CS6701-

CRYPTOGRAPHY AND NETWORK SECURITY

UNIT 1 NOTES

UNIT – I INTRODUCTION & NUMBER THEORY

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid‟s algorithm-Finite fields-Polynomial Arithmetic –Prime numbers-Fermat‟s and Euler‟s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms.

COMPUTER SECURITY CONCEPTS

Computer Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information / data, and telecommunications)

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner.
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability

- Assures that systems work promptly and service is not denied to authorized users.

CIA Triad

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

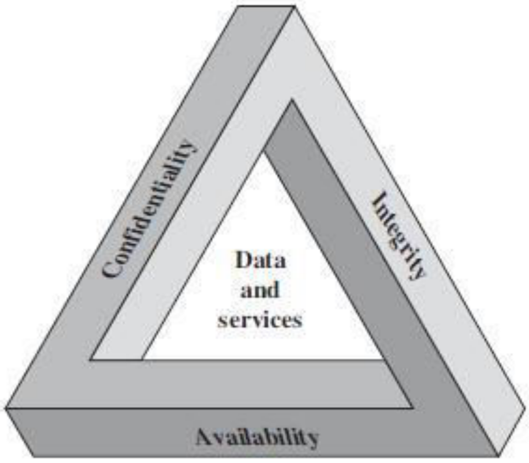


Figure 1.1 The Security Requirements Triad

Availability

- Ensuring timely and reliable access to and use of information
- A loss of availability is the disruption of access to or use of information or an information system.

Authenticity

- The property of being genuine and being able to be verified and trusted

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

The OSI Security Architecture

- ITU-T Recommendation X.800, Security Architecture for OSI, defines such a systematic approach
- The OSI security architecture focuses on security attacks, mechanisms, and services.

Security attack

- Any action that compromises the security of information owned by an organization.

Security mechanism

- A process (or a device) that is designed to detect, prevent, or recover from a security attack.

Security service

- A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Security Attacks

- means of classifying security attacks, used both in X.800 and RFC 2828
- A passive attack attempts to learn or make use of information but does not affect system resources.
- An active attack attempts to alter system resources or affect their operation.

Passive Attacks

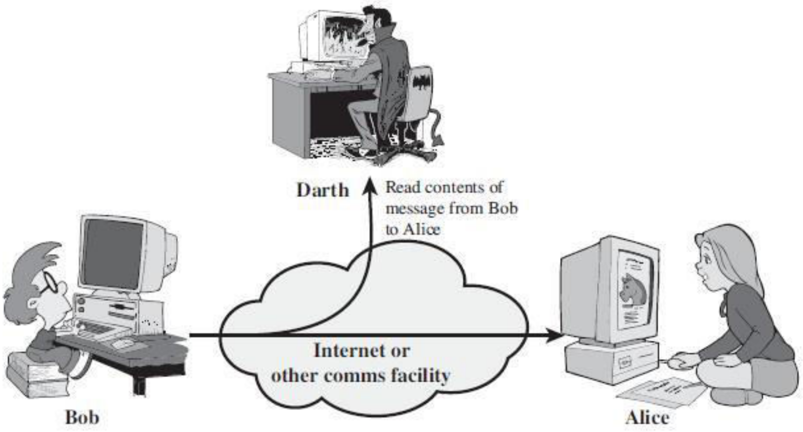
- in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal is to obtain information that is being transmitted.
- very difficult to detect, because they do not involve any alteration of the data
- feasible to prevent the success of these attacks, usually by means of encryption
- emphasis in dealing with passive attacks is on prevention rather than detection

Two types of passive attacks

- Release of message contents
- Traffic analysis.

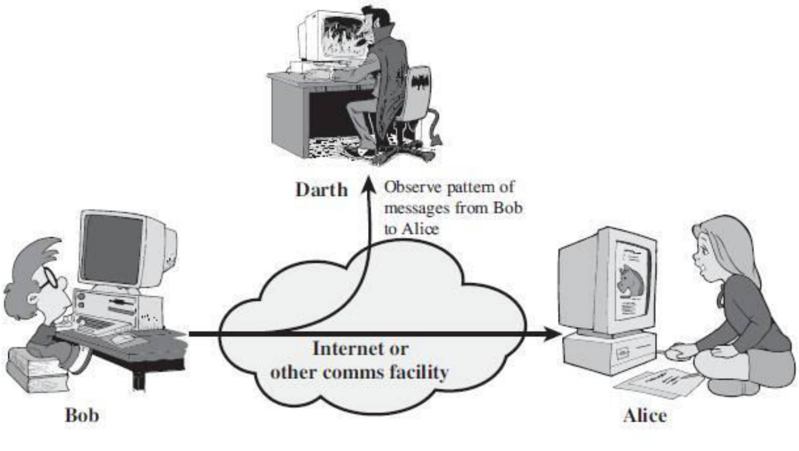
Release Of Message Contents

- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information
- prevent an opponent from learning the contents of these transmissions


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Traffic Analysis

- observe the pattern of these messages
- The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attacks

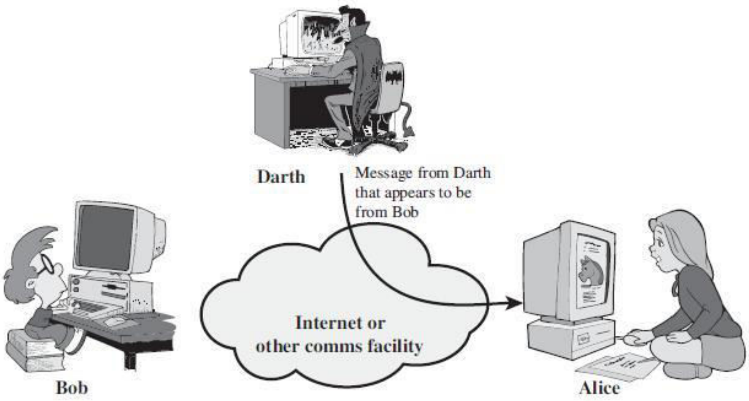
- Active attacks involve some modification of the data stream or the creation of a false stream
- detect and to recover from any disruption or delays caused by them
- can be subdivided into four categories:
  - masquerade,
  - replay,
  - modification of messages
  - denial of service

Masquerade

- one entity pretends to be a different entity
- usually includes one of the other forms of active attack

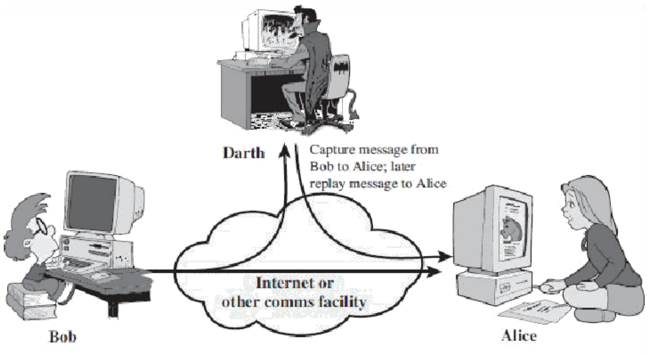
Example

- authentication sequences can be captured and replayed after a valid authentication sequence

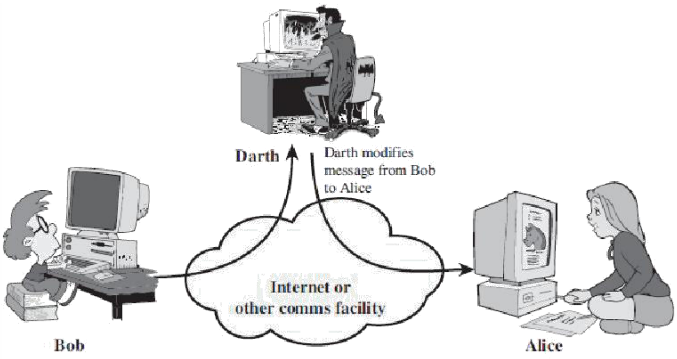

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Replay

- passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Modification Of Messages

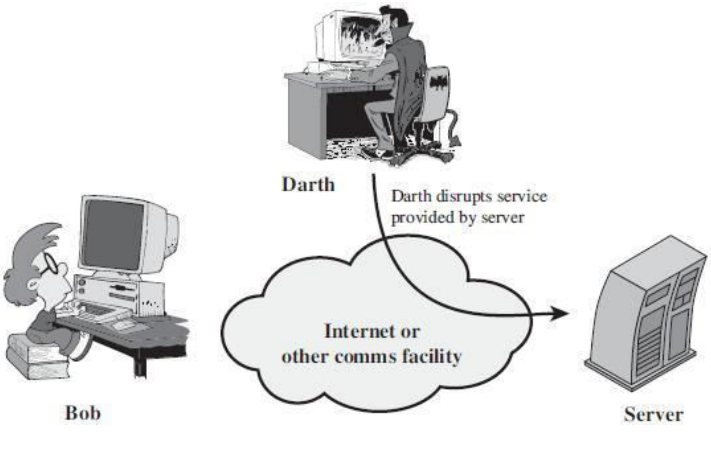
- some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect

Example

- a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

Denial Of Service

- prevents or inhibits the normal use or management of communications facilities
- may have a specific target; for example, an entity may suppress all messages directed to a particular destination
- disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

Security Services in X.800

- X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.
- RFC 2828, defines as a processing or communication service that is provided by a system to give a specific kind of protection to system resources;
  - security services implement security policies and are implemented by security mechanisms.

X.800

- divides these services into five categories and fourteen specific services

Authentication

- The assurance that the communicating entity is the one that it claims to be
- Two types
  - Peer Entity Authentication
  - Data-Origin Authentication

Access control

- The prevention of unauthorized use of a resource

Data confidentiality

- The protection of data from unauthorized disclosure.
- Four Types
  - Connection Confidentiality
  - Connectionless Confidentiality
  - Selective-Field Confidentiality
  - Traffic-Flow Confidentiality

Data integrity

- The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
- Five types
  - Connection Integrity with Recovery
  - Connection Integrity without Recovery
  - Selective-Field Connection Integrity
  - Connectionless Integrity
  - Selective-Field Connectionless Integrity

Nonrepudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication
- Two types
  - Nonrepudiation, Origin
  - Nonrepudiation, Destination

Security Mechanisms in X.800.

