COMP3260/6360 Data Security

Lecture 1

Prof Ljiljana Brankovic

Lecture Overview

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

Resources

- Textbook Chapter 1 Computer and Network Security Concepts
- Textbook Section 3.5 Classical Encryption Techniques (Steganography)
  Based on textbook [1] and official textbook slides by L. Brown [2].
- Textbook Chapter 5 Finite Fields
  Some slides based on “Cryptography and Data Security” by D. Denning [3]
- Textbook Chapter 2 Introduction to Number Theory
  Slides 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

  Email: Ljiljana.Brankovic@newcastle.edu.au

  Office Hours: Tuesdays 12:00-13:00, ES237

- **Tutor:**

  Dr Matt Skerritt

  Email: matthew.skerritt@newcastle.edu.au

- **Lectures:** Tuesday 10:00 - 12:00; **Room:** ATC210
- **Tutorials:** Monday 15:00 - 17:00; **Room:** V105

  Wednesday 15:00 - 17:00; **Room:** ICT334

Course Overview

- Textbook:
  - W. Stallings. *Cryptography and Network Security*, 7th Edition, Pearson Education Australia, 2017.

- Web Page:

  Blackboard

- 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, 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 1	10%
Assignment 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 https://policies.newcastle.edu.au/document/view-current.php?id=35&version=1

Assignments 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	22 Feb	Introduction to Data Security Revision: Groups, rings, fields		
2	1 Mar	Number theory	Game 1	Quiz 1
3	8 Mar	Information theory, perfect secrecy, unicity distance Revision: Probability	Game 2	Quiz 2
4	15 Mar	Classical ciphers	Game 3	Test 1; Quiz 3 Assignment 1 out
5	22 Mar	Stream and block ciphers; Feistel cipher; DES and DES modes of operation	Game 4	Quiz 4
6	29 Mar	AES; AES polynomial arithmetic	Game 5	Quiz 5 Assignment 1 due Assignment 2 out
Mid Semester Break				
Mid Semester Break				
7	19 Apr	PK Encryption, RSA, ElGamal; elliptic Curves	Game 6	Quiz 6
8	26 Apr	Key management; message authentication	Game 7	Quiz 7
9	3 May	Hash functions and digital signatures	Game 8	Assignment 2 due Quiz 8
10	10 May	Selected topics in cryptography and security	Game 9	Quiz 9
11	17 May	Privacy; selected topics in cryptography and security	Game 10	Quiz 10
12	24 May	Privacy; selected topics in cryptography and security	Game 11	Test 2 Quiz 11
13	1 Jun	No lecture, exam preparation week		

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.

- Security requirements have changed in recent decades:

  - 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 - NIST Glossary of Key Information Security Terms 2013

Information Security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Data Security is the protection of data from unauthorised (accidental or intentional) modification, destruction, or disclosure.

Computer Security refers to measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored and communicated.

Definitions - NIST Glossary of Key Information Security Terms 2013

Cyber Security refers to the ability to protect or defend the use of cyberspace from cyber attacks.

Cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Network security is not explicitly defined by NIST Glossary of Key Information Security Terms 2013 but is instead equated with information assurance. It is widely used to denote protection of computer networks and resources accessible from the networks – these include protection of data during transmission, protection of network resources, as well as prevention of attacks that can be launched using networks.

Services, Mechanisms, Attacks

- We need a systematic way to define requirements.

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

Security Service

Security services:

- are intended to counter security attacks
- make use of one or more security mechanisms
- replicate functions normally associated with physical documents, e.g., have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed
- are often referred to as "security objectives" in the literature
- are inconsistently defined in the literature
  - 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
  - M. Bishop in "Computer Security: Art and Science", Addison Wesley, 2003, list confidentiality, integrity and availability.

Security Services

CIA Triad:

- **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

Other Services:

- **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
- **Anonymity** - electronic records such as medical histories, shopping baskets and search histories cannot be associated with a particular individual. Anonymity is tightly related to privacy, which we define as the right of individuals to control information about themselves.

Security Mechanisms

- 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**.
- Other security mechanisms include access control, backups, traffic padding and so on.

