COMP8760 Lecture - 1

Introduction and Maths Revision

Sanjay Bhattacherjee

University of Kent

Lectures:

Budi Arief
B.Arief@kent.ac.uk

Sanjay Bhattacherjee
S.Bhattacherjee@kent.ac.uk
(Convener)

Class Supervisors:

- Imad Mahaini
  m.i.mahaini@kent.ac.uk
- Joshua Sylvester
  jrs71@kent.ac.uk

Institute of Cyber Security for Society

https://research.kent.ac.uk/cyber/

- a University-wide hub promoting interdisciplinary research and educational activities
- Academic Centre of Excellence in Cyber Security Research (ACE-CSR)
- Academic Centre of Excellence in Cyber Security Education (ACE-CSE)

Weekly Seminars

https://research.kent.ac.uk/cyber/events-2024/

Moodle

https://moodle.kent.ac.uk/2024/course/view.php?id=927

Finding a Room

https://www.kent.ac.uk/timetabling/rooms/index.html

When you click on the link for a room one of the things you will see on the page is directions to find your way from the building entrance to the teaching room.

Attendance

Remember to submit your own attendance!

https://student.kent.ac.uk/studies/presto-student

- Click on the above link
- Log into Presto

Today's Password

452539

Attendance Monitoring

- You may get emails and letters from the University if you missed too many sessions
- If you are holding a Tier-4 visa, this is a legal requirement

Time Table*

Lecture	Mondays	1:00 - 1:50 pm
Lecture	Thursdays	10:00 - 10:50 am
PC session	Thursdays	3:00 - 4:50 pm

* - subject to change

Homework and Study Material

Lecture Slides

- A printer-friendly version (without animations)

Worksheets on Lectures: For Practice, Not Graded

- Solutions will be published before the next Lecture

Worksheets for Classes: working towards Assessments

- Solutions will not be provided

Solve the worksheets to keep up with the lessons

COMP8760: Assessments

50% Coursework		(Based mostly on classes)
	30% Programming Assessment (On Sanjay's part)	Due on 12 November 2024
	20% Report (On Budi's part)	Due on 15 January 2025
50% Examination		May/June 2025 (Based mostly on lectures)

Tentative Outline: Sanjay's Part (Weeks 9-13, 15)

Week 9	Lecture 1	Introduction and Maths Revision
Week 9	Lecture 2	Modular Arithmetic, Prime Factorisation, Euclidean Algorithm, Mutually Prime
Week 10	Lecture 3	Groups, Rings and Mutually Prime Numbers
Week 10	Lecture 4	Primality Testing, Contrapositivity
Week 11	Lecture 5	Extended Euclidean Algorithm, Exponentiation
Week 11	Lecture 6	RSA: its Correctness and Security
Week 13	Lecture 7	Chinese Remainder Theorem, Legendre and Jacobi Symbols
Week 13	Lecture 8	Homomorphic Encryption, Goldwasser-Micali Encryption
Week 15	Lecture 9	Hash Functions
Week 15	Lecture 10	Authentication: Naive-RSA Signature, its Security
Week 16	Lecture 11	Stream Ciphers
Week 16	Lecture 12	Block Ciphers
Week 17	Lecture 13	Post-quantum cryptography I
Week 17	Lecture 14	Post-quantum cryptography II

Tentative Outline: Budi's Part (Weeks 16-19)

Week 12	Lecture 13	User Authentication (Basic Concepts and Passwords)
Week 12	Lecture 14	User Authentication (Cracking Passwords and Improving Textual Password)
Week 18	Lecture 13	User Authentication (Beyond Passwords 1)
Week 18	Lecture 14	User Authentication (Beyond Passwords 2)
Week 19	Lecture 13	Non-user Authentication
Week 19	Lecture 14	Access Control and Authorisation 1
Week 20	Lecture 13	Access Control and Authorisation 2
Week 20	Lecture 14	Accountability

Resources: For Sanjay's Part

Book 1	*Cryptography Made Simple*
Author	Nigel P. Smart.
	Link to eBook
Book 2	*A Graduate Course in Applied Cryptography*
Authors	Dan Boneh and Victor Shoup
	Link to website
Book 3	*Handbook of Applied Cryptography*
Authors	A. Menezes, P. vanOorschot, and S. Vanstone
	Link to website
Book 4	*Mathematics of Public Key Cryptography*
Authors	Steven D Galbraith
	Link to website

