# COMP3260
# Data Security

# Lecture 1

Prof Ljiljana Brankovic

# Lecture Overview

- Course Overview
- Introduction to Data/Computer Security
- Steganography
- Introduction to Number Theory

# Resources

- Chapter 1 Computer and Network Security Concepts
- Chapter 3 Classical Encryption Techniques (Steganography)
  Based on textbook [1] and official textbook slides by L. Brown [2].
- Chapter 5 Finite Fields
  Some slides based on "Cryptography and Data Security" by D. Denning [3]
- Chapter 2 Introduction to Number Theory
  Based on "Cryptography and Data Security" by D. Denning [3]

Note that in-text references and quotes are omitted for clarity of the slides. When you write as essay or a report it is very important that you use both in-text references and quotes where appropriate.

# Course Overview

- Course Coordinator/Lecturer:

  Prof Ljiljana Brankovic

  **Room:** ES237

  **E-mail:** Ljiljana.Brankovic@newcastle.edu.au

  **Office Hours:** Wednesdays 13:00-14:00, ES237

# Course Overview

- Lectures:

  Wednesday 4pm - 6pm; **Room:** PG08

- Tutorials:

  Thursday 10am – 12am; **Room:** ICT334

  Friday 3pm - 5pm; **Room:** ES209

# Course Overview

- Text books:
  - W. Stallings. *Cryptography and Network Security*, Global Edition, Pearson Education Australia, 2016.

- Web Page:

  Blackboard

# Course Overview

- Aims:

  The course will provide an introduction to the principles and practice of data security. The course will focus on cryptography but it will also provide a brief introduction to other aspects of data security.

- Assumed knowledge:

  SENG1120, MATH1510

# Course Overview

- Assessment in Comp3260/6360:

  There will be 2 assignments/reports, 2 midterm tests and 11 quizzes during the semester. To pass the course, students have to score at least 40% of the total mark in the exam. Marked assignments and test will be returned to you as soon as possible, and no latter than 3 weeks after their due date.

| | |
|---|---|
| Assignment/Report 1 | 10% |
| Assignment/Report 2 | 10% |
| Midterm Test 1 | 10% |
| Midterm Test 2 | 20% |
| 10 Best Quizzes | 10% |
| Exam | 40% |

# Course Overview

- Course Policies:

All the quizzes are to be done individually. Cheating will not be tolerated and will imply 0 marks in the assignment. Please refer to the university Student Academic Integrity Policy at http://www.newcastle.edu.au/policy/000608.html

Assignments/Reports 1 and 2 are to be done in pairs, which will be organised in the first 3 weeks of the semester. All the pairs will be required to sign a Group Contract, to agree on the actions to be taken under certain circumstances.

Late assignments will be accepted, but for each day 10% of the maximum mark will be deducted from the mark. Assignment solutions will be published one week after the due date, and no assignments will be accepted after that.

| Week | Week Begins | Topic | Learning Activity | Assessment Due |
|---|---|---|---|---|
| 1 | 25 Feb | Introduction to Data Security<br>Revision: Groups, rings, fields | | |
| 2 | 4 Mar | Number theory | Game 1 | Quiz 1 |
| 3 | 11 Mar | Information theory, perfect secrecy, unicity distance<br>Revision: Probability | Game 2 | Quiz 2 |
| 4 | 18 Mar | Classical ciphers | Game 3 | Test 1; Quiz 3<br>Assignment 1 out |
| 5 | 25 Mar | Stream and block ciphers; Feistel cipher; DES and DES modes of operation | Game 4 | Quiz 4 |
| 6 | 1 Apr | AES; AES polynomial arithmetic | Game 5 | Quiz 5<br>Assignment 1 due<br>Assignment 2 out |
| 7 | 8 Apr | PK Encryption, RSA, ElGamal; elliptic Curves | Game 6 | Quiz 6 |
| Mid Semester Break | | | | |
| Mid Semester Break | | | | |
| 8 | 29 Apr | Key management; message authentication | Game 7 | Quiz 7 |
| 9 | 6 May | Hash functions and digital signatures | Game 8 | Assignment 2 due<br>Quiz 8 |
| 10 | 13 May | Selected topics in cryptography and security | Game 9 | Quiz 9 |
| 11 | 20 May | Privacy; selected topics in cryptography and security | Game 10 | Quiz 10 |
| 12 | 27 May | Privacy; selected topics in | Game 11 | Test 2 |

# Introduction to Computer Security

*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."*

**—The Art of War, Sun Tzu, 544 – 496 BC**

*"It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and its terminals in a shielded room, and put a guard at the door."*

***— F. T. Grampp and R. H. Morris. UNIX Operating System Security, 1984***

# Background

- In recent years, data is seen as one of the most valuable assets of companies and organisation.