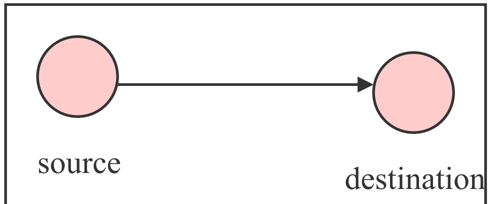
Security Attack (Threats)

- Security attack is any action that compromises the security of information owned by an organization.

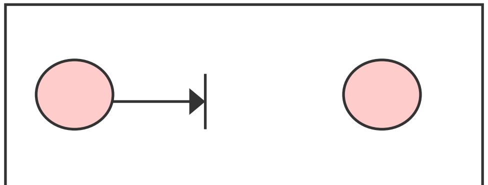
- Information security is about how to prevent attacks, or failing that, to detect and recover from attacks on information-based systems.

- **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

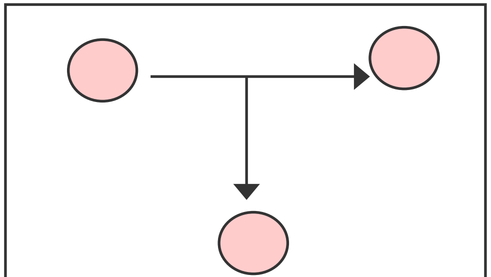
Security Attacks



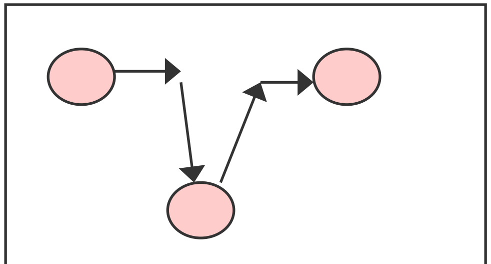
normal flow



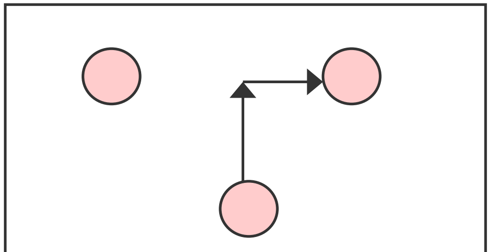
interruption



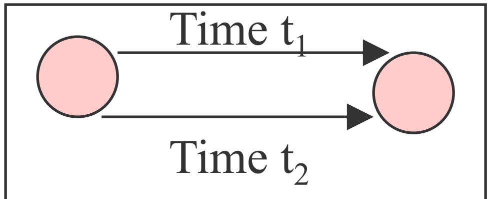
interception



modification



fabrication



replaying

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)