Study Material for Lecture 1

Book 1	*Cryptography Made Simple*
Author	Nigel P. Smart.
	Link to eBook

Section 1.1 Modular Arithmetic

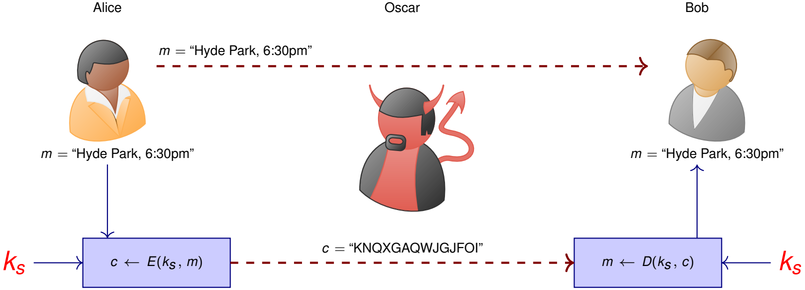
What is Cryptology?

Scientific study of “secure communication” in the presence of an adversary

What does “secure” mean?

Security property	Intuitive meaning	Mechanism
Confidentiality	message unintelligible	Encryption
Data Integrity	message unaltered	Hash functions
Authentication	source has not changed	Digital signatures
Non-repudiation	once committed, no way to deny	Digital signatures
Revocation	retraction of privilege	Encryption / Signatures

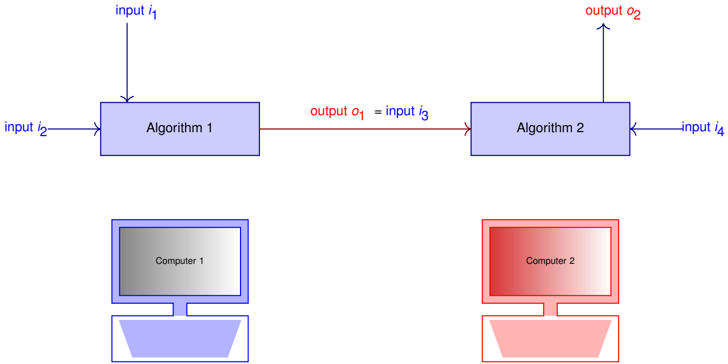
Symmetric Key Encryption System



First step towards confidentiality!

Algorithms / Computer Programs

- A set of instructions that execute on a computing device (laptop, mobile phone, et cetera).
- Data fed as input to the algorithm and provided as output by the algorithm



Key (A special kind of input to a cryptographic algorithm)

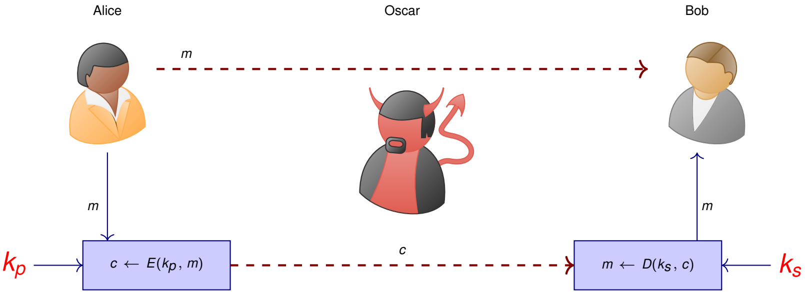
1011000110101011... (randomly generated 0's and 1's - bits)

Kerckhoffs's Principle

Nigel Smart's book (Section 10.1):

Any cryptographic system should be secure even if everything about the system,
except the secret key,
is public knowledge.

Asymmetric Key Encryption System



Confidentiality with
two different keys (k_s and k_p) of Bob (recipient)!

Symmetric vs Asymmetric Encryption

Symmetric

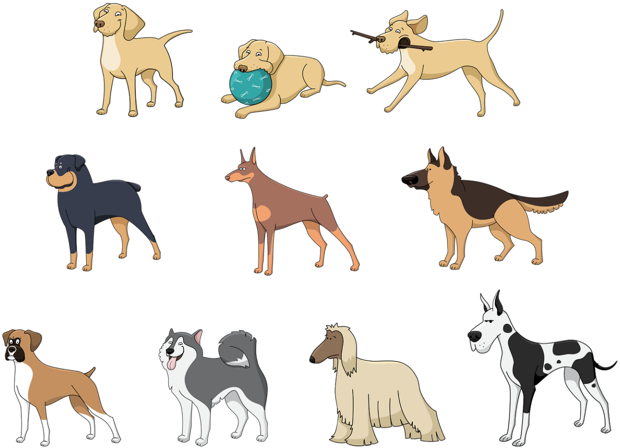
1. Same secret key k_s is used for encryption and decryption
2. To encrypt and send, the secret key k_s has to be known

