CHAPTER 1 INTRODUCTION

ANSWERS TO QUESTIONS

1.1 The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

1.2 **Passive attacks:** release of message contents and traffic analysis.
Active attacks: masquerade, replay, modification of messages, and denial of service.

1.3 **Authentication:** The assurance that the communicating entity is the one that it claims to be.
Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
Data confidentiality: The protection of data from unauthorized disclosure.
Data integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Availability service: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

1.4 **Cryptographic algorithms**: Transform data between plaintext and ciphertext.
Data integrity: Mechanisms used to assure the integrity of a data unit or stream of data units.
Digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

Authentication exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.
Traffic padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
Routing control: Enables selection of particular physically or logically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
Notarization: The use of a trusted third party to assure certain properties of a data exchange.
Access control: A variety of mechanisms that enforce access rights to resources.

1.5 **Keyless**: Do not use any keys during cryptographic transformations.
Single-key: The result of a transformation are a function of the input data and a single key, known as a secret key.
Two-key: At various stages of the calculate two different but related keys are used, referred to as private key and public key.

1.6 **Communications security**: Deals with the protection of communications through the network, including measures to protect against both passive and active attacks.
Device security: Deals with the protection of network devices, such as routers and switches, and end systems connected to the network, such as client systems and servers.

1.7 **Trust**: The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.
Trustworthiness: A characteristic of an entity that reflects the degree to which that entity is deserving of trust.

ANSWERS TO PROBLEMS

1.1 The system must keep personal identification numbers confidential, both in the host system and during transmission for a transaction. It must protect the integrity of account records and of individual transactions. Availability of the host system is important to the economic well being of the bank, but not to its fiduciary responsibility. The availability of individual teller machines is of less concern.

1.2 The system does not have high requirements for integrity on individual transactions, as lasting damage will not be incurred by occasionally losing a call or billing record. The integrity of control programs and configuration records, however, is critical. Without these, the switching

function would be defeated and the most important attribute of all - availability - would be compromised. A telephone switching system must also preserve the confidentiality of individual calls, preventing one caller from overhearing another.

1.3 a. The system will have to assure confidentiality if it is being used to publish corporate proprietary material.

b. The system will have to assure integrity if it is being used to laws or regulations.

c. The system will have to assure availability if it is being used to publish a daily paper.

1.4 a. An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability.

b. A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate.

c. A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

d. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

e. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. (Examples from FIPS 199.)

CHAPTER 2 INTRODUCTION TO NUMBER THEORY

ANSWERS TO QUESTIONS

2.1 A nonzero b is a **divisor** of a if $a = mb$ for some m, where a, b, and m are integers. That is, b is a **divisor** of a if there is no remainder on division.

2.2 It means that b is a divisor of a.

2.3 In modular arithmetic, all arithmetic operations are performed modulo some integer.

2.4 An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$.

2.5 Euler's totient function, written $\phi(n)$, is the number of positive integers less than n and relatively prime to n.

2.6 The algorithm takes a candidate integer n as input and returns the result "composite" if n is definitely not a prime, and the result "inconclusive" if n may or may not be a prime. If the algorithm is repeatedly applied to a number and repeatedly returns inconclusive, then the probability that the number is actually prime increases with each inconclusive test. The probability required to accept a number as prime can be set as close to 1.0 as desired by increasing the number of tests made.

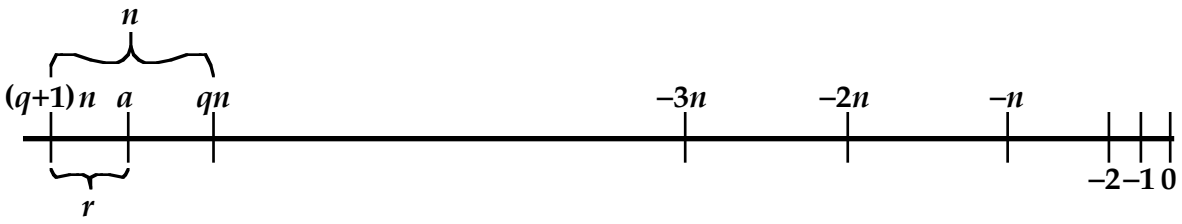
2.7 If r and n are relatively prime integers with $n > 0$. and if $\phi(n)$ is the least positive exponent m such that $a^m \equiv 1 \bmod n$, then r is called a primitive root modulo n.