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required

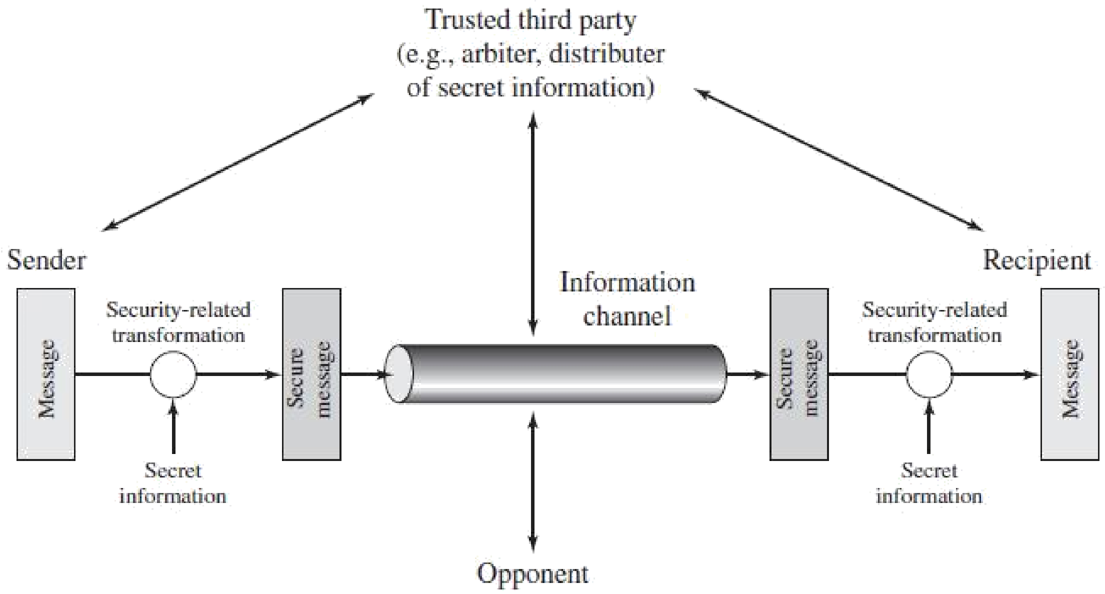
Specific security mechanisms:

- those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol
- encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

pervasive security mechanisms:

- trusted functionality, security labels, event detection, security audit trails, security recovery
- those that are not specific to any particular protocol layer or security service

Model for Network Security



- A message is to be transferred from one party to another across some sort of Internet service.
- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals

All the techniques for providing security have two components:

- A security-related transformation on the information to be sent.
  - Examples: encryption of the message, addition of a code based on the contents
- Some secret information shared by the two principals, unknown to the opponent o Example: encryption key used in conjunction with the transformation

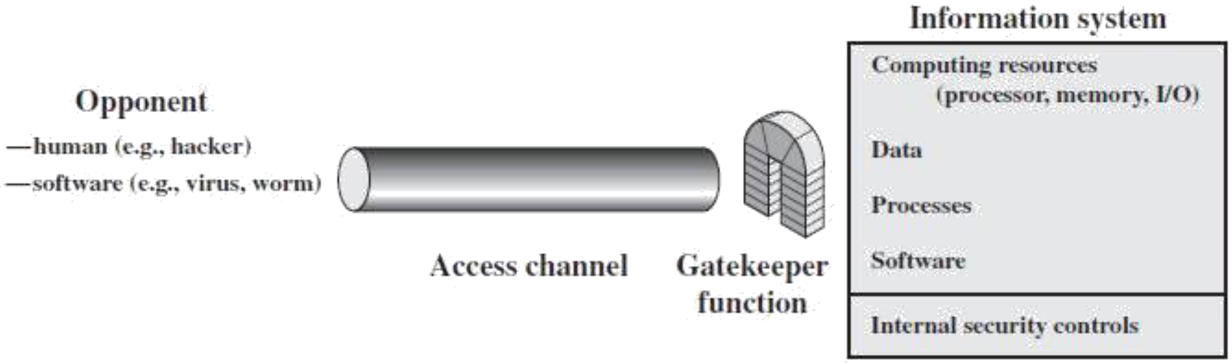
A trusted third party may be needed to achieve secure transmission.

- for distributing the secret information to the two principals
- to arbitrate disputes between the two principals concerning the authenticity of a message transmission

Four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation
   - such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service

Network Access Security Model



- protecting an information system from unwanted access from hacker, intruder
- hacker who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain
- placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers
  - Two kinds of threats:
  - **Information access threats**: Intercept or modify data on behalf of users who should not have access
  - **Service threats**: Exploit service flaws in computers to inhibit use by legitimate users
  - Examples: Viruses and worms, spread using disks & inserted over network

Classical Encryption Techniques

- Symmetric Cipher Model
  - Cryptanalysis and Brute-Force Attack
- Substitution Techniques
  - Caesar Cipher
  - Monoalphabetic Ciphers
  - Playfair Cipher
  - Hill Cipher
  - Polyalphabetic Ciphers
  - One-Time Pad
- Transposition Techniques
- Rotor Machines
- Steganography

Introduction

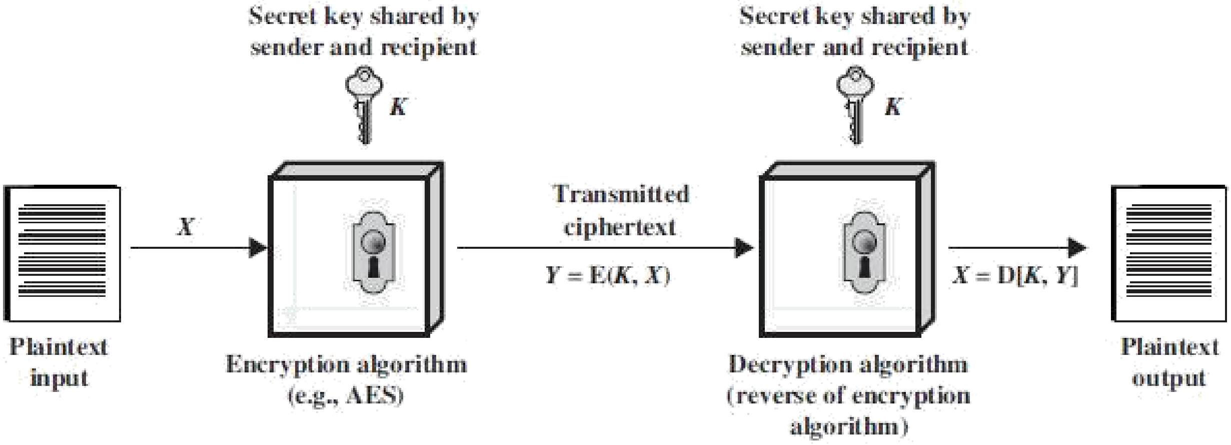
- **Symmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using the **same key**. It is also known as **conventional encryption**.
- Symmetric encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext.
- The two types of attack on an encryption algorithm are **cryptanalysis**,based on properties of the encryption algorithm, and **brute-force**, which involves trying all possible keys.
- Traditional (precomputer) symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into ciphertext elements. Transposition techniques systematically transpose the positions of plaintext elements.
- Rotor machines are sophisticated precomputer hardware devices that use substitution techniques.
- Steganography is a technique for hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message.
- An original message is known as the **plaintext**, while the coded message is called the **ciphertext**.
- The process of converting from plaintext to ciphertext is known as **enciphering or encryption**; restoring the plaintext from the ciphertext is **deciphering or decryption**.
- The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system or a cipher**.
- Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. **Cryptanalysis** is what the layperson calls “breaking the code.”The areas of cryptography and cryptanalysis together are called **cryptology**

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients

- Plaintext
- Encryption algorithm
  - performs various substitutions and transformations
- Secret key
  - another input to the encryption algorithm
  - a value independent of the plaintext and of the algorithm
- Ciphertext
  - For a given message, two different keys will produce two different ciphertexts
- Decryption algorithm
  - encryption algorithm run in reverse

Simplified Model of Symmetric Encryption


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Two requirements for secure use of conventional / symmetric encryption

- need a strong encryption algorithm
  - The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.
  - If someone can discover the key and knows the algorithm, all communication using this key is readable
  - do not need to keep the algorithm secret; we need to keep only the key secret
  - the principal security problem is maintaining the secrecy of the key

Model of Symmetric Cryptosystem

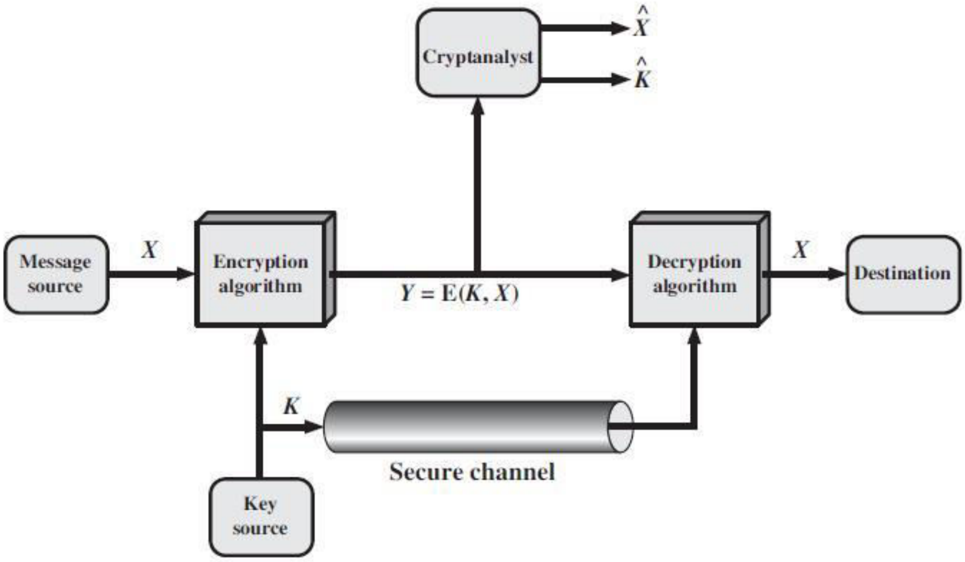
Plain Text: $X = [X_1, X_2, . . , X_M]$

Key: $K = [K_1, K_2, . . , K_J]$

Cipher text $Y = [Y_1, Y_2, . . , Y_N]$

$Y = E(K, X)$

$X = D(K, Y)$



Cryptanalysis and Brute-Force Attack

Cryptanalysis

- Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs.
- This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst

Type of Attack	Known to Cryptanalyst
• Ciphertext Only • Known Plaintext • Chosen Plaintext • Chosen Ciphertext • Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Two schemes

- **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
- **computationally secure**
  - meets either of the following criteria:
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.