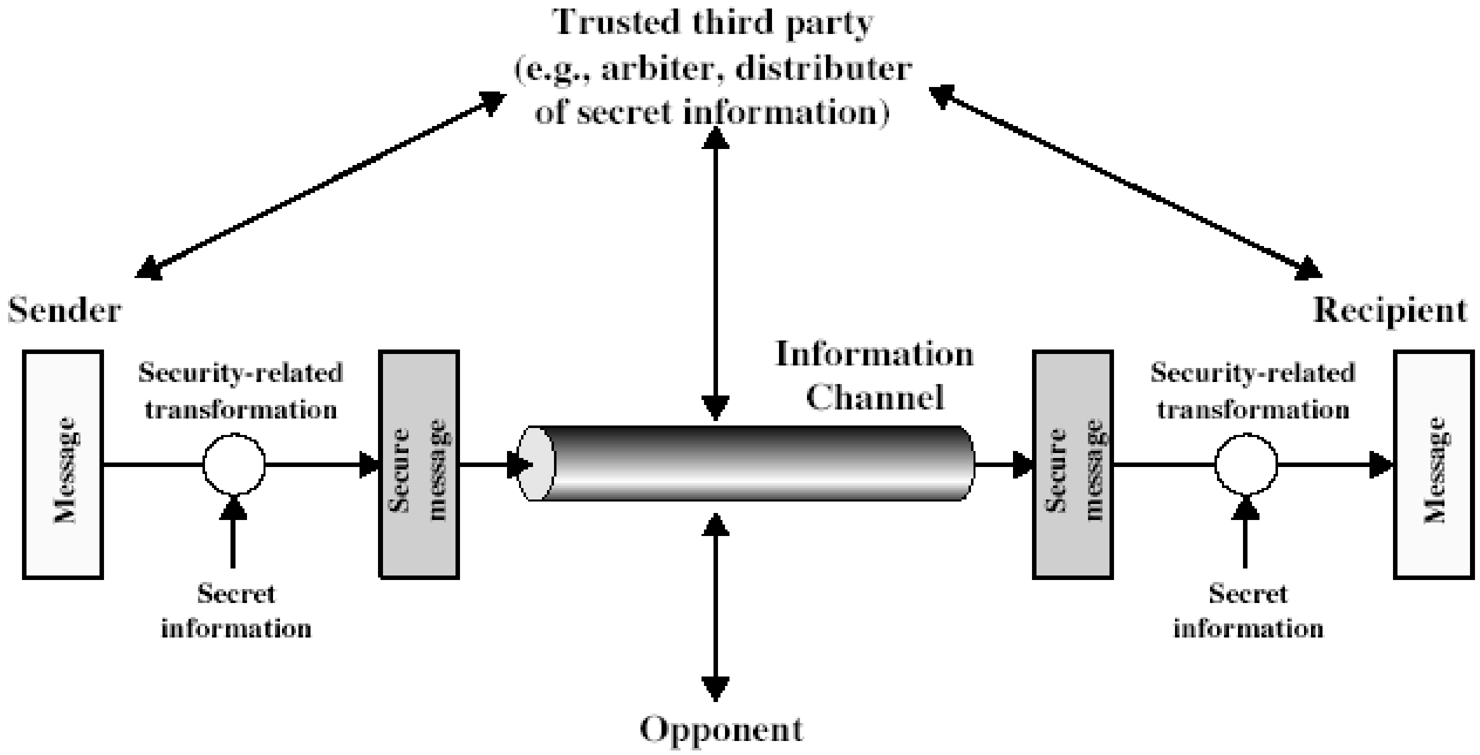
X.800 defines it in 5 major categories

- **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

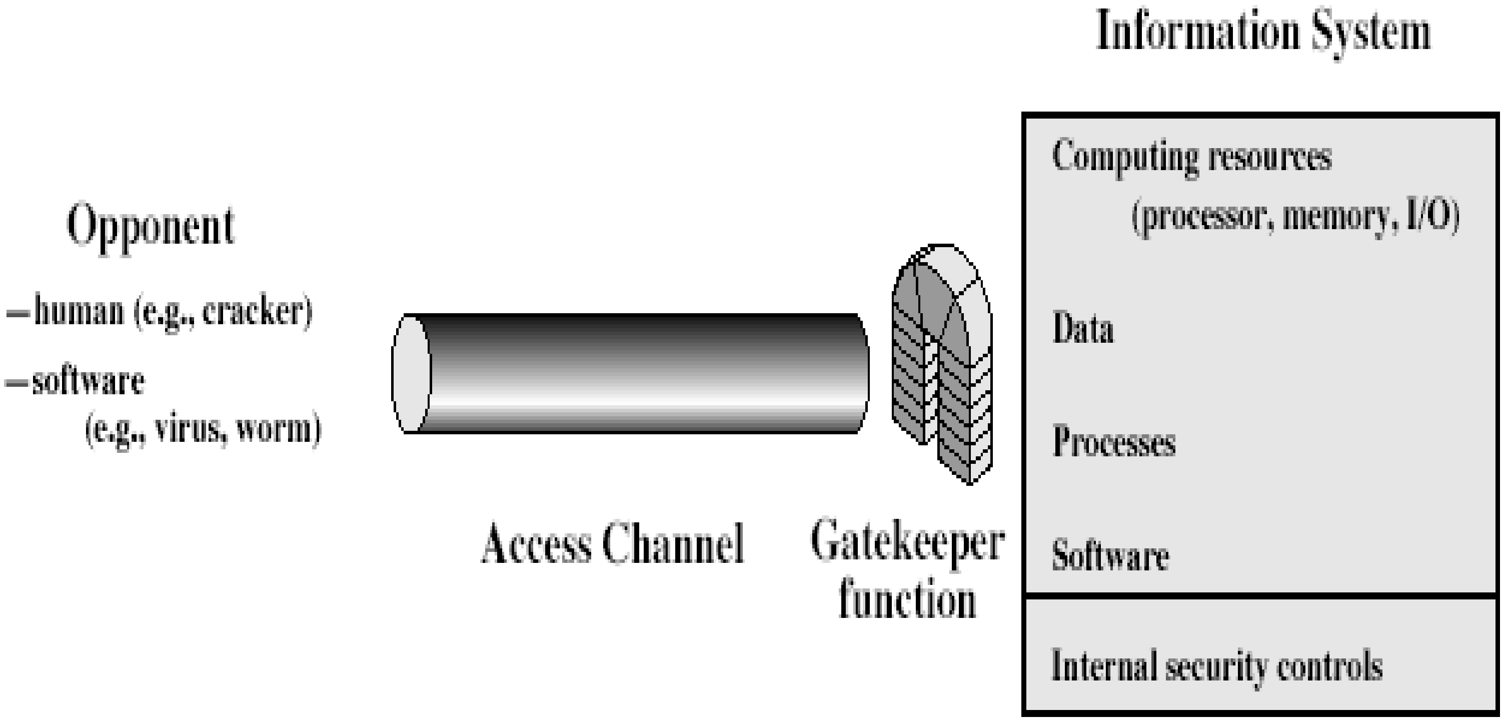
Security Mechanisms (X.800)

