CSCI971/471
Modern Cryptography

Subject Introduction

Rupeng Yang

SCIT UOW

Health and Safety Information for Students

Commencement of Session

UNIVERSITY OF WOLLONGONG AUSTRALIA

What to do in an emergency?

KEEP CALM – STAY SAFE

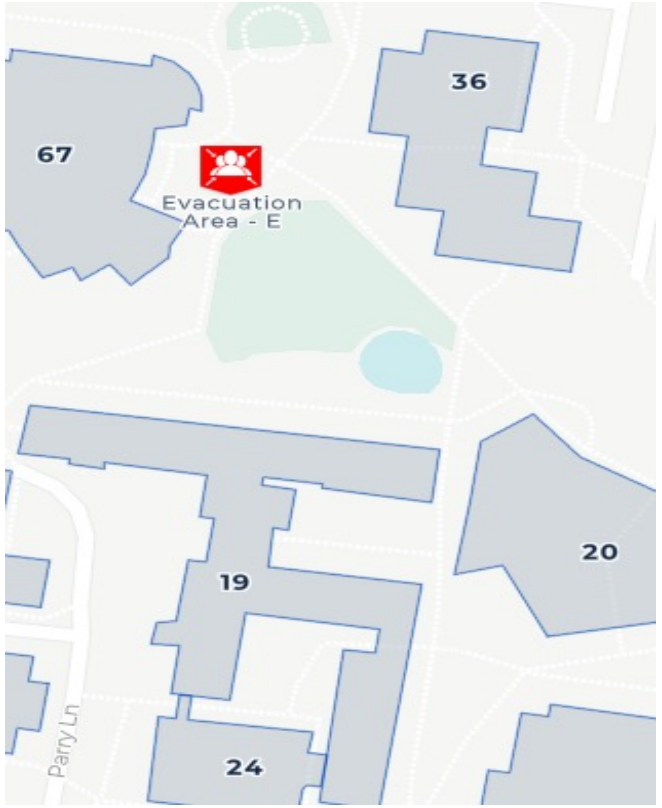
If the alarm sounds or you are notified to evacuate:

- Follow instructions of building warden or staff member
- Leave by the nearest safe emergency exit
- Proceed to your emergency evacuation assembly point
- Await further instructions
- Do not return to the building until it is safe to do so

If required to take shelter:

- Follow instructions of building warden or staff member
- Lock doors, close windows/blinds and seek refuge
- Await further instructions

The nearest assembly area for this building is:

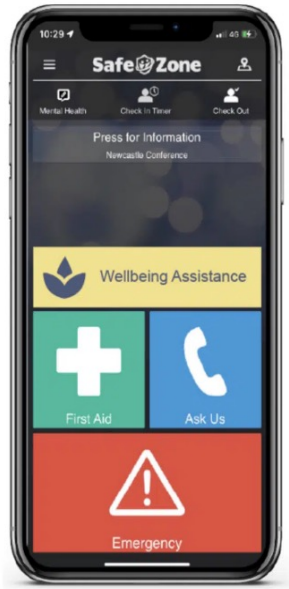


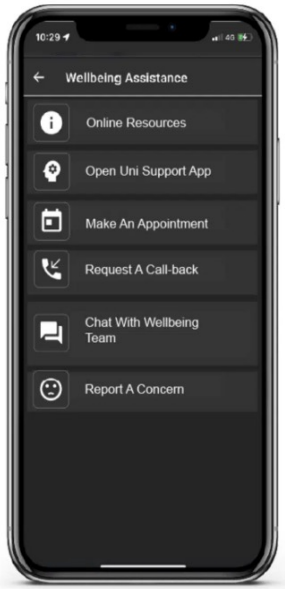
Need assistance on campus?

WE ARE HERE TO HELP

If you require first aid or medical assistance while on campus:

- Locate a first aid officer, or
- Call UOW Security on 4221 4900, or
- Use Wellbeing Assistance, First Aid or Emergency buttons on SafeZone App available free for iOS, Android and Windows.