Brute-force attack

- The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.

Cryptographic systems characterization

Three independent dimensions

- The type of operations used for transforming plaintext to ciphertext.
  - **substitution**
    - each element is mapped into another element
  - **transposition**
    - elements are rearranged
  - product systems, involve multiple stages of substitutions and transpositions
- The number of keys used
  - If both sender and receiver use the same key, the system is referred to as **symmetric**, single-key, secret-key, or conventional encryption.
  - If the sender and receiver use different keys, the system is referred to as **asymmetric**, two-key, or public-key encryption
- The way in which the plaintext is processed.
  - A **block cipher** processes the input one block of elements at a time, producing an output block for each
  - input block.
  - A **stream cipher** processes the input elements continuously, producing output one element at a time, as it goes along

Substitution Techniques

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Julius Caesar Cipher

- replacing each letter of the alphabet with the letter standing three places further down the alphabet
- alphabet is wrapped around, so that the letter following Z is A

can define transformation as:

a b c d e f g h i j k l m n o p q r s t u v w x y z D

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

mathematically give each letter a number

a b c d e f g h i j k l m n o p q r s t u v w x y z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

then have Caesar cipher as:

$c = E(p) = (p + k) \bmod (26)$ p

$= D(c) = (c - k) \bmod (26)$

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
- A maps to A,B,..Z
- could simply try each in turn
- a brute force search
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext

Monoalphabetic Ciphers

- rather than just shifting the alphabet shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long
- the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than $4x10^{26}$ possible keys.
- This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis
- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet
- A countermeasure is to provide multiple substitutes, known as **homophones**, for a single letter.
- For example, the letter e could be assigned a number of different cipher symbols, such as 16, 74, 35, and 21, with each homophone assigned to a letter in rotation or randomly

Language Redundancy and Cryptanalysis

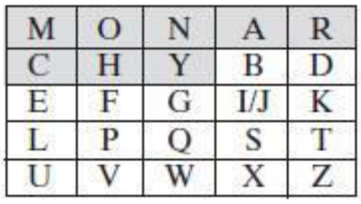
- human languages are redundant
- eg "th lrd s m shphrd shll nt wnt"
- letters are not equally commonly used
- in English E is by far the most common letter
- followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages
- two-letter combinations, known as **digrams** (ex: th)

Playfair Cipher

- best-known multiple-letter encryption cipher
- treats digrams in the plaintext as single units and translates these units into ciphertext digrams

Playfair Key Matrix

- 5 × 5 matrix of letters constructed using a keyword
- filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom,
- filling in the remainder matrix with the remaining letters in alphabetic order.
- The letters I and J count as one letter
- Example matrix using the keyword MONARCHY



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

Plaintext is encrypted two letters at a time, according to the following rules

- Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x,
  - Ex: balloon would be treated as ba lx lo on.
- Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
  - Ex: ar is encrypted as RM.
- Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
  - Ex: mu is encrypted as CM.
- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.
  - Ex: hs becomes BP and ea becomes IM (or JM, as the encipherer wishes)

Example

Given the key MONARCHY apply Play fair cipher to plain text “FACTIONALISM”

Solution

(p) FA CT IO NA LI SM

(c) IO DL FA AR SE LA

(d) FA CT IO NA LI SM

Security of Playfair Cipher

- security much improved over monoalphabetic since have 26 x 26 = 676 digrams
- would need a 676 entry frequency table to analyse and correspondingly more ciphertext
- was widely used for many years eg. by US & British military in WW1
- it can be broken, given a few hundred letters since still has much of plaintext structure

Hill Cipher

Findin

3x3 Matrix $\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$

$|A| = k_{11}k_{22}k_{33} - k_{11}k_{23}k_{32} - k_{12}k_{21}k_{33} + k_{12}k_{23}k_{31} + k_{13}k_{21}k_{32} - k_{13}k_{22}k_{31}$

Example:

$$\det\begin{pmatrix}5 & 8\\ 17 & 3\end{pmatrix} = (5 \times 3) - (8 \times 17) = -121 \bmod 26 = 9$$

We can show that $9^{-1} \bmod 26 = 3$, because $9 \times 3 = 27 \bmod 26 = 1$ (see Chapter 4 or Appendix E). Therefore, we compute the inverse of **A** as

$$\mathbf{A} = \begin{pmatrix}5 & 8\\ 17 & 3\end{pmatrix}$$

$$\mathbf{A}^{-1} \bmod 26 = 3\begin{pmatrix}3 & -8\\ -17 & 5\end{pmatrix} = 3\begin{pmatrix}3 & 18\\ 9 & 5\end{pmatrix} = \begin{pmatrix}9 & 54\\ 27 & 15\end{pmatrix} = \begin{pmatrix}9 & 2\\ 1 & 15\end{pmatrix}$$

The Hill algorithm

- This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters.
- The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, . , z = 25)
- For m = 3, the system can be described as

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

This can be expressed in terms of row vectors and matrices:

$$(c_1\ c_2\ c_3) = (p\ \ p_2\ p_3)\begin{pmatrix}k_{11} & k_{12} & k_{13}\\ k_{21} & k_{22} & k_{23}\\ k_{31} & k_{32} & k_{33}\end{pmatrix} \bmod 26$$

or

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

- where C and P are row vectors of length 3 representing the plaintext and ciphertext, and K is a 3x3 matrix representing the encryption key.
- Operations are performed mod 26.
- In general terms, the Hill system can be expressed as

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

Example

Encrypt the message “meet me at the usual place at ten rather than eight oclock” using the Hill cipher with the key ( ). Show your calculations and the result.Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

1) mathematically give each letter a number

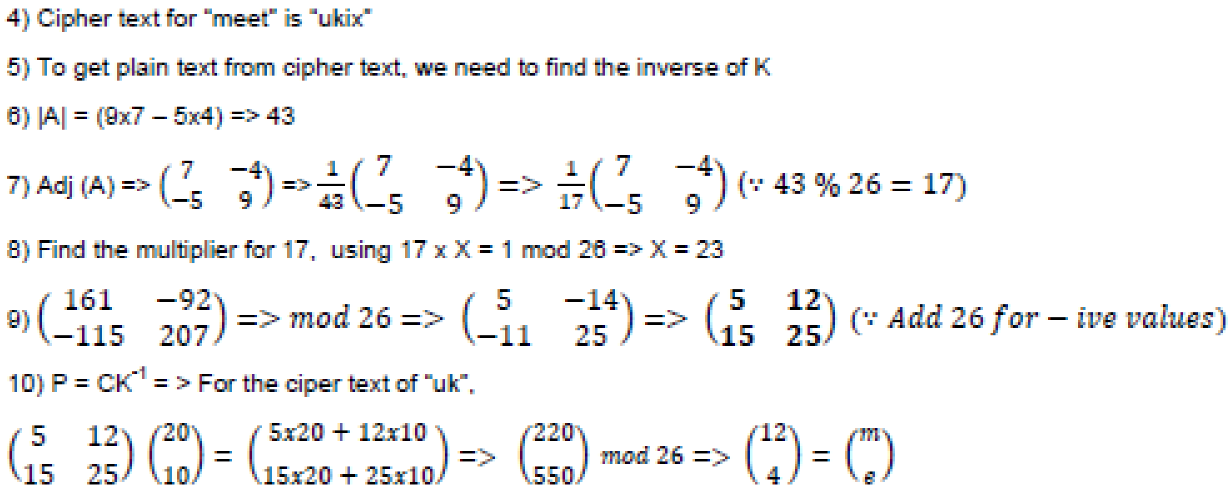
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2) 1^{st} pair from plain text "me" => $\begin{pmatrix}12\\ 4\end{pmatrix}$

$$\begin{pmatrix}9 & 4\\ 5 & 7\end{pmatrix}\begin{pmatrix}12\\ 4\end{pmatrix} => \begin{pmatrix}9x12 + 4x4\\ 5x12 + 7x4\end{pmatrix} = \begin{pmatrix}124\\ 88\end{pmatrix} => mod\ 26 => \begin{pmatrix}20\\ 10\end{pmatrix} => \begin{pmatrix}u\\ k\end{pmatrix}$$

3) 2^{nd} pair fro plain text "et"

$$\begin{pmatrix}9 & 4\\ 5 & 7\end{pmatrix}\begin{pmatrix}4\\ 19\end{pmatrix} => \begin{pmatrix}9x4 + 4x19\\ 5x4 + 7x19\end{pmatrix} = \begin{pmatrix}112\\ 153\end{pmatrix} => mod\ 26 => \begin{pmatrix}8\\ 23\end{pmatrix} => \begin{pmatrix}i\\ x\end{pmatrix}$$



4) Cipher text for "meet" is "ukix"

5) To get plain text from cipher text, we need to find the inverse of K

6) |A| = (9x7 – 5x4) => 43

7) Adj (A) => $\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$ => $\frac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$ $=> \frac{1}{17}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\because 43 \% 26 = 17)$

8) Find the multiplier for 17, using 17 x X = 1 mod 26 => X = 23

9) $\begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix} => mod\ 26 => \begin{pmatrix} 5 & -14 \\ -11 & 25 \end{pmatrix} => \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} (\because Add\ 26\ for - ive\ values)$

10) P = CK^{-1} = > For the ciper text of "uk",

$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \begin{pmatrix} 20 \\ 10 \end{pmatrix} = \begin{pmatrix} 5x20 + 12x10 \\ 15x20 + 25x10 \end{pmatrix} => \begin{pmatrix} 220 \\ 550 \end{pmatrix} mod\ 26 => \begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} m \\ e \end{pmatrix}$

Hence the plain text is “me”

Polyalphabetic Ciphers

- use different monoalphabetic substitutions as one proceeds through the plaintext message.
- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- general name for this approach is **polyalphabetic substitution cipher**
- has the following features in common:
  - A set of related monoalphabetic substitution rules is used.
  - A key determines which particular rule is chosen for a given transformation.