- 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

Model for Network Security



Model for Network Access Security



Opponent

- human (e.g., cracker)
- software
  (e.g., virus, worm)

Access Channel

Gatekeeper function

Information System

Computing resources
(processor, memory, I/O)

Data

Processes

Software

Internal security controls

Steganography

- An alternative to encryption

- Hides existence of a 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 less of a problem)
  - once broken, the system becomes worthless

Example 1

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 1

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 2

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 2

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

$n \mid (a\text{-}b)$

Congruences and Modular Arithmetic

Example 3: $17 \equiv_5 7$, because $(17 - 7) = 10 = 2*5$.

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 $a \equiv_n r_i$.

Example 4: $\{5, 7, 12, 10\}$ is called a complete set of residues modulo 4

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 5: $7 \bmod 3 = 1$

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) mod n = [(a mod n) op (b mod n)] mod 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 $r_1, r_2 \in [0, n\text{-}1]$.

Congruences and Modular Arithmetic

Proof (cont'd):

For addition we have:

$$\begin{aligned}(a + b) \bmod n &= [(kn + r_1) + (hn + r_2)] \bmod n \\ &= [(k + h)n + (r_1 + r_2)] \bmod n \\ &= [r_1 + r_2] \bmod n \\ &= [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$

Subtraction is very similar. For multiplication we have:

$$\begin{aligned}(a*b) \bmod n &= [(kn + r_1) * (hn + r_2)] \bmod n \\ &= [(khn + r_1h + r_2k)n + r_1r_2)] \bmod n \\ &= [(a \bmod n) * (b \bmod n)] \bmod n\end{aligned}$$

Congruences and Modular Arithmetic

Example 6:

Integer Arithmetic	Modular Arithmetic
(mod 9)	
135273	3
261909	0
+522044	+8
---------------	-----
919226	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 7: Consider expression 3^5 mod 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
    x = 1
    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
}
```

Example 8

$$3^{10}\ mod\ 5 = \ 9^5 mod\ 5$$

$$= 4^5 mod\ 5$$

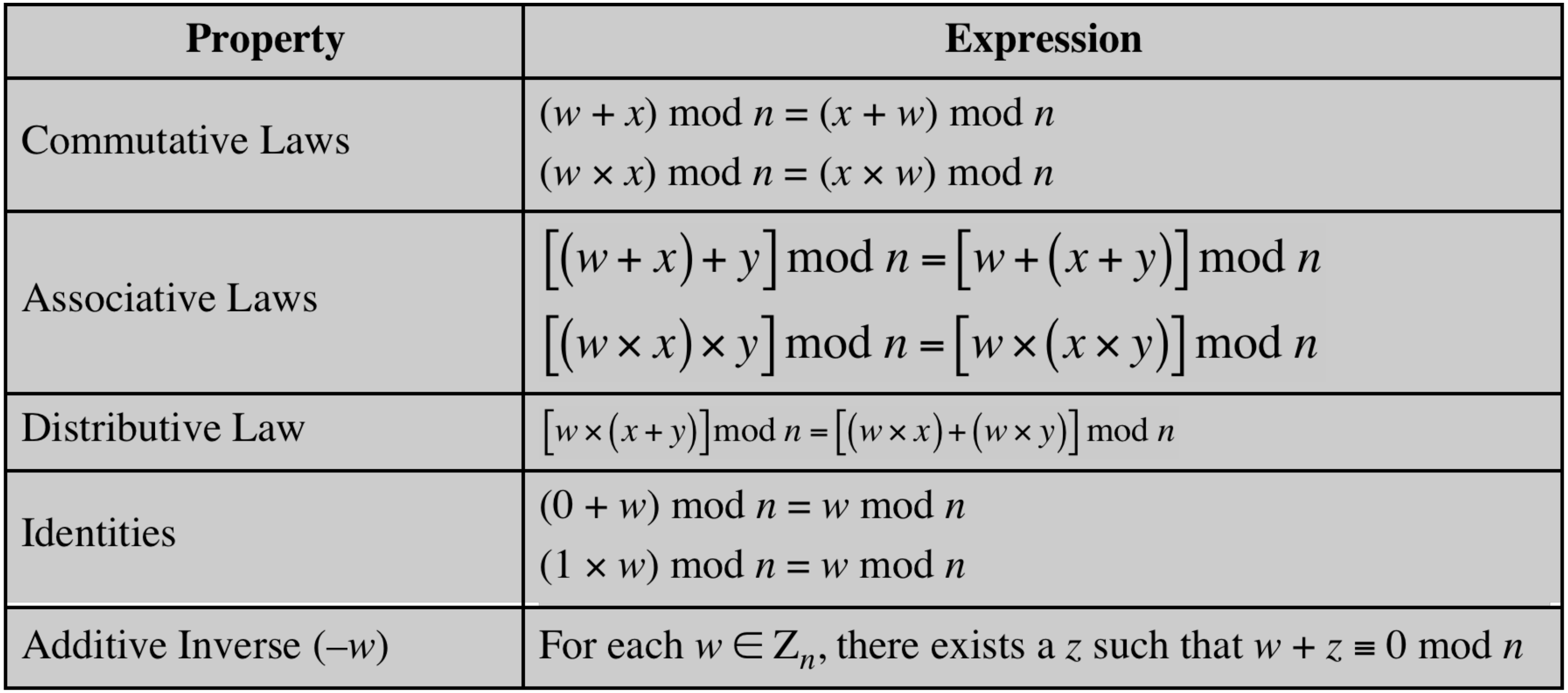
$$= \left(4 \times 4^4\right)\ mod\ 5$$

$$= \left(4 \times 16^2\right) mod\ 5$$

$$= \left(4 \times 1^2\right) mod\ 5$$

$$= 4$$

Properties of Modular Arithmetic for Integers in Z_n



Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$\left[(w + x) + y\right] \bmod n = \left[w + (x + y)\right] \bmod n$ $\left[(w \times x) \times y\right] \bmod n = \left[w \times (x \times y)\right] \bmod n$
Distributive Law	$\left[w \times (x + y)\right] \bmod n = \left[(w \times x) + (w \times y)\right] \bmod n$
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 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 $a \times 1 = 1 \times a = a$ 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

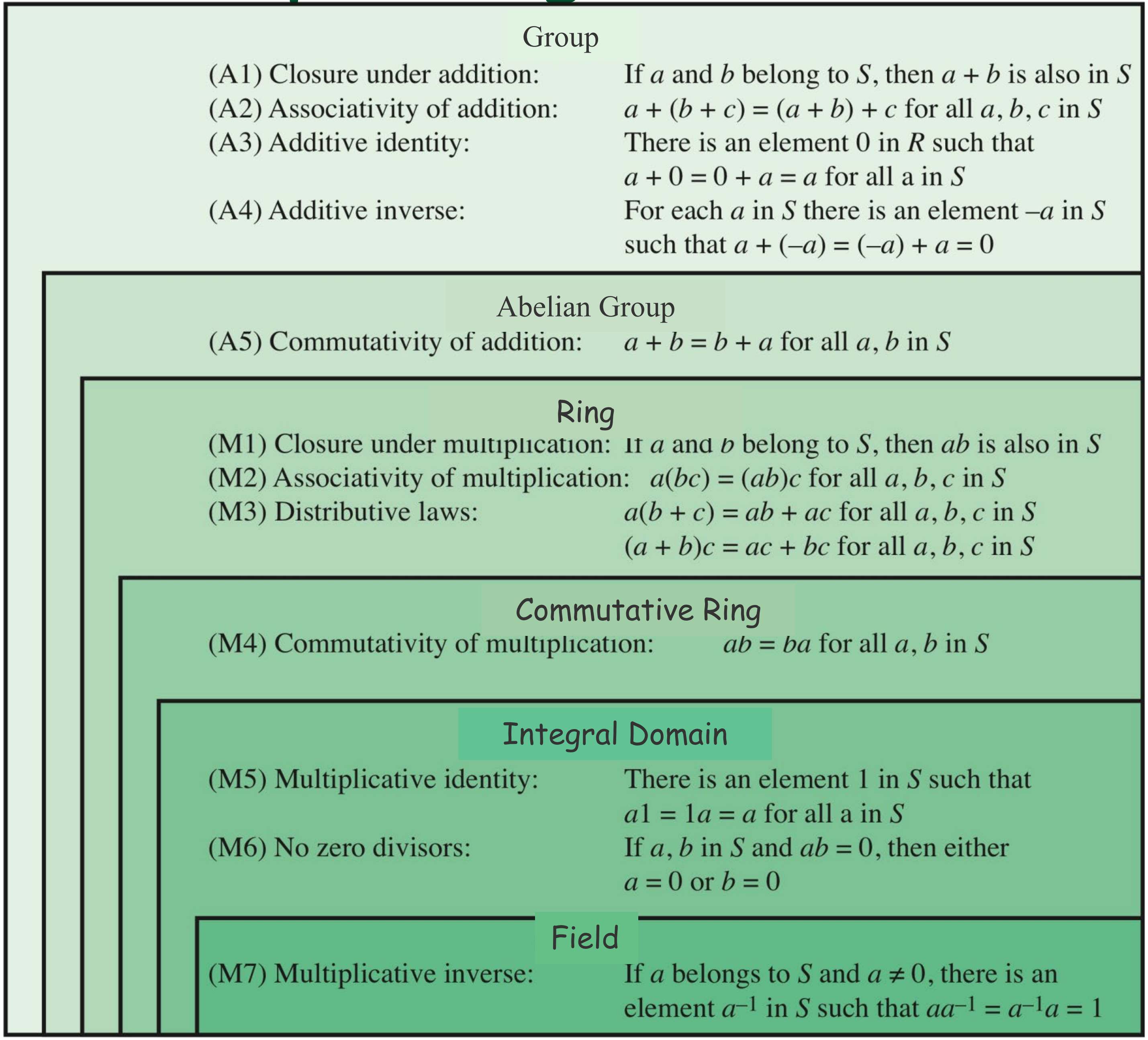
  (M7) Multiplicative inverse:

  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



Group

(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 $a + (-a) = (-a) + a = 0$

Abelian Group

(A5) Commutativity of addition: $a + b = b + a$ for all a, b in S

Ring

(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

Commutative Ring

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

Integral Domain

(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 $b = 0$

Field

(M7) Multiplicative inverse: If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Chinese Remainder Theorem