Reporting hazards

KEEPING YOUR UNIVERSITY SAFE AND COMFORTABLE

If you notice any hazards (e.g. broken furniture or equipment) in your teaching area or anywhere on Campus:

- Report it to your Lecturer/Tutor/Supervisor
- The University has an online hazard and incident reporting tool called SafetyNet
- Report IT equipment hazards to Information Management and Technology Services on 4221 3000
- Report building and grounds hazards to Facilities Management Division on 4221 3217

Smoke-Free University

SAY GOODBYE TO SECONDHAND SMOKE

All UOW public areas including buildings, eating areas, grounds, pathways and transport stops have been smoke-free since July 2016.

This includes the use of vapes and e-cigarettes.

Please co-operate with this policy to help make our campus healthier for everyone.

For more information:

uow.info/smoke-free

For more information: uow.info/safe-at-work

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contact Info

Dr. Rupeng Yang

Room: 3.212

Email: rupengy@uow.edu.au

If you email me it makes it easier if you include the subject and topic in the subject line: For example: CSCI971: Assignment 1.

- This way I can tell if an email is about almost due assessment or similar important matters.
- While I generally reply to emails within a couple of working days there will be times when other activities may take priority.
- **Use your university email.**

Consultation times

Dr Yang’s consultation times:

Friday:	09:30 – 10:30
Friday:	13:30 – 16:30

The consultation is face-to-face at 3.212

Please book a consultation at least 30 mins in advance via email

Consultation hours are subject to change under some circumstances such as public holidays or urgent meetings.

Subject contact hours

- Lectures (W1 – W13):
  - Friday: 10:30 – 12:30

- Workshops (W2 – W12):
  - Friday: 12:30 – 13:30 (By Dr. Rupeng Yang)
  - Friday: 13:30 – 14:30 (By Ms. Parisasadat Shojaei)
  - Friday : 14:30 – 15:30 (By Ms. Parisasadat Shojaei)

  - Friday : 12:30 – 13:30 (By Dr. Mir Md. Jahangir Kabir)

- Webex Links are also available on Moodle

Subject contact hours

- This subject is worth 6 credit points.
- Each week we will have a 2-hour lecture and a 1-hour workshop.
- According to University policy, 1 credit point is equivalent to 1.5 to 2 hours of work including class attendance, per week.
- So you should be doing about 6 to 9 hours of work a week on this subject outside of class attendance.

The Moodle Site

- The subject materials are available in Moodle
- Check the Moodle site for this subject regularly
  - Any change to the subject will be announced on the Moodle site.
  - Any information posted to the Moodle site is deemed to have been notified to all students.
- Check SOLS mail too, since urgent updates are likely to be sent there.

What is this subject about

- Basic security & cryptography concepts and principles
- Cryptographic Schemes
  - Why we need it
  - What properties it should have
  - How to construct it
  - Why it is (in)secure
  - How to implement it
- Basic cryptanalysis
- Cryptographic applications

The objectives of this subject

1. Understand modern cryptographic techniques.
2. Undertake basic cryptanalysis on cryptographic schemes.
3. Apply appropriate techniques to design cryptographic schemes satisfying specific conditions.
4. Evaluate the design of modern cryptographic schemes.

No coding

No complex computation

But abstracted notions.