2.8 The two terms are synonymous.

ANSWERS TO PROBLEMS

2.1 The equation is the same. For integer $a < 0$, a will either be an integer multiple of n of fall between two consecutive multiples qn and $(q + 1)n$, where $q < 0$. The remainder satisfies the condition $0 \le r \le n$.

2.2 In this diagram, q is a negative integer.



2.3 **a.** 2 **b.** 3 **c.** 4 There are other correct answers.

2.4 Section 2.3 defines the relationship: $a = n \times \lfloor a/n \rfloor + (a \bmod n)$. Thus, we can define the mod operator as: $a \bmod n = a - n \times \lfloor a/n \rfloor$.

a. $5 \bmod 3 = 5 - 3\lfloor 5/3 \rfloor = 2$
b. $5 \bmod -3 = 5 - (-3)\lfloor 5/(-3) \rfloor = -1$
c. $-5 \bmod 3 = -5 - 3\lfloor (-5)/3 \rfloor = 1$
d. $-5 \bmod -3 = -5 - (-3)\lfloor (-5)/(-3) \rfloor = -2$

2.5 $a = b$

2.6 Recall Figure 2.1 and that any integer a can be written in the form

$$a = qn + r$$

where q is some integer and r one of the numbers

$$0, 1, 2, \ldots, n - 1$$

Using the second definition, no two of the remainders in the above list are congruent (mod n), because the difference between them is less than n and therefore n does not divide that difference. Therefore, two numbers that are not congruent (mod n) must have different remainders. So we conclude that n divides $(a - b)$ if and only if a and b are numbers that have the same remainder when divided by n.

2.7 1, 2, 4, 6, 16, 12

2.8 **a.** This is the definition of congruence as used in Section 2.3.

b. The first two statements mean

$$a - b = nk; \quad b - c = nm$$

so that

$$a - c = (a - b) + (b - c) = n(k + m)$$

2.9 **a.** Let c = a mod n and d = b mod n. Then

$c = a + kn$; $d = b + mn$; $c - d = (a - b) + (k - m)n$.

Therefore $(c - d) = (a - b) \bmod n$

b. Using the definitions of c and d from part (a),

$cd = ab + n(kb + ma + kmn)$

Therefore $cd = (a \times b) \bmod n$

2.10 $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

2.11 We have $1 \equiv 1 \pmod 9$; $10 \equiv 1 \pmod 9$; $10^2 \equiv 10(10) \equiv 1(1) \equiv 1 \pmod 9$; $10^{n-1} \equiv 1 \pmod 9$. Express N as $a_0 + a_1 10^1 + \ldots + a_{n-1}10^{n-1}$. Then $N \equiv a_0 + a_1 + \ldots + a_{n-1} \pmod 9$.

2.12 **a.** gcd(24140, 16762) = gcd(16762, 7378) = gcd(7378, 2006) = gcd(2006, 1360) = gcd(1360, 646) = gcd (646, 68) = gcd(68, 34) = gcd(34, 0) = 34

b. 35

2.13 **a.** We want to show that m > 2r. This is equivalent to qn + r > 2r, which is equivalent to qn > r. Since n > r, we must have qn > r.

b. If you study the pseudocode for Euclid's algorithm in the text, you can see that the relationship defined by Euclid's algorithm can be expressed as

$$A_i = q_i A_{i+1} + A_{i+2}$$

The relationship $A_{i+2} < A_i/2$ follows immediately from (a).

c. From (b), we see that $A_3 < 2^{-1}A_1$, that $A_5 < 2^{-1}A_3 < 2^{-2}A_5$, and in general that $A_{2j+1} < 2^{-j}A_1$ for all integers j such that $1 < 2j + 1 \leq k + 2$, where k is the number of steps in the algorithm. If k is odd, we take j = (k + 1)/2 to obtain N > (k + 1)/2, and if k is even, we take j = k/2 to obtain N > k/2. In either case k < 2N.