In 3rd century AD, the Chinese mathematician Sun Tzu (or Sun Zi) asked the following question in his book Sun Tzu Suan Ching (literally, "Sun Tzu's Calculation Classic"):

"We have a number of things, but we do not know exactly how many. If we count them by threes we have two left over. If we count them by fives we have three left over. If we count them by sevens we have two left over. How many things are there?"

Chinese Remainder Theorem

Chinese Remainder Theorem: Let $d_1, \dots, d_t$ be pairwise relatively prime, and let $n = d_1 d_2 \dots d_t$. Then the system of equations

$(x \bmod d_i) = x_i \ (i = 1, \dots, t)$

has a common solution x in the range $[0, n-1]$.

Proof Outline: The common solution is

$$x = [\sum_{i=1}^{t} \frac{n}{d_i} y_i x_i] \bmod n$$

where y_i is a solution of $\frac{n}{d_i} y_i \bmod d_i = 1$ (note that $\frac{n}{d_i}$ is relatively prime to $d_{i,}$ thus there is always a solution).

Chinese Remainder Theorem

Example 9: Solve $3x\ mod\ 10\ =\ 1$ (in other words, find a mulplicative inverse of *3* modulo *10*).

$10\ =\ 2 \times 5$ so $d_1\ =\ 2$ and $d_2\ =\ 5$.

We first find solutions x_1 and x_2:

$$3x\ mod\ 2\ =\ 1 \rightarrow x_1\ = 1$$
$$3x\ mod\ 5\ =\ 1 \rightarrow x_2\ = 2$$

We now apply Chinese reminder theorem to find a common solution to the equations

$$x\ mod\ 2\ =\ x_1\ =\ 1$$
$$x\ mod\ 5\ =\ x_2\ =\ 2$$

Chinese Remainder Theorem

First find y_1 and y_2 such that

$$\frac{10}{2} y_1 \bmod 2 = 1 \ \rightarrow \ y_1 = 1$$

$$\frac{10}{5} y_2 \bmod 5 = 1 \rightarrow y_2 = 3$$

We now have

$$\begin{aligned} x &= \left(\frac{10}{2} y_1 x_1 + \frac{10}{5} y_2 x_2\right) \bmod 10 \\ &= \ (5 \times 1 \times 1 + 2 \times 3 \times 2) \bmod 10 = 7 \end{aligned}$$