Asymmetric

1. Public key k_p of recipient is used for encryption
2. Secret key k_s of recipient is used for decryption
3. To encrypt and send, the public key k_p has to be known

Set

A collection of elements

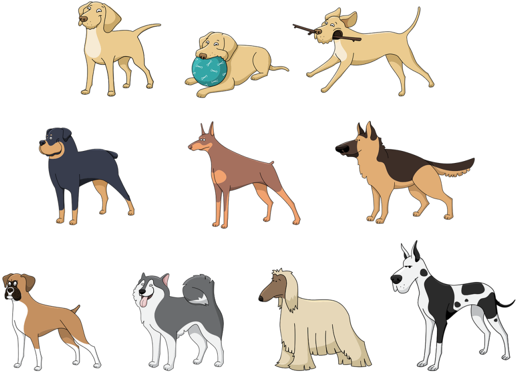


Let us denote this set of dogs by the letter A

Set Membership

$\in$

(belongs to)

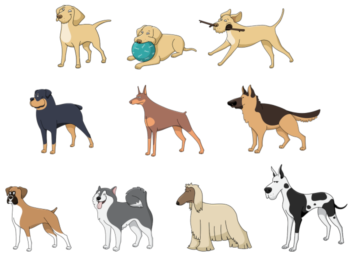


$\notin$

(does not belong to)

Cardinality

The number of elements in a set

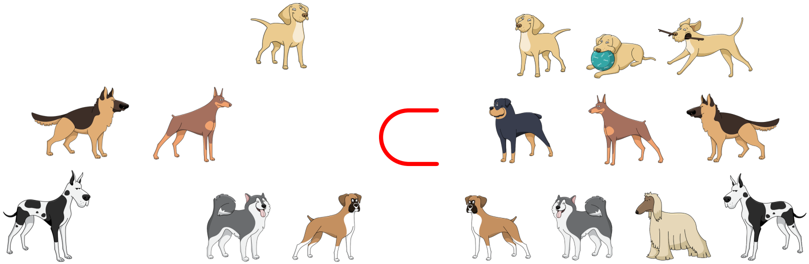
$\Bigg|$  $\Bigg| = 10$

We denote the cardinality of A by

$$|A|$$

Subset

A sub-collection of elements from the set



$$B \subset A$$

$$|B| = 6 \qquad |A| = 10$$

Integers: $\mathbb{Z}$

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Division Theorem

Let n, d be positive integers.

If we divide n (dividend) by d (divisor),
we get a unique quotient-remainder pair.

$$n = \underbrace{q}_{\text{quotient}} \times d + \underbrace{r}_{\text{remainder}}$$

and

$$0 \leq r < d.$$

Division Theorem: Examples

$$13 = \underbrace{\underline{2}}_{\text{quotient}} \times 5 + \underbrace{\underline{3}}_{\text{remainder}}$$

$$112 = \underbrace{1\underline{6}}_{\text{quotient}} \times 7 + \underbrace{\underline{0}}_{\text{remainder}}$$

Division Theorem: Negative n

If n is negative, q is taken to be negative, so that $0 \leq r < d$.

$$-13 = \underbrace{-3}_{\text{quotient}} \times 5 + \underbrace{2}_{\text{remainder}}$$

$$-112 = \underbrace{-16}_{\text{quotient}} \times 7 + \underbrace{0}_{\text{remainder}}$$

Clock Arithmetic / Modular Arithmetic

Hour	$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	$\pmod{12}$
Minute / Second	$\{0, 1, \ldots, 59\}$	$\pmod{60}$

$\mathbb{Z}_N$: set of remainders of N

$$\mathbb{Z}_N = \{0, 1, 2, 3, \ldots, N - 1\}$$

Some examples:

$\mathbb{Z}_2 = \{0, 1\}$
$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$\mathbb{Z}_{1001} = \{0, 1, \ldots, 1000\}$

The $\pmod{}$ operator

We define

$$a \pmod{N} = \underline{r}$$

remainder

This operator gives the remainder on dividing the integer *a* with *N*.

Examples

- $13 \pmod 5 = 3$
- $112 \pmod 7 = 0$

Congruent $\pmod{N}$

When $x - y$ is a multiple of N, we define

$$x = y \pmod{N}.$$

In other words, integers x and y both have the same remainder on dividing with N.