One-Time Pad

- improvement to the Vernam cipher that yields the ultimate in security
- using a random key that is as long as the message, so that the key need not be repeated
- the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message

Example

```
ciphertext:ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key:       pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih

plaintext: mr mustard with the candlestick in the hall

ciphertext:ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key:       mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt

plaintext: miss scarlet with the knife in the library
```

two fundamental difficulties

- problem of making large quantities of random keys
- problem of key distribution and protection

Transposition Techniques

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters

Rail Fence Technique

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

The encrypted message is

```
MEMATRHTGPRYETEFETEOAAT
```

Pure Transposition Cipher

write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

The order of the columns then becomes the key to the algorithm

Example

```
Key:         4 3 1 2 5 6 7
Plaintext: a t t a c k p
           o s t p o n e
           d u n t i l t
           w o a m x y z
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Double Transposition

performing more than one stage of transposition

Example

if the foregoing message is reencrypted using the same algorithm

```
Key:       4 3 1 2 5  6 7
Input:     t t n a a p t
           m t s u o a o
           d w c o i x k
           n l y p e t z
Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

This is a much less structured permutation and is much more difficult to cryptanalyze

Rotor Machines (Skip)

The machine consists of a set of independently rotating cylinders through which electrical pulses can flow.

Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin

Steganography

A plaintext message may be hidden in one of two ways.

- The methods of steganography conceal the existence of the message
- The methods of cryptography render the message unintelligible to outsiders ○ by various transformations of the text

Various ways to conceal the message

arrangement of words or letters within an apparently innocuous text spells out the real message

Character marking

Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Invisible ink

A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied

Pin punctures

Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon

Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

hiding a message by using the least significant bits of frames on a CD

- the Kodak Photo CD format's maximum resolution is 2048 by 3072 pixels, with each pixel containing 24 bits of RGB color information.
- The least significant bit of each 24-bit pixel can be changed without greatly affecting the quality of the image
- Thus you can hide a 2.3-megabyte message in a single digital snapshot

Number of drawbacks

- lot of overhead to hide a relatively few bits of information
- once the system is discovered, it becomes virtually worthless
- the insertion method depends on some sort of key
  - Alternatively, a message can be first encrypted and then hidden using steganography

Advantage of steganography

- can be employed by parties who have something to lose should the fact of their secret communication be discovered
- Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide

FINITE FIELDS AND NUMBER THEORY

Number Theory concepts

Divisibility and The Division Algorithm

Divisibility

- We say that a nonzero b **divides** a if a = mb for some m, where a, b and m are integers.
- That is, b divides a, if there is no remainder on division.
- The notation b|a is commonly used to mean b divides a.
- If b|a, we say that b is a **divisor** of a.

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
$13|182;\ -5|30;\ 17|289;\ -3|33;\ 17|0$

Properties of divisibility for integers

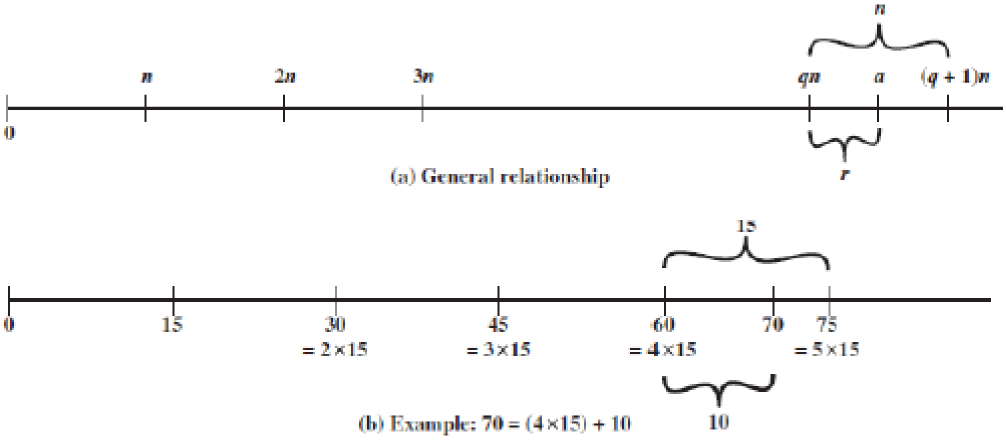
- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $a|b$ and $b|c$, then $a|c$: $11|66$ and $66|198 = 11|198$
- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n.

The Division Algorithm

Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient an integer remainder r that obey the following relationship: The remainder r is often referred to as a residu

$$a = qn + r \qquad 0 \le r < n;\ q = \lfloor a/n \rfloor$$

where $\lfloor x \rfloor$ is the largest integer less than or equal to x.



(a) General relationship

(b) Example: 70 = (4×15) + 10

Primality

Prime Numbers

- An integer p > 1 is prime number, if its divisors are +/- 1 and +/1 p
- Any non negative integer a > 1 can be factored in the form as $a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$
- where p1 < p2 < ... < pt are prime numbers and where each a is a positive integer.
- This is known as the fundamental theorem of arithmetic
- Examples: 91 = 7 x 13, 3600 = 24 x 32 x 52

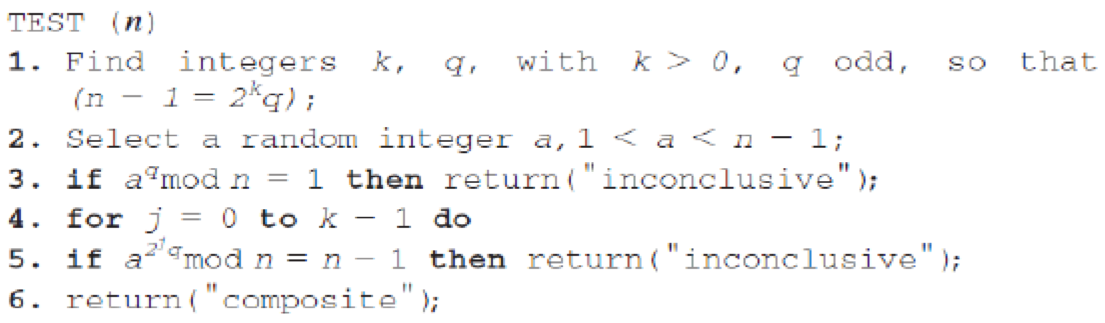
Miller-Rabin Algorithm

- also known as Rabin-Miller algorithm, or the Rabin-Miller test, or the Miller-Rabin test
- typically used to test a large number for primality

Two Properties of Prime Numbers

- If p is prime and a is a positive integer less than p, then a^2 mod p = 1, if and only if either a mod p = 1 or a mod p = -1 mod p = p – 1
- Let p be a prime number greater than 2. We can then write p - 1 = 2^kq with k > 0, q odd

Algorithm



```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   ($n - 1 = 2^k q$);
2. Select a random integer a, $1 < a < n - 1$;
3. if $a^q \bmod n = 1$ then return("inconclusive");
4. for $j = 0$ to $k - 1$ do
5. if $a^{2^j q} \bmod n = n - 1$ then return("inconclusive");
6. return("composite");
```

Chinese Remainder Theorem

the CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli

Formula

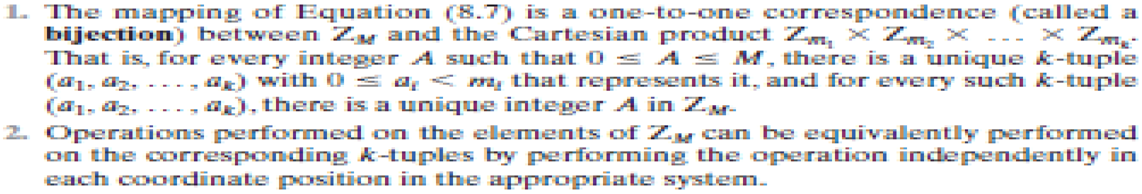
$$M = \prod_{i=1}^{k} m_i$$

where the m_i are pairwise relatively prime; that is, $\gcd(m_i, m_j) = 1$ for $1 \leq i, j \leq k$, and $i \neq j$.

