the AP knows the key, so authentication is only one way.

c. If an attacker is eavesdropping, this scheme provides the attacker with a plaintext-ciphertext pair to use in cryptanalysis.

24.3 a.

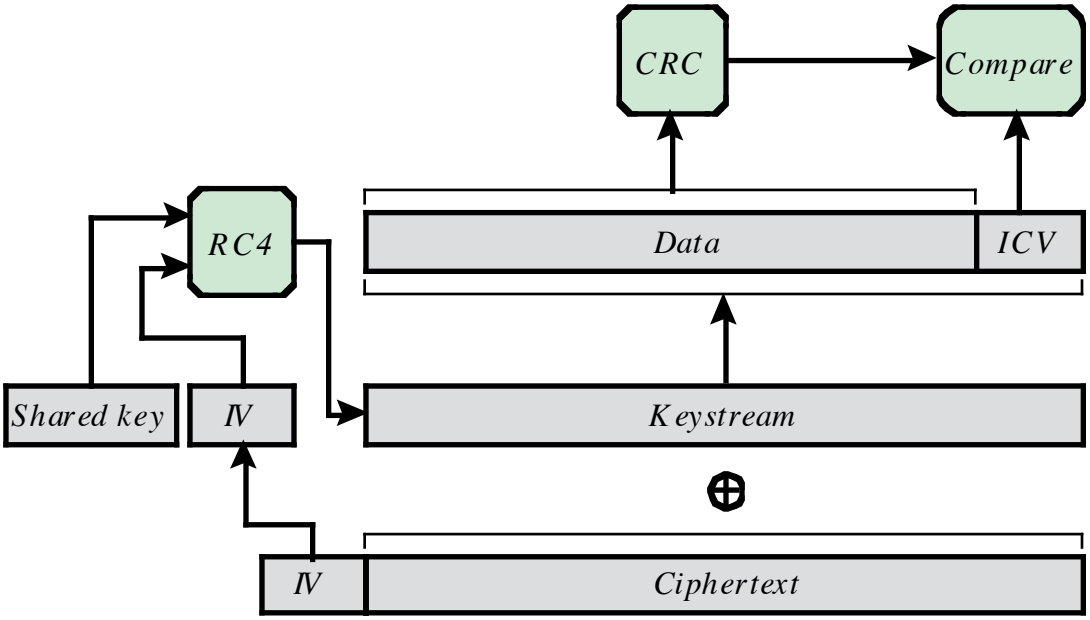


b. 1. The IV value, which is received in plaintext, is concatenated with the WEP key shared by transmitter and receiver to form the seed, or key input, to RC4.

2. The ciphertext portion of the received MPDU is decrypted using RC4 to recover the Data block and the ICV.

3. The ICV is computed over the plaintext received Data block and compared to the received plaintext ICV to authenticate the Data block.

c.



24.4 Because WEP works by XORing the data to get the ciphertext, bit flipping survives the encryption process. Flipping a bit in the plaintext always flips the same bit in the ciphertext and vice versa.