SOLUTIONS MANUAL

CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE SEVENTH EDITION

CHAPTERS 1–10

WILLIAM STALLINGS

NOTICE

This manual contains solutions to the review questions and homework problems in *Cryptography and Network Security, Sixth 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-Crypto7e-mmyy.

W.S.

TABLE OF CONTENTS

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 threats** have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. **Active threats** include the modification of transmitted data and attempts to gain unauthorized access to computer systems.

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

1.4 **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).

1.5 See Table 1.3.

1.6 **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).

1.7 An attack surface consists of the reachable and exploitable vulnerabilities in a system. An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

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.

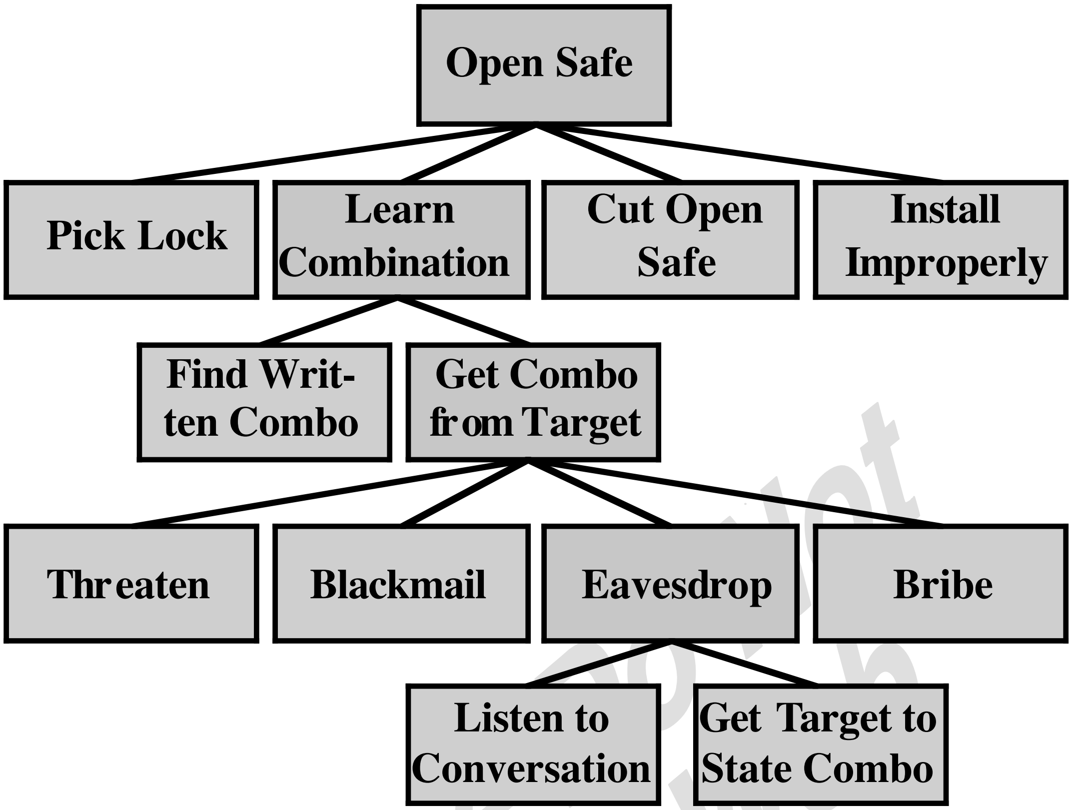
1.5

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

1.6

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

1.7



1.8 We present the tree in text form; call the company X:

Survivability Compromise: Disclosure of X proprietary secrets
OR 1. Physically scavenge discarded items from X
  OR 1. Inspect dumpster content on-site
    2. Inspect refuse after removal from site
  2. Monitor emanations from X machines
  AND 1. Survey physical perimeter to determine optimal monitoring position
    2. Acquire necessary monitoring equipment
    3. Setup monitoring site
    4. Monitor emanations from site
  3. Recruit help of trusted X insider
  OR 1. Plant spy as trusted insider
    2. Use existing trusted insider
  4. Physically access X networks or machines
  OR 1. Get physical, on-site access to Intranet
    2. Get physical access to external machines
  5. Attack X intranet using its connections with Internet
  OR 1. Monitor communications over Internet for leakage
    2. Get trusted process to send sensitive information to attacker over Internet
    3. Gain privileged access to Web server
  6. Attack X intranet using its connections with public telephone network (PTN)
  OR 1. Monitor communications over PTN for leakage of sensitive information