- **Data security** refers to the protection of data from unauthorised disclosure, destruction and alternation.

# Background

- Security requirements have changed in recent times.
- Traditionally provided by physical and administrative mechanisms.
- Computer use requires automated tools to protect files and other stored information.
- Use of networks and communications links requires measures to protect data during transmission.

# Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers (or, more generally, to protect resources).

- **Network (Internet) Security** - measures to deter, prevent, detect and correct violations that involve transmission of data.

# Services, Mechanisms, Attacks

- We need systematic way to define requirements

- Consider three aspects of information security:
  - **security attacks**
  - **security mechanisms**
  - **security services**

# Security Service

- enhance the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
    - eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

# Security Mechanism

- A security mechanism is a  mechanism that is designed to detect, prevent, or recover from a security attack
- There is no single mechanism that will support all functions required
- However. one particular element underlies many of the security mechanisms in use: **cryptographic techniques**.
- Hence our focus on this area.

# Security Attack

- Security attack is any action that compromises the security of information owned by an organization.
- Information security is about how to prevent attacks, or failing that, to detect and recover from attacks on information-based systems.
- There is  a wide range of attacks.
- We focus on generic types of attacks.
- Note: often *threat* & *attack*  mean same

# Security Services

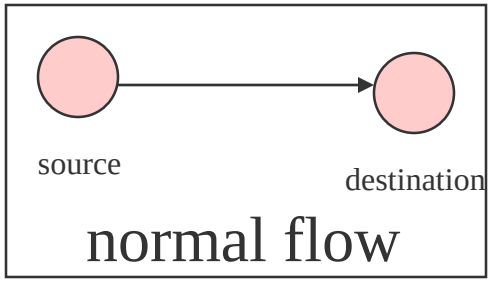
- **Confidentiality*** - data should be accessible only by authorised users
- **Authenticity** - the origin of an electronic document can be correctly identified
- **Integrity** - data can be modified only by authorised users
- **Non-repudiation** - neither the sender not the receiver of the message can deny the transition
- **Availability** - computer assets are available to authorised users when needed

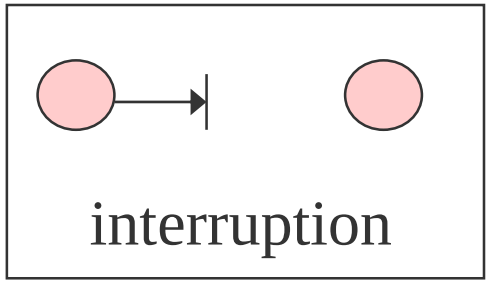
***Privacy** is often mixed up with **confidentiality** – privacy is a right of individuals to control information about themselves

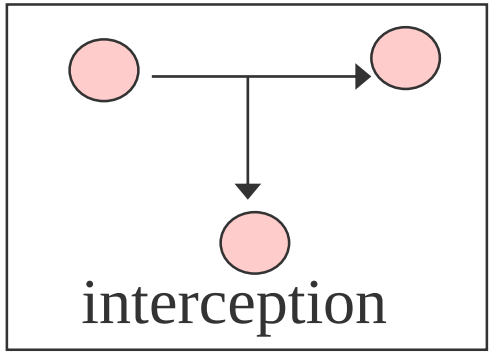
# Security Services

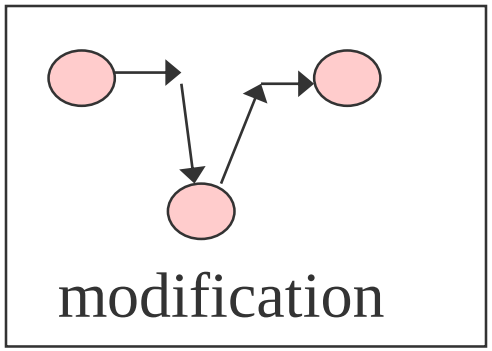
- Security services are often referred to as "security objectives" in the literature.
- There are inconsistencies in the literature re these objectives and the terminology.
- For example, A. Menezes , P. van Oorschot, and S. Vanstone in "Handbook of Applied Cryptography", CRC Press, 1996, list confidentiality, integrity, authentication and non-repudiation, while M. Bishop in "Computer Security: Art and Science", Addison Wesley, 2003, list confidentiality, integrity and availability.