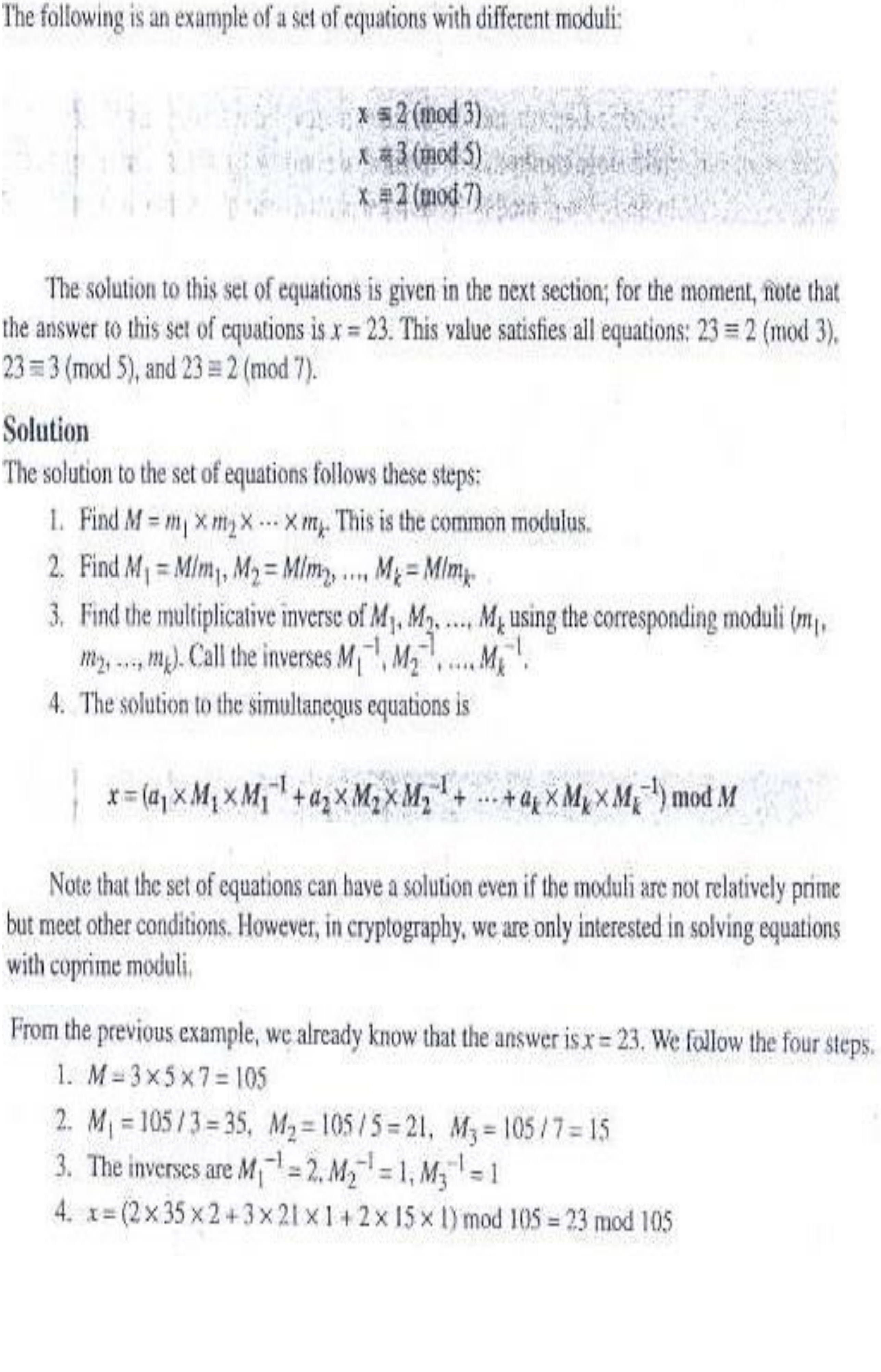
Relatively Prime

- Two integers are relatively prime, if their only common positive integer factor is 1
- **Example:** 8, 15 are relatively prime because positive divisors of 8 are 1, 2, 4, 8. Positive divisors of 15 are 1, 3, 5, 15. Common positive factor = 1

TWO ASSERTION OF CRT



1. The mapping of Equation (8.7) is a one-to-one correspondence (called a **bijection**) between Z_M and the Cartesian product $Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}$. That is, for every integer A such that $0 \leq A \leq M$, there is a unique k-tuple $(a_1, a_2, \ldots, a_k)$ with $0 \leq a_i < m_i$ that represents it, and for every such k-tuple $(a_1, a_2, \ldots, a_k)$, there is a unique integer A in Z_M.
2. Operations performed on the elements of Z_M can be equivalently performed on the corresponding k-tuples by performing the operation independently in each coordinate position in the appropriate system.



The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is $x = 23$. This value satisfies all equations: $23 \equiv 2 \pmod 3$, $23 \equiv 3 \pmod 5$, and $23 \equiv 2 \pmod 7$.

Solution

The solution to the set of equations follows these steps:

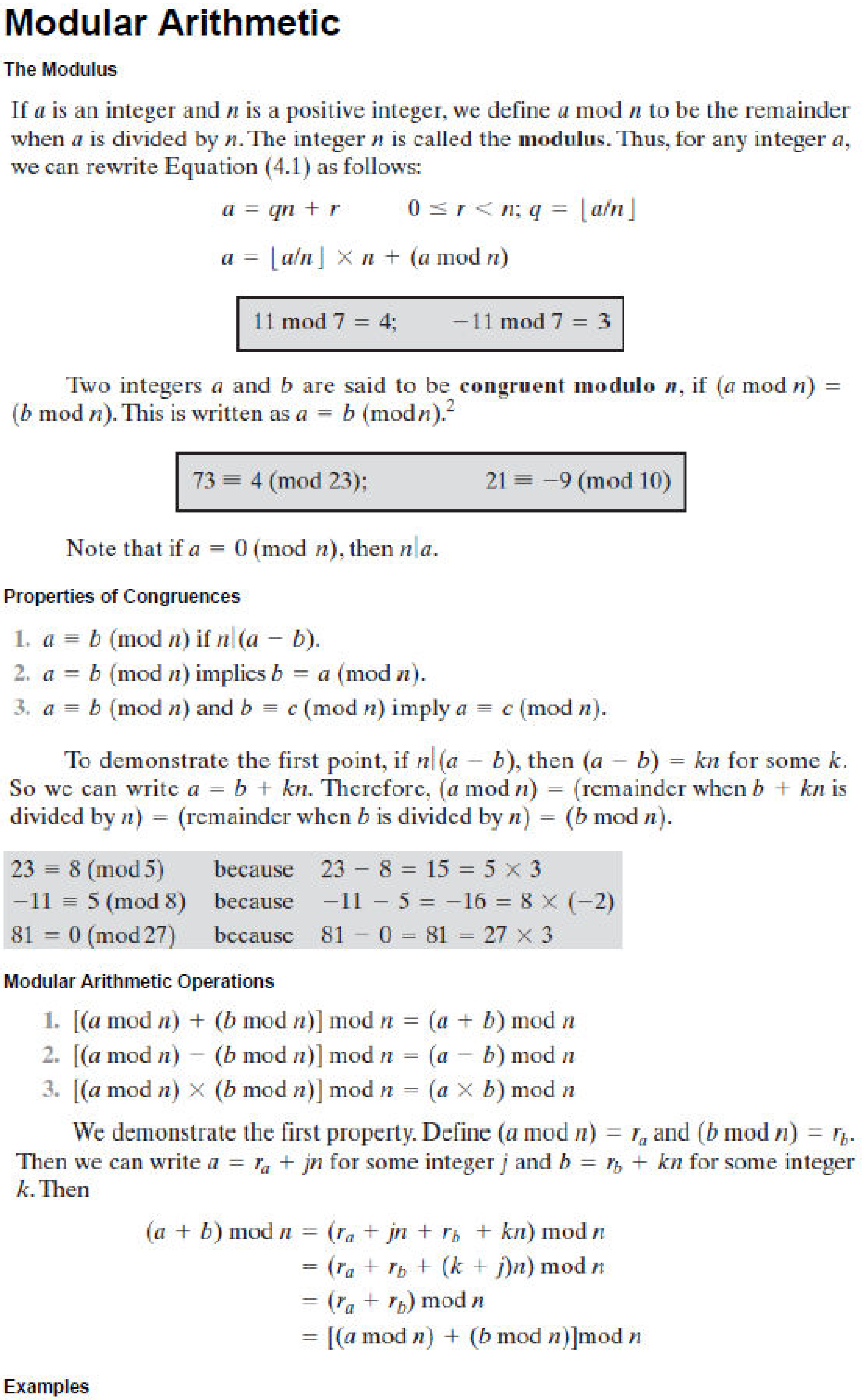
1. Find $M = m_1 \times m_2 \times \cdots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, ..., $M_k = M/m_k$.
3. Find the multiplicative inverse of $M_1, M_2, \ldots, M_k$ using the corresponding moduli ($m_1, m_2, \ldots, m_k$). Call the inverses $M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}$.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Note that the set of equations can have a solution even if the moduli are not relatively prime but meet other conditions. However, in cryptography, we are only interested in solving equations with coprime moduli.

From the previous example, we already know that the answer is $x = 23$. We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$
3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$



Modular Arithmetic

The Modulus

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the **modulus**. Thus, for any integer a, we can rewrite Equation (4.1) as follows:

$$a = qn + r \qquad 0 \le r < n;\ q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$

Two integers a and b are said to be **congruent modulo** $\boldsymbol{n}$, if $(a \bmod n) = (b \bmod n)$. This is written as $a = b \pmod n$.[2]

$73 \equiv 4 \pmod{23}; \qquad 21 \equiv -9 \pmod{10}$

Note that if $a = 0 \pmod n$, then $n \mid a$.

Properties of Congruences

1. $a = b \pmod n$ if $n \mid (a - b)$.
2. $a = b \pmod n$ implies $b = a \pmod n$.
3. $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$.

To demonstrate the first point, if $n \mid (a - b)$, then $(a - b) = kn$ for some k. So we can write $a = b + kn$. Therefore, $(a \bmod n) =$ (remainder when $b + kn$ is divided by n) $=$ (remainder when b is divided by n) $= (b \bmod n)$.

$23 \equiv 8 \pmod 5$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \pmod 8$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 = 0 \pmod{27}$	because	$81 - 0 = 81 = 27 \times 3$

Modular Arithmetic Operations

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

We demonstrate the first property. Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$. Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k. Then

$$\begin{aligned}(a + b) \bmod n &= (r_a + jn + r_b + kn) \bmod n \\ &= (r_a + r_b + (k + j)n) \bmod n \\ &= (r_a + r_b) \bmod n \\ &= [(a \bmod n) + (b \bmod n)]\bmod n\end{aligned}$$

Examples

$11 \bmod 8 = 3;\ 15 \bmod 8 = 7$
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$
$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$
$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$
$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 = 4 \pmod{13}$$
$$11^4 = (11^2)^2 = 4^2 = 3 \pmod{13}$$
$$11^7 = 11 \times 4 \times 3 = 132 = 2 \pmod{13}$$

Properties of Modular Arithmetic

set of residues, or residue classes (mod n)

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n - 1)\}$$

precise, each integer in Z_n represents a residue class. We can label the residue classes (mod n) as $[0], [1], [2], \ldots, [n - 1]$, where

$$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$$

The residue classes (mod 4) are

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

reducing k modulo n.

Finding the smallest nonnegative integer to which k is congruent modulo n

if $(a + b) = (a + c) \pmod{n}$ **then** $b = c \pmod{n}$

$(5 + 23) = (5 + 7) \pmod{8};\ 23 = 7 \pmod{8}$

if $(a \times b) = (a \times c) \pmod{n}$ **then** $b = c \pmod{n}$ **if** a **is relatively prime to** n

Properties of Modular Arithmetic for Integers in Zn

Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n - (x + w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n - [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a a z such that $w + z = 0 \bmod n$

Table 4.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

GROUPS, RINGS AND FIELDS

Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra. In abstract algebra, we are concerned with sets on whose elements we can operate algebraically; that is, we can combine two elements of the set, perhaps in several ways, to obtain a third element of the set. These operations are subject to specific rules, which define the nature of the set. By convention, the notation for the two principal classes of operations on set elements is usually the same as the notation for addition and multiplication on ordinary numbers. However, it is important to note that, in abstract algebra, we are not limited to ordinary arithmetical operations. All this should become clear as we proceed.