2.14 **a.** **Euclid:** gcd(2152, 764) = gcd(764, 624) = gcd(624, 140) = gcd(140, 64) = gcd(64, 12) = gcd(12, 4) = gcd(4, 0) = 4

Stein: $A_1 = 2152$, $B_1 = 764$, $C_1 = 1$; $A_2 = 1076$, $B_2 = 382$, $C_2 = 2$; $A_3 = 538$, $B_3 = 191$, $C_3 = 4$; $A_4 = 269$, $B_4 = 191$, $C_4 = 4$; $A_5 = 78$, $B_5 = 191$, $C_5 = 4$; $A_5 = 39$, $B_5 = 191$, $C_5 = 4$; $A_6 = 152$, $B_6 = 39$, $C_6 = 4$; $A_7 = 76$, $B_7 = 39$, $C_7 = 4$; $A_8 = 38$, $B_8 = 39$, $C_8 = 4$; $A_9 = 19$, $B_9 = 39$, $C_9 = 4$; $A_{10} = 20$, $B_{10} = 19$, $C_{10} = 4$; $A_{11} = 10$, $B_{11} = 19$, $C_{11} = 4$; $A_{12} = 5$, $B_{12} = 19$, $C_{12} = 4$; $A_{13} = 14$, $B_{13} = 5$, $C_{13} = 4$; $A_{14} = 7$, $B_{14} = 5$, $C_{14} = 4$; $A_{15} = 2$, $B_{15} = 5$, $C_{15} = 4$; $A_{16} = 1$, $B_{16} = 5$, $C_{16} = 4$; $A_{17} = 4$, $B_{17} = 1$, $C_{17} = 4$; $A_{18} = 2$, $B_{18} = 1$, $C_{18} = 4$; $A_{19} = 1$, $B_{19} = 1$, $C_{19} = 4$; $\gcd(2152, 764) = 1 \times 4 = 4$

b. Euclid's algorithm requires a "long division" at each step whereas the Stein algorithm only requires division by 2, which is a simple operation in binary arithmetic.

2.15 a. If A_n and B_n are both even, then $2 \times \gcd(A_{n+1}, B_{n+1}) = \gcd(A_n, B_n)$. But $C_{n+1} = 2C_n$, and therefore the relationship holds.

If one of A_n and B_n is even and one is odd, then dividing the even number does not change the gcd. Therefore, $\gcd(A_{n+1}, B_{n+1}) = \gcd(A_n, B_n)$. But $C_{n+1} = C_n$, and therefore the relationship holds.

If both A_n and B_n are odd, we can use the following reasoning based on the rules of modular arithmetic. Let $D = \gcd(A_n, B_n)$. Then D divides $|A_n - B_n|$ and D divides $\min(A_n, B_n)$. Therefore, $\gcd(A_{n+1}, B_{n+1}) = \gcd(A_n, B_n)$. But $C_{n+1} = C_n$, and therefore the relationship holds.

b. If at least one of A_n and B_n is even, then at least one division by 2 occurs to produce A_{n+1} and B_{n+1}. Therefore, the relationship is easily seen to hold.

Suppose that both A_n and B_n are odd; then A_{n+1} is even; in that case the relationship obviously holds.

c. By the result of (b), every 2 iterations reduces the AB product by a factor of 2. The AB product starts out at $< 2^{2N}$. There are at most $\log(2^{2N}) = 2N$ pairs of iterations, or at most 4N iterations.

d. At the very beginning, we have $A_1 = A$, $B_1 = B$, and $C_1 = 1$. Therefore $C_1 \times \gcd(A_1, B_1) = \gcd(A, B)$. Then, by (a), $C_2 \times \gcd(A_2, B_2) = C_1 \times \gcd(A_1, B_1) = \gcd(A, B)$. Generalizing, $C_n \times \gcd(A_n, B_n) = \gcd(A, B)$. The algorithm stops when $A_n = B_n$. But, for $A_n = B_n$, $\gcd(A_n, B_n) = A_n$. Therefore, $C_n \times \gcd(A_n, B_n) = C_n \times A_n = \gcd(A, B)$.

2.16 a. 3239