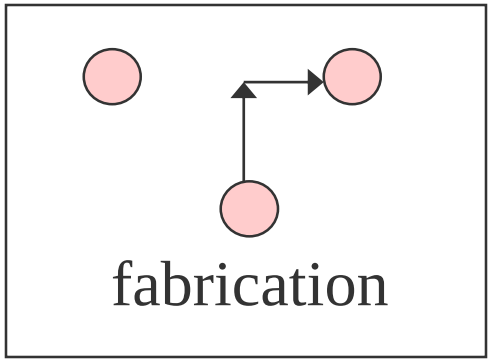
# Security Attacks

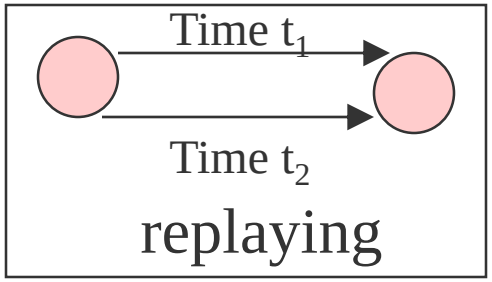


**Another way at looking at security threats:**

- unauthorised users
- authorised users having unauthorised access
- authorised users using authorised access to obtain access to data they should not access

# OSI Security Architecture

- ITU-T* X.800 Security Architecture for OSI** gives a systematic way of defining and providing security requirements

- *ITU-T (International Telecommunication Union, Telecommunication Standardization Sector)
- **OSI (Open Systems Interconnection), created at International Organization for Standardization (ISO)

# Security Services

- X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers

- RFC 2828* defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources

*The Requests for Comments (RFC) document series is a set of technical and organizational notes about the Internet; published by Internet Engineering Task Force which develops Internet standards.

# Security Services (X.800)

X.800 defines it in 5 major categories

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

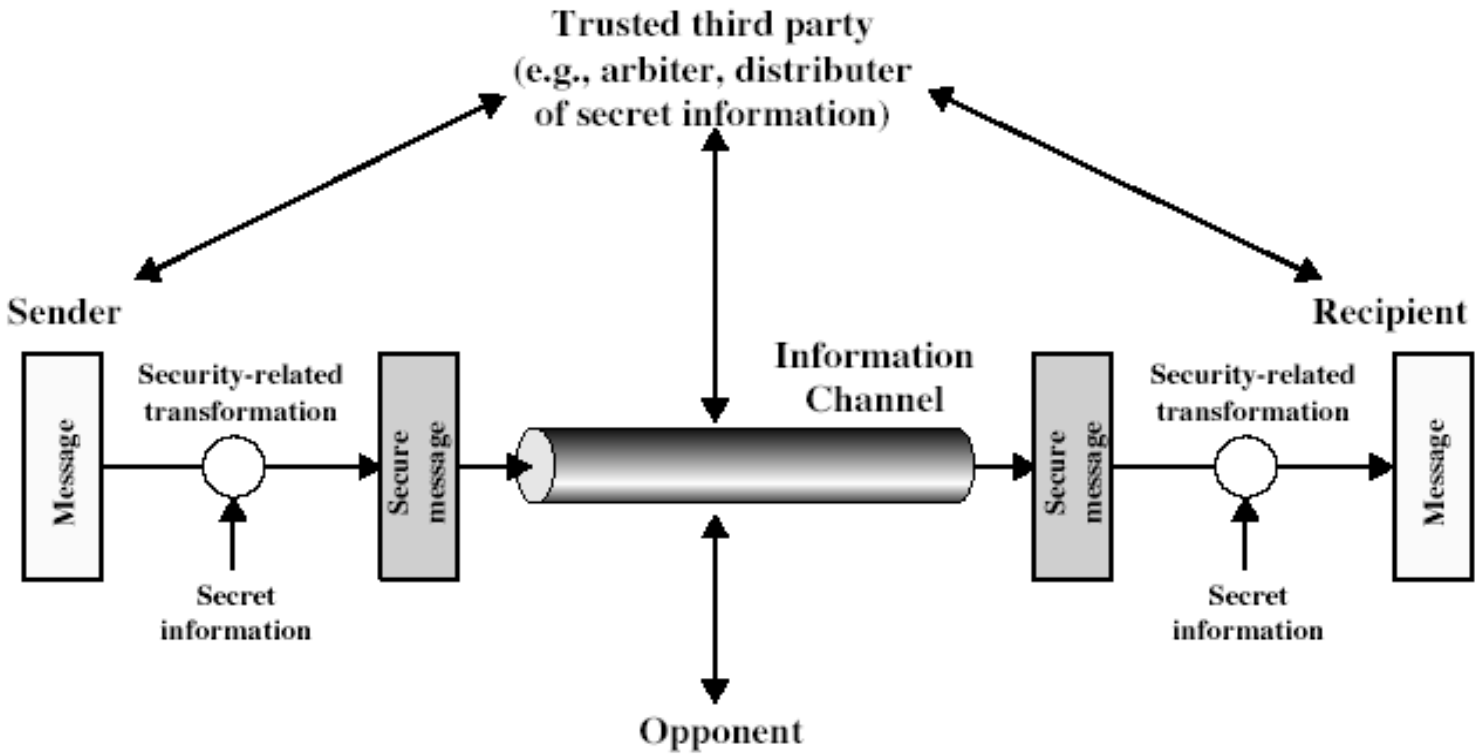
# Security Mechanisms (X.800)