Groups

A **group** G, sometimes denoted by $\{G, \cdot\}$, is a set of elements with a binary operation denoted by $\cdot$ that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G, such that the following axioms are obeyed:[4]

(A1) Closure:	If a and b belong to G, then $a \cdot b$ is also in G.
(A2) Associative:	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G.
(A3) Identity element:	There is an element e in G such that $a \cdot e = e \cdot a = a$ for all a in G.
(A4) Inverse element:	For each a in G, there is an element a' in G such that $a \cdot a' = a' \cdot a = e$.

If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**.

A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G.

> The set of integers (positive, negative, and 0) under addition is an abelian group. The set of nonzero real numbers under multiplication is an abelian group. The set S_n from the preceding example is a group but not an abelian group for $n > 2$.

When the group operation is addition, the identity element is 0; the inverse element of a is $-a$; and subtraction is defined with the following rule: $a - b = a + (-b)$.

Cyclic Group We define exponentiation within a group as a repeated application of the group operator, so that $a^3 = a \cdot a \cdot a$. Furthermore, we define $a^0 = e$ as the identity element, and $a^{-n} = (a')^n$, where a' is the inverse element of a within the group. A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic group is always abelian and may be finite or infinite.

> The additive group of integers is an infinite cyclic group generated by the element 1. In this case, powers are interpreted additively, so that n is the nth power of 1.

Rings

A **ring** R, sometimes denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*,[6] such that for all a, b, c in R the following axioms are obeyed.

(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.

(M1) Closure under multiplication:	If a and b belong to R, then ab is also in R.
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in R.
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in R. $(a + b)c = ac + bc$ for all a, b, c in R.

In essence, a ring is a set in which we can do addition, subtraction $[a - b = a + (-b)]$, and multiplication without leaving the set.

> With respect to addition and multiplication, the set of all n-square matrices over the real numbers is a ring.

A ring is said to be **commutative** if it satisfies the following additional condition:

(M4) Commutativity of multiplication: $ab = ba$ for all a, b in R.

> Let S be the set of even integers (positive, negative, and 0) under the usual operations of addition and multiplication. S is a commutative ring. The set of all n-square matrices defined in the preceding example is not a commutative ring.
>
> The set Z_n of integers $\{0, 1, \ldots, n - 1\}$, together with the arithmetic operations modulo n, is a commutative ring (Table 4.3).

Next, we define an **integral domain**, which is a commutative ring that obeys the following axioms.

(M5) Multiplicative identity: There is an element 1 in R such that $a1 = 1a = a$ for all a in R.

(M6) No zero divisors: If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.

> Let S be the set of integers, positive, negative, and 0, under the usual operations of addition and multiplication. S is an integral domain.

Fields

A **field** F, sometimes denoted by $\{F, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a, b, c in F the following axioms are obeyed.

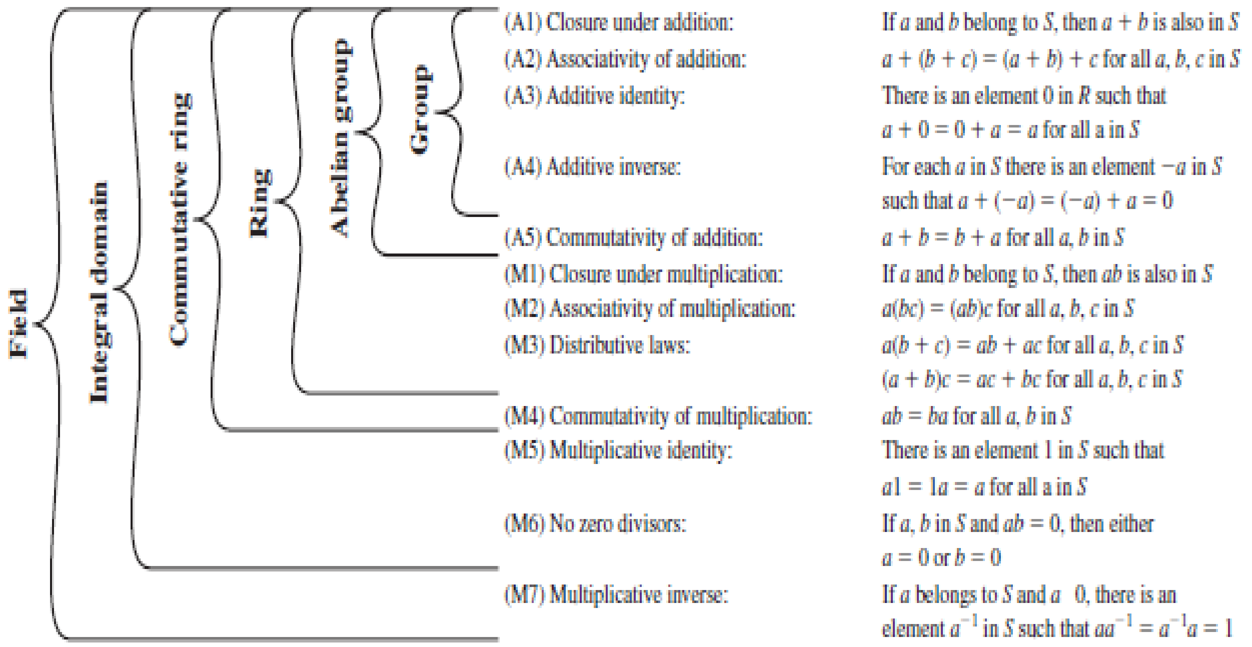
(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

In essence, a field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with the following rule: $a/b = a(b^{-1})$.

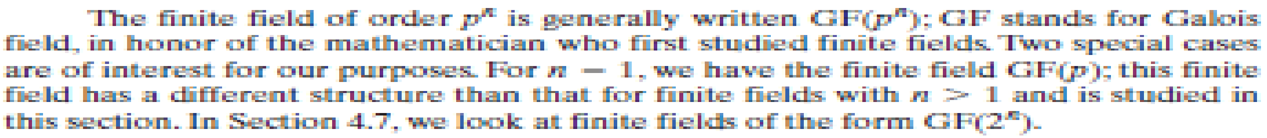
> Familiar examples of fields are the rational numbers, the real numbers, and the complex numbers. Note that the set of all integers is not a field, because not every element of the set has a multiplicative inverse; in fact, only the elements 1 and –1 have multiplicative inverses in the integers.

Figure 4.2 summarizes the axioms that define groups, rings, and fields.

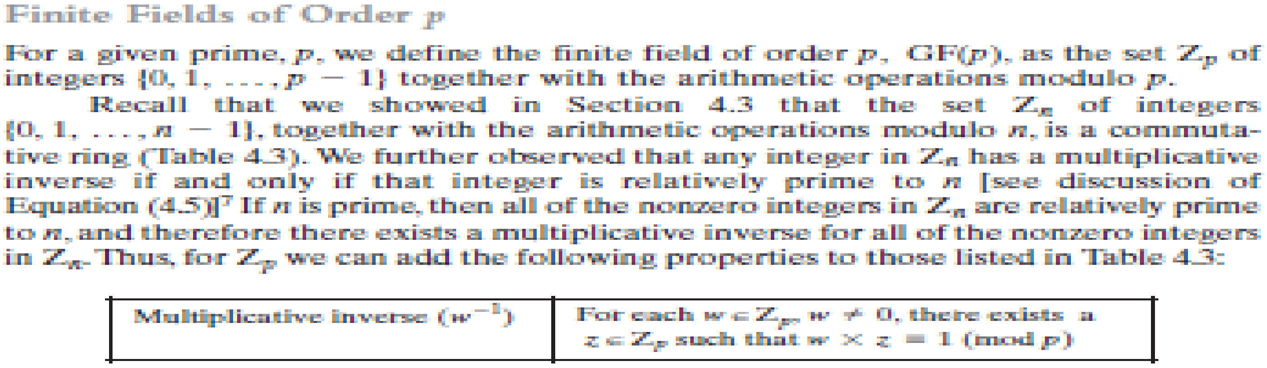


(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

FINITE FIELDS OF THE FORM GF(p)



The finite field of order p^n is generally written GF(p^n); GF stands for Galois field, in honor of the mathematician who first studied finite fields. Two special cases are of interest for our purposes. For $n = 1$, we have the finite field GF(p); this finite field has a different structure than that for finite fields with $n > 1$ and is studied in this section. In Section 4.7, we look at finite fields of the form GF(2^n).

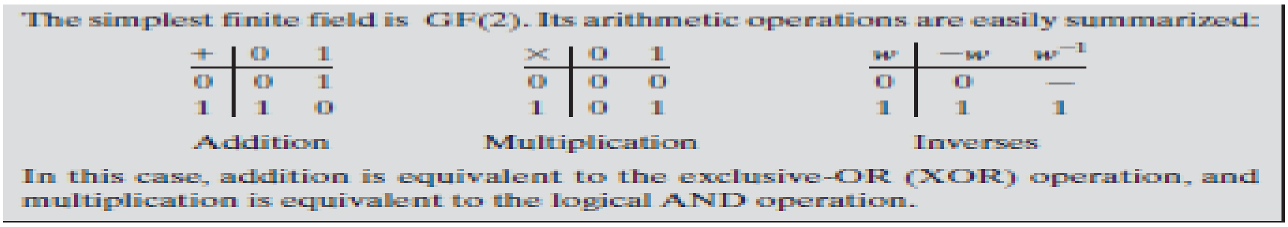


Finite Fields of Order p

For a given prime, p, we define the finite field of order p, GF(p), as the set Z_p of integers $\{0, 1, \ldots, p - 1\}$ together with the arithmetic operations modulo p.

