SOLUTIONS MANUAL

CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE EIGHTH EDITION

CHAPTERS 1–10

WILLIAM STALLINGS

TABLE OF CONTENTS

NOTICE

This manual contains solutions to the review questions and homework problems in *Cryptography and Network Security, Eighth 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 https://www.box.com/shared/nh8hti5167 File name is S-Crypto8e-mmyy.

W.S.

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.

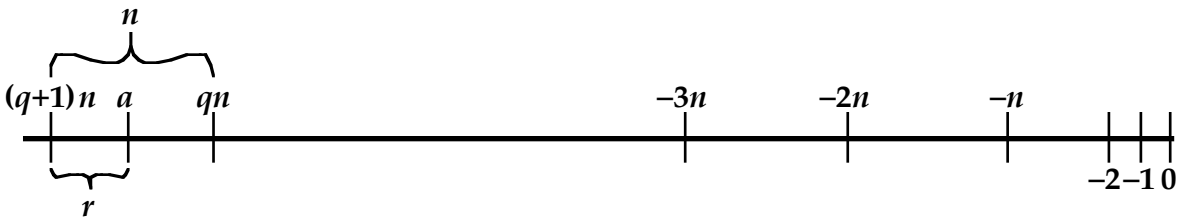
2.7 If r and n are relatively prime integers with $n > 0$. and if $\phi(n)$ is the least positive exponent m such that $a^m \equiv 1 \bmod n$, then r is called a primitive root modulo n.

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

b. gcd(40902, 24240) = 34 ≠ 1, so there is no multiplicative inverse.
c. 550

2.17 a. We are assuming that p_n is the largest of all primes. Because $X > p_n$, X is not prime. Therefore, we can find a prime number p_m that divides X.
b. The prime number p_m cannot be any of $p_1, p_2, \ldots, p_n$; otherwise p_m would divide the difference $X - p_1p_2\ldots p_n = 1$, which is impossible. Thus, $m > n$.
c. This construction provides a prime number outside any finite set of prime numbers, so the complete set of prime numbers is not finite.
d. We have shown that there is a prime number $>p_n$ that divides $X = 1 + p_1p_2\ldots p_n$, so p_{n+1} is equal to or less than this prime. Therefore, since this prime divides X, it is ≤ X and therefore $p_{n+1} \leq X$.

2.18 a. gcd(a, b) = d if and only if a is a multiple of d and b is a multiple of d and gcd(a/d, b/d) = 1. The probability that an integer chosen at random is a multiple of d is just 1/d. Thus the probability that gcd(a, b) = d is equal to 1/d times 1/d times P, namely, P/d^2.
b. We have

$$\sum_{d\geq 1} \Pr\left[\gcd(a,b) = d\right] = \sum_{d\geq 1} \frac{P}{d^2} = P\sum_{d\geq 1} \frac{1}{d^2} = P \times \frac{\pi^2}{6} = 1$$

To satisfy this equation, we must have $P = \frac{6}{\pi^2}$ = 0.6079.

2.19 If p were any prime dividing n and $n + 1$ it would also have to divide

$$(n + 1) - n = 1$$

2.20 Fermat's Theorem states that if p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Therefore $3^{10} \equiv 1 \pmod{11}$. Therefore

$$3^{201} = (3^{10})^{20} \times 3 \equiv 3 \pmod{11}.$$

2.21 12

2.22 6

2.23 1

2.24 6

2.25 If a is one of the integers counted in $\phi(n)$, that is, one of the integers not larger than n and prime to n, the n – 1 is another such integer, because gcd(a, n) = gcd(m – a, m). The two integers, a and n – a, are distinct, because a = n – a gives n = 2a, which is inconsistent with the assumption that gcd(a, n) = 1. Therefore, for n > 2, the integers counted in $\phi(n)$ can be paired off, and so the number of them must be even.

2.26 Only multiples of p have a factor in common with p^n, when p is prime. There are just p^{n-1} of these $\leq p^n$, so $\phi(p^n) = p^n - p^{n-1}$.

2.27 **a.** $\phi(41) = 40$, because 41 is prime
b. $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$
c. $\phi(231) = \phi(3) \times \phi(7) \times \phi(11) = 2 \times 6 \times 10 = 120$
d. $\phi(440) = \phi(2^3) \times \phi(5) \times \phi(11) = (2^3 - 2^2) \times 4 \times 10 = 160$