- specific security mechanisms:
  - 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

# Classify Security Attacks as

- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

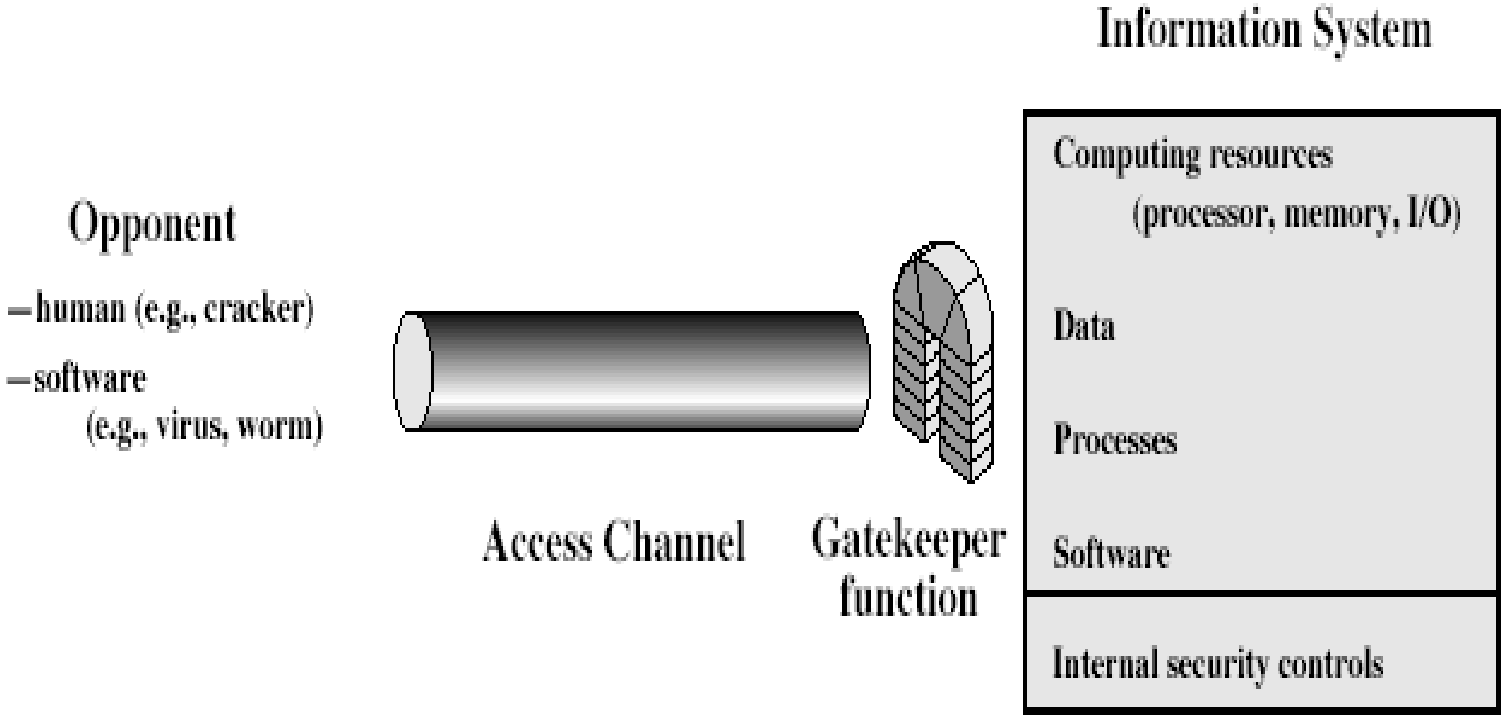
# Model for Network Security



# Model for Network Security

- Using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

# Model for Network Access Security



# Model for Network Access Security

- Using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- Trusted computer systems can be used to implement this model

# Steganography

- An alternative to encryption
- Hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB (Least Significant Bit) in graphic image or sound file
- Has drawbacks
  - high overhead to hide relatively few info bits (now becoming less of a problem)
  - once broken, the system becomes worthless

# Example

Dear George,
Greetings to all at Oxford. Many thanks for your letter and for the summer examination package. All Entry Forms and Fees Forms should be ready for final dispatch to the syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

# Example

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the summer examination package. All Entry Forms and Fees Forms should be ready For final dispatch to the syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

# Example

A German spy transmitted the following message during the WWI:

*Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.*

# Example

A German spy transmitted the following message during the WWI:

*Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.*

Pershing sails from NY June 1

# Underlying theories

- Cryptography, one of the main focuses of this course, is based on 3 underlying theories:
  - number theory,
  - information theory, and
  - complexity theory.

- We will present the basics of the number and information theory; complexity theory was taught in COMP2230 Introduction to Algorithmics.