Examples

- $8 = 13 \pmod{5}$
- $21 = 112 \pmod{7}$

Modular Addition

We define

$$(x + y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

$$(6 + 7) \pmod 5 \quad = 13 \pmod 5 \quad = 3 \in \mathbb{Z}_5$$

$$(62 + 50) \pmod 7 \quad = 112 \pmod 7 \quad = 0 \in \mathbb{Z}_7$$

Modular Addition in $\mathbb{Z}_5$

For any two integers x and y,

$$x + y \pmod{N} \in \{0, 1, 2, 3, 4\}.$$

The following table shows the results of additions $\pmod{N}$ of all elements of $\mathbb{Z}_5$ with each other.

Addition $\pmod{5}$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Modular Multiplication

We define

$$(x \times y) \pmod{N} =$$

$$z \pmod{N} = \underbrace{r}_{\text{remainder}} \in \mathbb{Z}_N$$

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$$(6 \times 7) \pmod{5} = 42 \pmod{5} = 2 \in \mathbb{Z}_5$$

$$(62 \times 50) \pmod{7} = 3100 \pmod{7} = 6 \in \mathbb{Z}_7$$

Modular Multiplication in $\mathbb{Z}_5$

For any two integers x and y,

$$x \times y \pmod{N} \in \{0, 1, 2, 3, 4\}.$$

The following table shows the results of multiplications $\pmod{N}$ of all elements of $\mathbb{Z}_5$ with each other.

Multiplication $\pmod{5}$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Algorithm: Check if n is prime or composite

- For each divisor $2 \leq d \leq \sqrt{n}$: {
  - If $n \mod d = 0$, then n is not a prime: {
    - hence, break the loop.

    }

  }
- If the above loop was not broken, then n is prime, else it is composite.

Note: $\sqrt{n}$ is a positive number such that $(\sqrt{n})^2 = n$

Prime Numbers

Is 56 a prime number?

No, $d = 2$

Is 57 a prime number?

No, $d = 3$

Is 59 a prime number?

Yes

Prime Numbers $\leq$ 100

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	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Prime Factorisation

Definition:

The prime factorisation of a positive integer n is defined as

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

where

- $p_1, \ldots, p_k$ are prime numbers and
- $\alpha_1, \ldots, \alpha_k$ are positive integers

Examples:

2	$= 2^1$
13	$= 13^1$
26	$= 2^1 \times 13^1$
3468	$= ?$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 = 0$	$289 = 11^0 \times 289$	$n_6 = 289$
$n_6 = 289$	$p_6 = 13$	$\alpha_6 = 0$	$289 = 13^0 \times 289$	$n_7 = 289$
$n_7 = 289$	$p_7 = 17$	$\alpha_7 = 2$	$289 = 17^2 \times 1$	$n_8 = 1$

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$\begin{aligned}
3468 \quad &= 2^2 \times 867 \\
&= 2^2 \times 3^1 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 11^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 11^0 \times 13^0 \times 289
\end{aligned}$$

We omit the primes with exponent 0 to write it in compact form:

$$3468 = 2^2 \times 3^1 \times 17^2.$$

LCM and GCD

Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \alpha_i \geq 0$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \beta_i \geq 0$$

Then,

$$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

and

$$gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}.$$

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm 1:

- Find the prime factorisation of both a and b
- $$lcm(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Example: $lcm(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$
- $lcm(20, 12) = 2^{\max(2,2)} \times 3^{\max(1,0)} \times 5^{\max(0,1)} = 2^2 \times 3^1 \times 5^1 = 60$

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm 1:

- Find the prime factorisation of both a and b
- $$gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}.$$

Example: $\gcd(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$
- $\gcd(20, 12) = 2^{\min(2,2)} \times 3^{\min(1,0)} \times 5^{\min(0,1)} = 2^2 \times 3^0 \times 5^0 = 4$

Reminder: Homework

Worksheet: For Practice, Not Graded

- Available on Moodle
- Solutions will be published before Lecture 2

Interesting Reads:

- Nigel Smart's book, Part 2: Historical Ciphers
- D. Kahn. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1996.
- S. Singh. The Codebook: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography. Doubleday, 2000.

Summary

- Introduction to COMP8760
- Introduction to Cryptography
- Sets
- Modular Arithmetic
- Prime Numbers, GCD and LCM

Thank you for your kind attention!