Recall that we showed in Section 4.3 that the set Z_n of integers $\{0, 1, \ldots, n - 1\}$, together with the arithmetic operations modulo n, is a commutative ring (Table 4.3). We further observed that any integer in Z_n has a multiplicative inverse if and only if that integer is relatively prime to n [see discussion of Equation (4.5)][7] If n is prime, then all of the nonzero integers in Z_n are relatively prime to n, and therefore there exists a multiplicative inverse for all of the nonzero integers in Z_n. Thus, for Z_p we can add the following properties to those listed in Table 4.3:

Multiplicative inverse (w^{-1})	For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod{p}$



The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

+	0	1
0	0	1
1	1	0

Addition

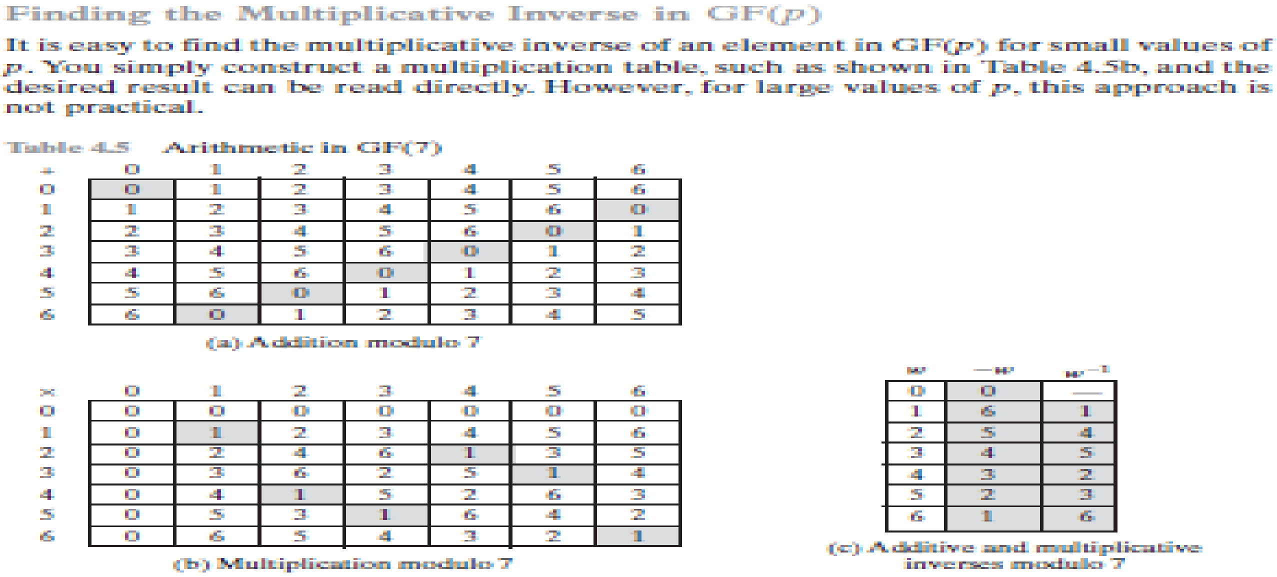
×	0	1
0	0	0
1	0	1

Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1

Inverses

In this case, addition is equivalent to the exclusive-OR (XOR) operation, and multiplication is equivalent to the logical AND operation.



Finding the Multiplicative Inverse in GF(p)

It is easy to find the multiplicative inverse of an element in GF(p) for small values of p. You simply construct a multiplication table, such as shown in Table 4.5b, and the desired result can be read directly. However, for large values of p, this approach is not practical.

Table 4.5 Arithmetic in GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

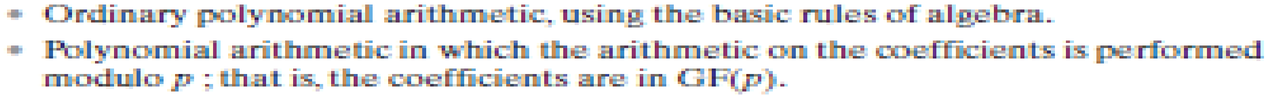
(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

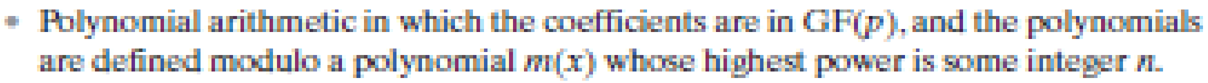
(c) Additive and multiplicative inverses modulo 7

POLYNOMIAL ARITHMETIC

Three classes of polynomial arithmetic:



- Ordinary polynomial arithmetic, using the basic rules of algebra.
- Polynomial arithmetic in which the arithmetic on the coefficients is performed modulo p ; that is, the coefficients are in GF(p).



- Polynomial arithmetic in which the coefficients are in GF(p), and the polynomials are defined modulo a polynomial $m(x)$ whose highest power is some integer n.

$$\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
+ \quad (x^2 - x + 1) \\
\hline
x^3 + 2x^2 - x + 3
\end{array}$$

(a) Addition

$$\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
- \quad (x^2 - x + 1) \\
\hline
x^3 \qquad + x + 1
\end{array}$$

(b) Subtraction

$$\begin{array}{rrrr}
 & x^3 + x^2 & & + 2 \\
 & \times \quad (x^2 - & x + & 1) \\
\hline
 & x^3 + x^2 & & + 2 \\
 -x^4 - x^3 & & -2x & \\
 x^5 + x^4 & & +2x^2 & \\
\hline
 x^5 & & +3x^2 - 2x & + 2
\end{array}$$

(c) Multiplication

$$\begin{array}{r}
x + 2 \\
x^2 - x + 1 \,\big)\, \overline{x^3 + x^2 \qquad + 2} \\
\underline{x^3 - x^2 + x \qquad\quad} \\
2x^2 - x + 2 \\
\underline{2x^2 - 2x + 2} \\
x
\end{array}$$

(d) Division

Figure 4.3 Examples of Polynomial Arithmetic

A polynomial $f(x)$ over a field F is called **irreducible** if and only if $f(x)$ cannot be expressed as a product of two polynomials, both over F, and both of degree lower than that of $f(x)$. By analogy to integers, an irreducible polynomial is also called a **prime polynomial**.

The polynomial[9] $f(x) = x^4 + 1$ over GF(2) is reducible, because

$$x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1).$$

Consider the polynomial $f(x) = x^3 + x + 1$. It is clear by inspection that x is not a factor of $f(x)$. We easily show that $x + 1$ is not a factor of $f(x)$:

$$\begin{array}{r}
x^2 + x \qquad\qquad \\
x + 1 \,\big)\, \overline{x^3 \qquad + x + 1} \\
\underline{x^3 + x^2 \qquad\qquad} \\
x^2 + x \qquad \\
\underline{x^2 + x} \qquad \\
1
\end{array}$$

Thus, $f(x)$ has no factors of degree 1. But it is clear by inspection that if $f(x)$ is reducible, it must have one factor of degree 2 and one factor of degree 1. Therefore, $f(x)$ is irreducible.

$$\begin{array}{r}
x^7 \qquad + x^5 + x^4 + x^3 \qquad + x + 1 \\
+ \,(x^3 \qquad + x + 1) \\
\hline
x^7 \qquad + x^5 + x^4 \qquad\qquad\qquad\qquad
\end{array}$$

(a) Addition

$$\begin{array}{r}
x^7 \qquad + x^5 + x^4 + x^3 \qquad + x + 1 \\
- \,(x^3 \qquad + x + 1) \\
\hline
x^7 \qquad + x^5 + x^4 \qquad\qquad\qquad\qquad
\end{array}$$

(b) Subtraction

$$\begin{array}{rrrrr}
 & x^7 & + x^5 + x^4 + x^3 & & + x + 1 \\
 & & \times \,(x^3 & & + x + 1) \\
\hline
 & x^7 & + x^5 + x^4 + x^3 & & + x + 1 \\
 & x^8 & + x^6 + x^5 + x^4 & + x^2 + x & \\
 x^{10} & + x^8 + x^7 + x^6 & + x^4 + x^3 & & \\
\hline
 x^{10} & & + x^4 & + x^2 & + 1
\end{array}$$

(c) Multiplication

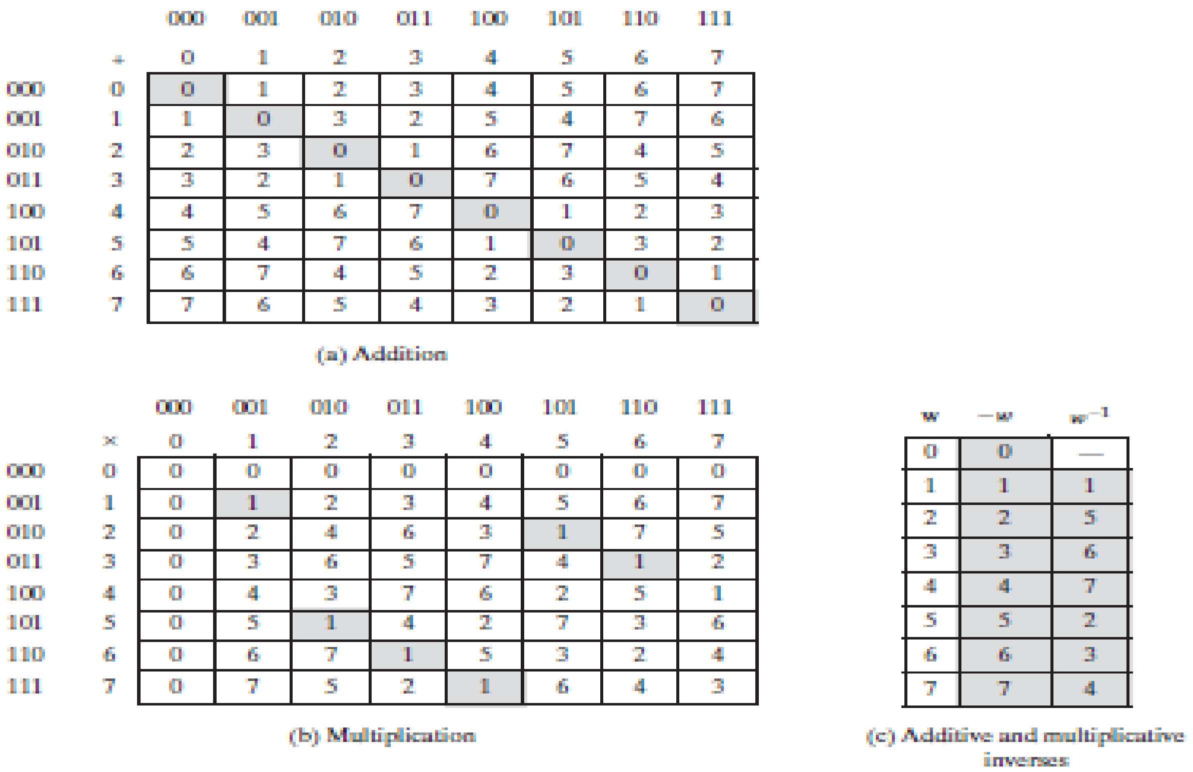
$$\begin{array}{r}
x^4 + 1 \qquad\qquad\qquad\qquad\qquad\qquad \\
x^3 + x + 1 \,\big)\, \overline{x^7 \qquad + x^5 + x^4 + x^3 \qquad + x + 1} \\
\underline{x^7 \qquad + x^5 + x^4} \qquad\qquad\qquad\qquad \\
x^3 \qquad + x + 1 \\
\underline{x^3 \qquad + x + 1}
\end{array}$$