# Introduction to Number Theory

"God made integers; all else is the work of man".

-Leopold Kronecker (1823 -1891) German algebraist and number theorist.

# Congruences and Modular Arithmetic

Given integers $a$, $b$ and $n \neq 0$, $a$ is congruent to $b$ modulo $n$ written $a \equiv_n b$ or $a \equiv b \bmod n$ if and only if

$$a - b = kn$$

for some integer $k$.

That means that $n$ divides $a-b$, written

$$n \mid (a-b)$$

# Congruences and Modular Arithmetic

***Example:***
$17 \equiv_5 7$, because $(17 - 7) = 2*5$.

If $a \equiv_n b$, then $b$ is called a residue of $a$ modulo $n$ (also, $a$ is a residue of $b$ modulo $n$).

A set of integers $\{r_1, r_2, \ldots, r_n\}$ is called a complete set of residues modulo $n$ if, for every integer $a$, there is exactly one $r_i$ in the set such that $a \equiv_n r_i$.

For any $n$, the set of integers $\{0, 1, \ldots, n-1\}$ form a complete set of residues modulo $n$.

# Congruences and Modular Arithmetic

We shall use $a \bmod n$ to denote the residue $r$ of $a$ modulo $n$ in the range $[0, n-1]$.

***Example***: $7 \bmod 3 = 1$

Note that $a \bmod n = r$ implies $a \equiv_n r$ but $a \equiv_n r$ does not imply $a \bmod n = r$. Also note that $a \equiv_n b$ if and only if $a \bmod n = b \bmod n$ (congruent integers have the same residue in the range $[0, n-1]$ ).

# Congruences and Modular Arithmetic

Computing in modular arithmetic gives the same result as computing in ordinary integer arithmetic and reducing the result modulo n.

***Theorem:*** Let $a$ and $b$ be integers, and let $op$ be one of the binary operators +, -, or *. Then

$(a \; op \; b) \bmod n = [(a \bmod n) \; op \; (b \bmod n)] \bmod n$

***Proof:*** We shall write $a$ and $b$ as follows

$a = kn + r_1$

$b = hn + r_2$

where $k$ and $h$ are integers and $r_1, r_2 \in [0, n-1]$.