2.28 It follows immediately from the result stated in Problem 2.26.

2.29 totient

2.30 **a.** For n = 5, $2^n - 2 = 30$, which is divisible by 5.
b. We can rewrite the Chinese test as $(2^n - 2) \equiv 0 \bmod n$, or equivalently,
$2^n \equiv 2 \pmod n$. By Fermat's Theorem, this relationship is true **if** n is prime (Equation 2.10).
c. For n = 15, $2^n - 2 = 32{,}766$, which is divisible by 15.
d. $2^{10} = 1024 \equiv 1 \pmod{341}$
$2^{340} = (2^{10})^{34} \equiv (1 \bmod 341)$
$2^{341} \equiv 2 \pmod{341}$

2.31 First consider a = 1. In step 3 of TEST(n), the test is **if** $1^q \bmod n = 1$ **then** return("inconclusive"). This clearly returns "inconclusive." Now consider a = n – 1. In step 5 of TEST(n), for j = 0, the test is if $(n - 1)^q \bmod n = n - 1$ **then** return("inconclusive"). This condition is met by inspection.

2.32 In Step 1 of TEST(2047), we set k = 1 and q = 1023, because $(2047 - 1) = (2^1)(1023)$.
In Step 2 we select a = 2 as the base.
In Step 3, we have $a^q \bmod n = 2^{1023} \bmod 2047 = (2^{11})^{93} \bmod 2047 = (2048)^{93} \bmod 2047 = 1$ and so the test is passed.

2.33 There are many forms to this proof, and virtually every book on number theory has a proof. Here we present one of the more concise proofs. Define $M_i = M/m_i$. Because all of the factors of M are pairwise

relatively prime, we have $\gcd(M_i, m_i) = 1$. Thus, there are solutions N_i of

$$N_i M_i \equiv 1 \pmod{m_i}$$

With these N_i, the solution x to the set of congruences is:

$$x \equiv a_1 N_1 M_1 + \ldots + a_k N_k M_k \pmod{M}$$

To see this, we introduce the notation $\langle x \rangle_m$, by which we mean the least positive residue of x modulo m. With this notation, we have

$$\langle x \rangle_{mi} \equiv a_i N_i M_i \equiv a_i \pmod{m_i}$$

because all other terms in the summation above that make up x contain the factor m_i and therefore do not contribute to the residue modulo m_i. Because $N_i M_i \equiv 1 \pmod{m_i}$, the solution is also unique modulo M, which proves this form of the Chinese Remainder Theorem.

2.34 We have $M = 3 \times 5 \times 7 = 105$; $M/3 = 35$; $M/5 = 21$; $M/7 = 15$. The set of linear congruences

$$35b_1 \equiv 1 \pmod{3}; \quad 21b_2 \equiv 1 \pmod{5}; \quad 15b_3 \equiv 1 \pmod{7}$$

has the solutions $b_1 = 2$; $b_2 = 1$; $b_3 = 1$. Then,

$$x \equiv 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 \equiv 233 \pmod{105} = 23$$

2.35 If the day in question is the xth (counting from and including the first Monday), then

$$x = 1 + 2K_1 = 2 + 3K_2 = 3 + 4K_3 = 4 + K_4 = 5 + 6K_5 = 6 + 5K_6 = 7K_7$$

where the K_i are integers; i.e.,

(1) $x \equiv 1 \bmod 2$; (2) $x \equiv 2 \bmod 3$; (3) $x \equiv 3 \bmod 4$; (4) $x \equiv 4 \bmod 1$; (5) $x \equiv 5 \bmod 6$; (6) $x \equiv 6 \bmod 5$; (7) $x \equiv 0 \bmod 7$

Of these congruences, (4) is no restriction, and (1) and (2) are included in (3) and (5). Of the two latter, (3) shows that x is congruent to 3, 7, or 11 (mod 12), and (5) shows the x is congruent to 5 or 11, so that (3) and (5) together are equivalent to $x \equiv 11 \pmod{12}$. Hence, the problem is that of solving:

$x \equiv 11 \pmod{12}$; $x \equiv 6 \bmod 5$; $x \equiv 0 \bmod 7$
or $x \equiv -1 \pmod{12}$; $x \equiv 1 \bmod 5$; $x \equiv 0 \bmod 7$

Then $m_1 = 12$; $m_2 = 5$; $m_3 = 7$; $M = 420$
$M_1 = 35$; $M_2 = 84$; $M_3 = 60$
Then,

$$x \equiv (-1)(-1)35 + (-1)1 \times 21 + 2 \times 0 \times 60 = -49 \equiv 371 \pmod{420}$$

The first x satisfying the condition is 371.

2.36 2, 3, 8, 12, 13, 17, 22, 23

2.37 **a.** $x = 2, 27 \pmod{29}$
b. $x = 9, 24 \pmod{29}$
c. $x = 8, 10, 12, 15, 18, 26, 27 \pmod{29}$

CHAPTER 3 CLASSICAL ENCRYPTION TECHNIQUES

ANSWERS TO QUESTIONS

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

3.2 Permutation and substitution.

3.3 One key for symmetric ciphers, two keys for asymmetric ciphers.

3.4 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.