Thus *7* is the multiplicative inverse of *3* modulo *10*.

Chinese Remainder Theorem

Example 10: An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Chinese Remainder Theorem

x mod 2 = 1
x mod 3 = 1
x mod 4 = 1
x mod 5= 1
x mod 6 = 1
x mod 7 = 0

Remember that in order to apply the Chinese remainder Theorem, we need $d_1, \ldots, d_t$ to be relatively prime. Is that the case here? Which ones should we keep?

Chinese Remainder Theorem

Note that $x \bmod 6 = 1$ implies $x \bmod 2 = 1$ but not the other way around! However, $x \bmod 2 = 1$ and $x \bmod 3 = 1$ together imply $x \bmod 6 = 1$ (by the Chinese Remainder Theorem :-)

x	x mod 2	x mod 3	x mod 6
1	1	1	1
2	0	2	2
3	1	0	3
4	0	1	4
5	1	2	5
6	0	0	0
7	1	1	1
8	0	2	2
9	1	0	3
10	0	1	4
11	1	2	5
12	0	0	0

Chinese Remainder Theorem

$$\begin{aligned} x \; mod\; 3 &= 1 \\ x \; mod\; 4 &= 1 \\ x \; mod\; 5 &= 1 \\ x \; mod\; 7 &= 0 \end{aligned}$$

$$n = 3 \times 4 \times 5 \times 7 = 420$$

$$\begin{aligned} 140\, y_1 \; mod\; 3 = 1 &\rightarrow 2\, y_1 \; mod\; 3 = 1 \rightarrow y_1 = 2 \\ 105 y_2 \; mod\; 4 = 1 &\rightarrow y_2 \; mod\; 4 = 1 \rightarrow y_2 = 1 \\ 84\, y_3 \; mod\; 5 = 1 &\rightarrow 4\, y_3 \; mod\; 5 = 1 \rightarrow y_3 = 4 \\ 60 y_4 \; mod\; 7 = 1 &\rightarrow 4 y_4 \; mod\; 7 = 1 \rightarrow y_4 = 2 \end{aligned}$$

$$x = (140\times2\times1 + 105\times1\times1 + 84\times4\times1 + 60\times2\times0) \; mod\; 420$$
$$= 721 \; mod\; 420 = 301$$

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
- Chinese Remainder Theorem

References

1. W. Stallings. Cryptography and Network Security, 7th Edition, Pearson Education Australia, 2017.

2. Official textbook slides by L. Brown.

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