# Congruences and Modular Arithmetic

***Proof (cont'd):***

For addition we have:

$$(a + b) \bmod n = [(kn + r_1) + (hn + r_2)] \bmod n$$
$$= [(k + h)n + (r_1 + r_2)] \bmod n$$
$$= [r_1 + r_2] \bmod n$$
$$= [(a \bmod n) + (b \bmod n)] \bmod n$$

Subtraction is very similar. For multiplication we have:

$$(a*b) \bmod n = [(kn + r_1) * (hn + r_2)] \bmod n$$
$$= [(khn + r_1h + r_2k)n + r_1r_2)] \bmod n$$
$$= [(a \bmod n) * (b \bmod n)] \bmod n$$

# Congruences and Modular Arithmetic

***Example:***

| Integer Arithmetic (mod 9) | Modular Arithmetic |
|---|---|
| 1 3 5 2 7 3 | 3 |
| 2 6 1 9 0 9 | 0 |
| +5 2 2 0 4 4 | +8 |
| --- | --- |
| 9 1 9 2 2 6 | 2 |

# Congruences and Modular Arithmetic

Note that this principle doesn't apply to the exponentiation in the sense of reducing exponent modulo n; that is, $e^{t \bmod n} \bmod n$ is not necessarily equal to $e^t \bmod n$.

For example, $2^{5 \bmod 3} \bmod 3 = 1$, but $2^5 \bmod 3 = 2$.

However, because of repeated multiplications, we have

$$e^t \bmod n = [\Pi_{i=1}^{t} (e \bmod n)] \bmod n$$

# Congruences and Modular Arithmetic

***Example:*** Consider expression $3^5 \bmod 7$. Computing in on ordinary integer arithmetic and then reducing the result mod 7 gives:

1. 3*3=9
2. 9*9=81
3. 81*3=243
4. 243 mod 7 = 5

In modular arithmetic we have:

1. 3*3 mod 7 =2
2. 2*2 mod 7 = 4
3. 4*3 mod 7 = 5

Thus computing in modular arithmetic has an advantage of reducing intermediate results.

# Fast Exponentiation Algorithm

Input: a, z, n

Output: None

```
fastexp(a,z,n) {
      // x = a^z mod n
      while (z ≠ 0) {
            while (z mod 2 == 0) {
                  z= z/2
                  a = a*a mod n
            }
            z = z-1
            x = x*a mod n
      }
      return x
}
```

# Properties of Modular Arithmetic for Integers in $Z_n$

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

# Groups

A group $G$ is a set of elements with a binary operation denoted by • that associates to each ordered pair $(a,b)$ of elements in $G$ an element $(a \bullet b)$ in $G$, such that the following axioms are obeyed:

- **(A1)** Closure: If $a$ and $b$ belong to $G$, then $a \bullet b$ is also in $G$
- **(A2)** Associative: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c$ in $G$
- **(A3)** Identity element: There is an element $e$ in $G$ such that $a \bullet e = e \bullet a = a$ for all $a$ in $G$
- **(A4)** Inverse element: For each $a$ in $G$, there is an element $a^{-1}$ in $G$ such that $a \bullet a^{-1} = a^{-1} \bullet a = e$

# Groups

A group $G$ is called ***abelian*** if it obeys the following additional axiom:

- **(A5)** Commutative: $a \bullet b = b \bullet a$ for all $a, b$ in $G$

Group $G$ can be

- ***finite***, if it has a finite number of elements; then the number of elements in the group $G$ is called ***order of G***
- ***infinite,*** if it has an infinite number of elements

# Cyclic Group

- Exponentiation is defined within a group as a repeated application of the group operator, so that $a^3 = a \bullet a \bullet a$
- We define $a^0 = e$ as the identity element, and $a^{-n} = (a^{-1})^n$, 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
- 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

# Rings

A **ring** $R$ , sometimes denoted by $\{R , + , * \}$, is a set of elements with two binary operations, called *addition* and *multiplication*, 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 $R$

# Rings (cont.)

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

- 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

- An ***integral domain*** is a commutative ring that obeys the following axioms.