    2. Gain privileged access to machines on intranet connected via Internet

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.

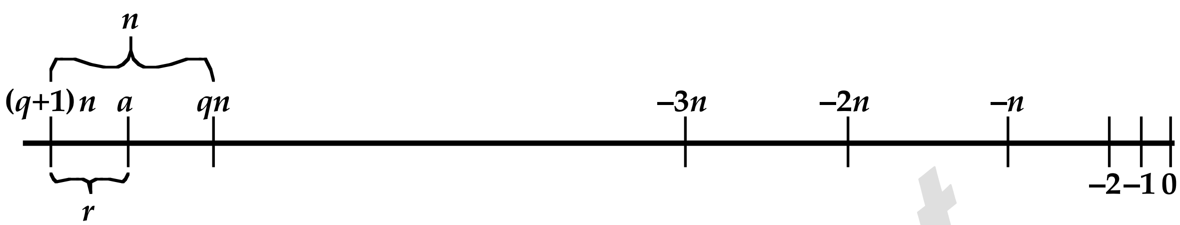
2.7 If r and n are relatively prime integers with $n > 0$. and if $\phi(n)$ is the least positive exponent m such that $a^m \equiv 1 \bmod n$, then r is called a primitive root modulo n.

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: $a = n \times \lfloor a/n \rfloor + (a \text{ mod } n)$. Thus, we can define the mod operator as: $a \text{ mod } n = a - n \times \lfloor a/n \rfloor$.

a. $5 \text{ mod } 3 = 5 - 3\lfloor 5/3 \rfloor = 2$

b. $5 \text{ mod } -3 = 5 - (-3)\lfloor 5/(-3) \rfloor = -1$

c. $-5 \text{ mod } 3 = -5 - 3\lfloor (-5)/3 \rfloor = 1$

d. $-5 \text{ mod } -3 = -5 - (-3)\lfloor (-5)/(-3) \rfloor = -2$

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
$c = a + kn; \quad d = b + mn; \;\; c - d = (a - b) + (k - m)n.$
Therefore $(c - d) = (a - b)$ mod n
b. Using the definitions of c and d from part (a),
$cd = ab + n(kb + ma + kmn)$
Therefore $cd = (a \times b)$ mod 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 $1 < 2j + 1 \le k + 2$, 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 $(2^n - 2) \equiv 0$ mod 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

$$N_iM_i \equiv 1 \pmod{m_i}$$

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

$$x \equiv a_1N_1M_1 + \ldots + a_kN_kM_k \pmod{M}$$

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

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

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 $N_iM_i \equiv 1 \pmod{m_i}$, 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

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

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:

$$x \equiv 11 \text{ (mod 12)}; \; x \equiv 6 \text{ mod } 5; \qquad x \equiv 0 \text{ mod } 7$$

or $$x \equiv -1 \text{ (mod 12)}; \; x \equiv 1 \text{ mod } 5; \qquad x \equiv 0 \text{ mod } 7$$

Then $m_1 = 12$; $m_2 = 5$; $m_3 = 7$; $M = 420$

$M_1 = 35$; $M_2 = 84$; $M_3 = 60$

Then,

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

The first x satisfying the condition is 371.

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

2.37 **a.** x = 2, 27 (mod 29)
b. x = 9, 24 (mod 29)
c. x = 8, 10, 12, 15, 18, 26, 27 (mod 29)