(d) Division

Figure 4.4 Examples of Polynomial Arithmetic over GF(2)

FINITE FIELDS OF THE FORM GF(2$^{n)}$

Table 4.6 Arithmetic in GF(2^3)



		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

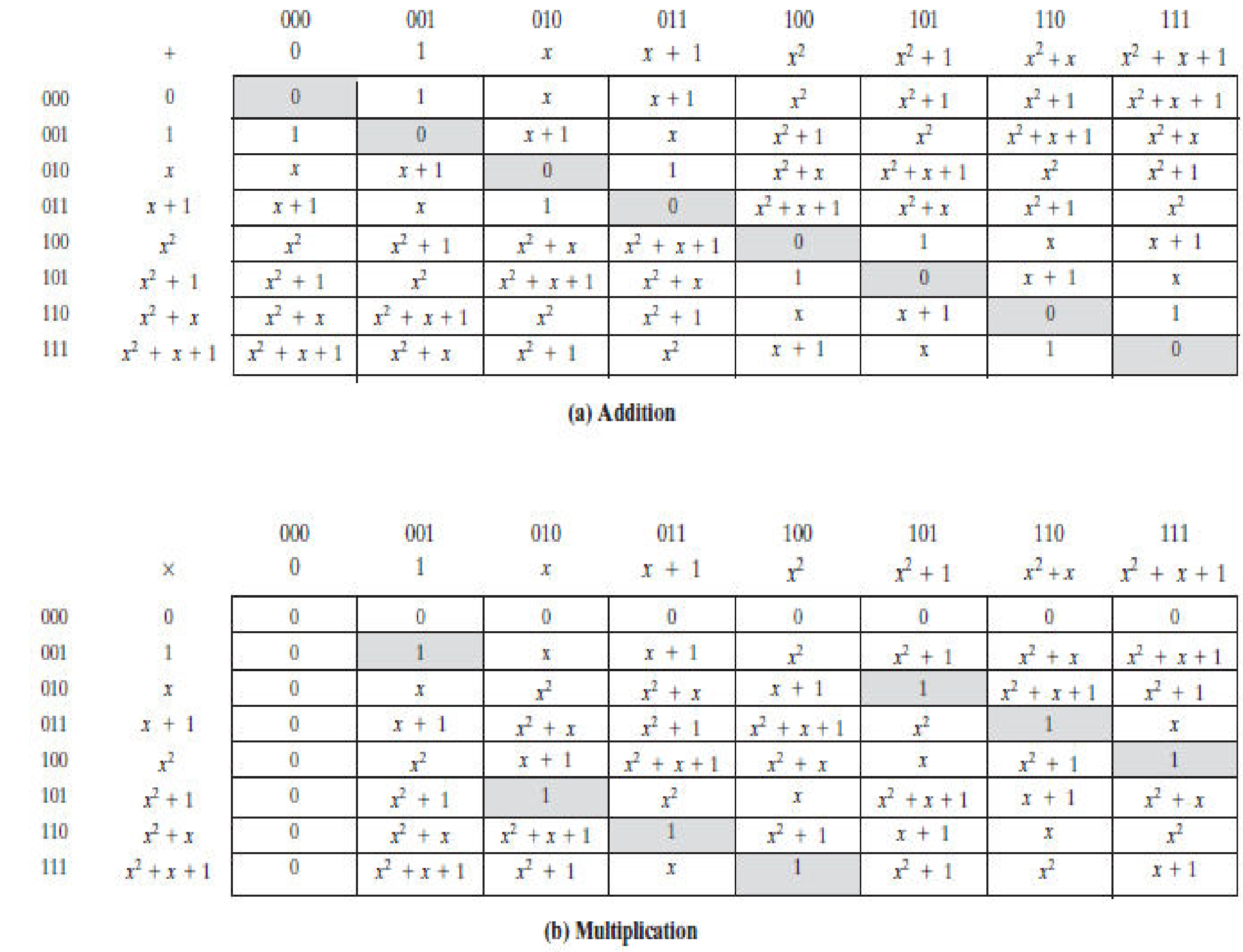
		000	001	010	011	100	101	110	111
	×	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

w	−w	w^{-1}
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(c) Additive and multiplicative inverses

Table 4.7 Polynomial Arithmetic Modulo ($x^3 + x + 1$)



		000	001	010	011	100	101	110	111
	+	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + 1$	$x^2 + x + 1$
001	1	1	0	$x + 1$	x	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$
010	x	x	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$
011	$x + 1$	$x + 1$	x	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2
100	x^2	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	x	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$	1	0	$x + 1$	x
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$	x	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2	$x + 1$	x	1	0

(a) Addition

		000	001	010	011	100	101	110	111
	×	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
010	x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
011	$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
100	x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	x	$x^2 + 1$	1
101	$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	$x^2 + x + 1$	$x + 1$	$x^2 + x$
110	$x^2 + x$	0	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	x	x^2
111	$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	x	1	$x^2 + 1$	x^2	$x + 1$

(b) Multiplication

Fermet & Euler Theorem

- play important roles in public-key cryptography

Fermat's Theorem

If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \,(\bmod\, p)$$

Proof:

- Consider the set of positive integers less than p: {1, 2, 3, ..., p-1}
- Multiply each element by a, modulo p to get the set
  - X = {a mod p, 2a mod p, ... (p - 1)a mod p}
- None of the elements of X is equal to zero because p does not divide a
- Therefore, we know that the (p - 1) elements of X are all positive integers with no two elements equal
- We can conclude the X consists of the set of integers {1, 2, ..., p - 1} in some order
- Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$a \times 2a \times \ldots \times (p-1)a = [(1 \times 2 \times \ldots \times (p-1)](\bmod p)$$
$$a^{p-1}(p-1)! \equiv (p-1)! \,(\bmod\, p)$$

We can cancel the (p -1)! term because it is relatively prime to p, which prooves the theorem

Example:

$$\begin{aligned}
&a = 7, p = 19\\
&7^2 = 49 \equiv 11 \,(\bmod 19)\\
&7^4 \equiv 121 \equiv 7 \,(\bmod 19)\\
&7^8 \equiv 49 \equiv 11 \,(\bmod 19)\\
&7^{16} \equiv 121 \equiv 7 \,(\bmod 19)\\
&a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \,(\bmod 19)
\end{aligned}$$

An alternative form of Fermat's theorem

If p is prime and a is a positive integer, then $a^p \equiv a(\bmod p)$

$$\begin{aligned}
&p = 5, a = 3 \qquad a^p = 3^5 = 243 \equiv 3(\bmod 5) = a(\bmod p)\\
&p = 5, a = 10 \qquad a^p = 10^5 = 100000 \equiv 10(\bmod 5) \equiv 0(\bmod 5) = a(\bmod p)
\end{aligned}$$

Euler's Theorem

Euler's totient function (ϕ (n))

- the number of positive integers less than n and relatively prime to n. ϕ (1) = 1
- for a prime number p, ϕ (p) = p - 1
- for two prime numbers where p # q,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$$

$$\phi(21) = \phi(3) \times \phi(7) = (3-1) \times (7-1) = 2 \times 6 = 12$$
where the 12 integers are {1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}.

To see that $\phi(n) = \phi(p) \times \phi(q)$, consider that the set of positive integers less that n is the set $\{1, \ldots, (pq - 1)\}$. The integers in this set that are not relatively prime to n are the set $\{p, 2p, \ldots, (q - 1)p\}$ and the set $\{q, 2q, \ldots, (p - 1)q\}$. Accordingly,

$$\begin{aligned}\phi(n) &= (pq - 1) - [(q - 1) + (p - 1)]\\ &= pq - (p + q) + 1\\ &= (p - 1) \times (q - 1)\\ &= \phi(p) \times \phi(q)\end{aligned}$$

Euler's Theorem

- for every a and n that are relatively prime $a^{\phi(n)} \equiv 1(\text{mod } n)$
- alternative form $a^{\phi(n)+1} = a\,(\text{mod } n)$

Proof:

Consider the set of positive integers less thann that are relatively prime to n, labeled as

$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \text{ mod } n), (ax_2 \text{ mod } n), \ldots, (ax_{\phi(n)} \text{ mod } n)\}$$

The set S is a permutation[6] of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.

2. There are no duplicates in S. Refer to Equation (4.5). If ax_i mod n $= ax_j \; mod \; n$, then $x_i = x_j$.

Therefore,

$$\begin{aligned}\prod_{i=1}^{\phi(n)} (ax_i \text{mod } n) &= \prod_{i=1}^{\phi(n)} x_i\\ \prod_{i-1}^{\phi(n)} ax_i &\equiv \prod_{i-1}^{\phi(n)} x_i (\text{mod } n)\\ a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] &= \prod_{i=1}^{\phi(n)} x_i (\text{mod } n)\\ a^{\phi(n)} &= 1\,(\text{mod } n)\end{aligned}$$

which completes the proof. This is the same line of reasoning applied to the proof of Fermat's theorem.