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

  **(M6) No zero divisors:**

  If $a, b$ in R and $ab = 0$, then either $a = 0$ or $b = 0$

# Fields

- A **field** $F$ , sometimes denoted by {F, +,* }, 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

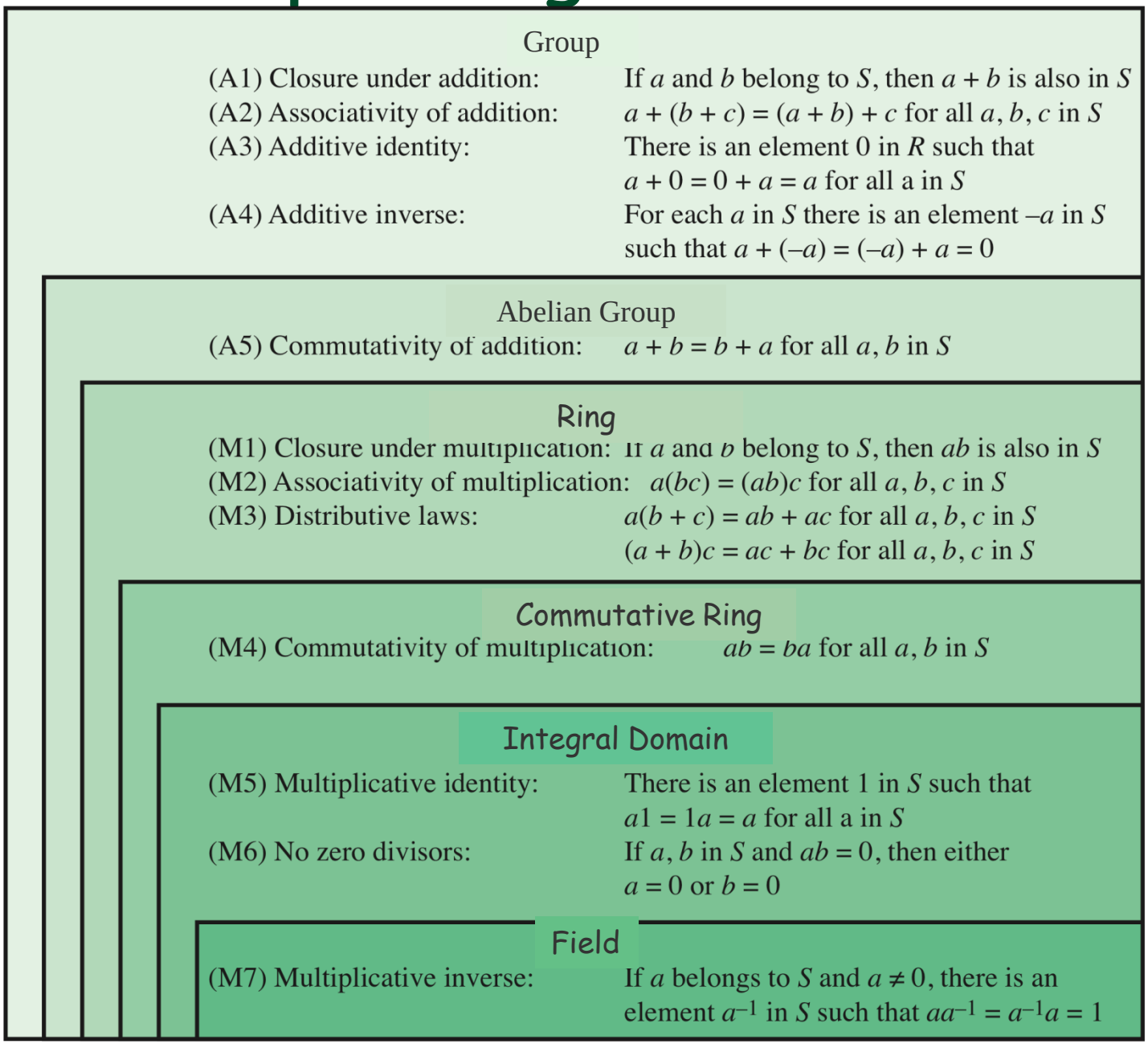
  **(M7) Multiplicative inverse:**

  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.

# Groups, Rings and Fields



# Summary

- Introduction to computer security:
  - computer, network, internet security definitions
  - security services, mechanisms, attacks
  - X.800 standard
  - models for network (access) security
- Steganography
- Introduction to number theory
  - Congruencies
  - Modular arithmetic
  - Fast exponentiation
- Introduction to Finite Fields
  - Groups, Rings and Fields

# References


1. W. Stallings. Cryptography and Network Security, Global Edition, Pearson Education Australia, 2016.

2. Official textbook slides by L. Brown.

3. D. Denning. "Cryptography and Data Security", Addison Wesley, 1982.