3.5 Cryptanalysis and brute force.

3.6 **Ciphertext only**. One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying various statistical tests to it. **Known plaintext.** The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed. **Chosen plaintext.** If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

3.7 An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be **computationally secure** if: (1) the cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.

3.8 The **Caesar cipher** involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.

3.9 A **monoalphabetic substitution cipher** maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.

3.10 The **Playfair algorithm** is based on the use of a 5×5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

3.11 A **polyalphabetic substitution cipher** uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

3.12 **1.** There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

3.13 A **transposition cipher** involves a permutation of the plaintext letters.

ANSWERS TO PROBLEMS

3.1 **a.** No. A change in the value of b shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one.
b. 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24. Any value of a larger than 25 is equivalent to a mod 26.
c. The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that $E(a, p) = E(a, q)$ $(0 \le p \le q < 26)$ if and only if $a(p - q)$ is divisible by 26. **1.** Suppose that a and 26 are relatively prime. Then, $a(p - q)$ is not divisible by 26, because there is no way to reduce the fraction $a/26$ and $(p - q)$ is less than 26. **2.** Suppose that a and 26 have a common factor $k > 1$. Then $E(a, p) = E(a, q)$, if $q = p + m/k \neq p$.

3.2 There are 12 allowable values of a (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25). There are 26 allowable values of b, from 0 through 25). Thus the total number of distinct affine Caesar ciphers is $12 \times 26 = 312$.

3.3 Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are e = 4; B = 1; t = 19; U = 20. Then we have the following equations:

$1 = (4a + b) \bmod 26$
$20 = (19a + b) \bmod 26$

Thus, $19 = 15a \bmod 26$. By trial and error, we solve: $a = 3$.
Then $1 = (12 + b) \bmod 26$. By observation, $b = 15$.

3.4 A good glass in the Bishop's hostel in the Devil's seat—twenty-one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death's head— a bee line from the tree through the shot fifty feet out. (from *The Gold Bug*, by Edgar Allan Poe)

3.5 **a.** The first letter t corresponds to A, the second letter h corresponds to B, e is C, s is D, and so on. Second and subsequent occurrences of a letter in the key sentence are ignored. The result

```
ciphertext:  SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
plaintext:   basilisk to leviathan blake is contact
```

b. It is a monoalphabetic cipher and so easily breakable.
c. The last sentence may not contain all the letters of the alphabet. If the first sentence is used, the second and subsequent sentences may also be used until all 26 letters are encountered.

3.6 The cipher refers to the words in the page of a book. The first entry, 534, refers to page 534. The second entry, C2, refers to column two. The remaining numbers are words in that column. The names DOUGLAS and BIRLSTONE are simply words that do not appear on that page. Elementary! (from *The Valley of Fear*, by Sir Arthur Conan Doyle)

3.7 a.

2	8	10	7	9	6	3	1	4	5
C	R	Y	P	T	O	G	A	H	I
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

4	2	8	10	5	6	3	7	1	9
N	E	T	W	O	R	K	S	C	U
T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D
I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

```
ISRNG  BUTLF  RRAFR  LIDLP  FTIYO  NVSEE  TBEHI  HTETA
EYHAT  TUCME  HRGTA  IOENT  TUSRU  IEADR  FOETO  LHMET
NTEDS  IFWRO  HUTEL  EITDS
```

b. The two matrices are used in reverse order. First, the ciphertext is laid out in columns in the second matrix, taking into account the order dictated by the second memory word. Then, the contents of the second matrix are read left to right, top to bottom and laid out in columns in the first matrix, taking into account the order dictated by the first memory word. The plaintext is then read left to right, top to bottom.

c. Although this is a weak method, it may have use with time-sensitive information and an adversary without immediate access to good cryptanalysis (e.g., tactical use). Plus it doesn't require anything more than paper and pencil, and can be easily remembered.

3.8 SPUTNIK

3.9 PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION

3.10 a.

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

b.

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

3.11 a. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ
b. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ
c. A cyclic rotation of rows and/or columns leads to equivalent substitutions. In this case, the matrix for part a of this problem is obtained from the matrix of Problem 3.10a, by rotating the columns by one step and the rows by three steps.

3.12 a. $25! \approx 2^{84}$
b. Given any 5x5 configuration, any of the four row rotations is equivalent, for a total of five equivalent configurations. For each of these five configurations, any of the four column rotations is equivalent. So each configuration in fact represents 25 equivalent configurations. Thus, the total number of unique keys is 25!/25 = 24!

3.13 A mixed Caesar cipher. The amount of shift is determined by the keyword, which determines the placement of letters in the matrix.