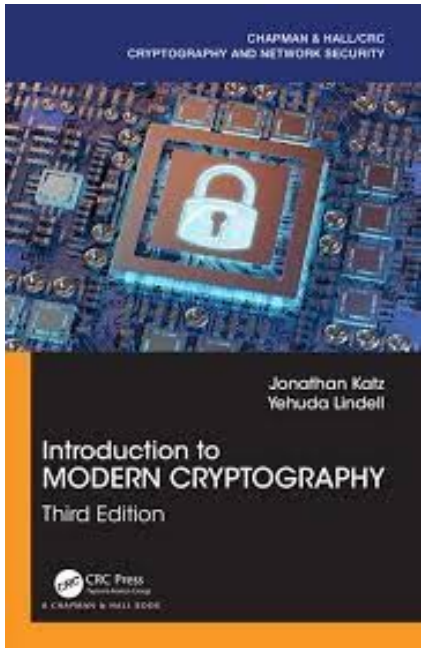
Subject contents

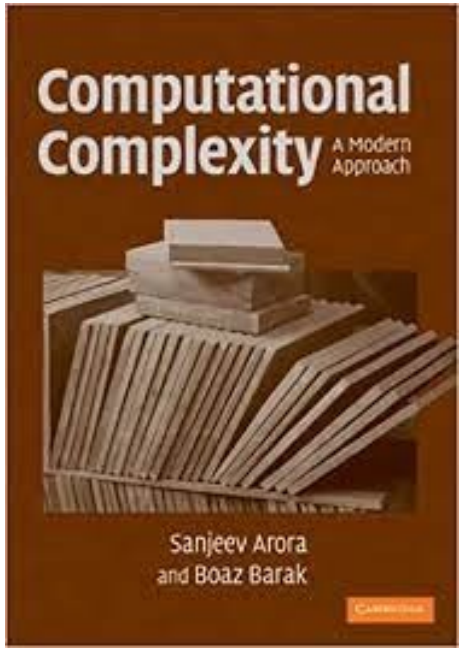
- Week 1- Week 2: Introduction & Basic Notions
- Week 3 – Week 4: Symmetric-key Cryptography
  - Tools: Block Cipher, Stream Cipher, Hash
  - Symmetric-Key Encryption
  - Message Authentication Code
- Week 5 – Week 7: Public-Key Cryptography
  - Tools: Number Theory
  - Public-Key Encryption
  - Digital Signature
- Week 8 – Week 12: Advanced Topics
  - Zero-Knowledge Proof
  - Identity-Based Cryptography
  - Multi-Party Computation
- Week 13: Revision

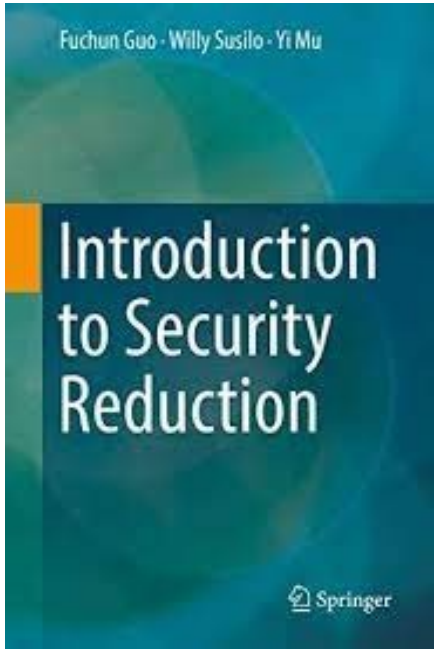
Recommended readings (No need to buy)

- Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, 2nd Edition, 2015

- Arora, Sanjeev, and Boaz Barak. Computational complexity: a modern approach. 2009
- Fuchun Guo, Willy Susilo, Yi Mu, Introduction to Security Reduction, Springer, 2018







Assessment tasks

- Two individual assignments (25% each)
  - Due in Week 6 & 12
  - Problem solving, cryptographic algorithm/protocol design, cryptanalysis

- 01 Sep 2024 (Sunday in Session Week 6) Final submission time: 11:30pm
- 20 Oct 2024 (Sunday in Session Week 12) Final submission time: 11:30pm

- Final exam (50%)
  - Online or hand-written (as per university instruction)
  - Students will receive a SOLSmail advising full details of the delivery format, time, and date of the final exam as they become available in the SOLS Exam Timetable.

How do you pass this subject

- You need to get at least 20/50 in the final exam.

AND

- Overall you need to get at least 50.

Assignment submission

- Assignments must be submitted via the submission links in Moodle
- No email submission
- Penalties apply to all late work, except if student academic consideration has been granted.
- Late submissions will attract a penalty of 5% of the assessment mark per day including weekends.
- Work more than four (4) days late will be awarded a mark of zero.

Plagiarism

- There are two primary concerns for us:
  - Students copying each other.
    - You can discuss ideas but need to write down your solution independently!
    - With mathematical solutions you need to work fairly independently.
  - Students copying directly without appropriate referencing.

Why to learn this subject

1. I hope to conduct researches on cryptography.
2. I hope to work as a cybersecurity engineer.
3. I hope to work as a general software engineer.
4. I do not know, but I am in the cybersecurity major, I need credits, …

Questions?

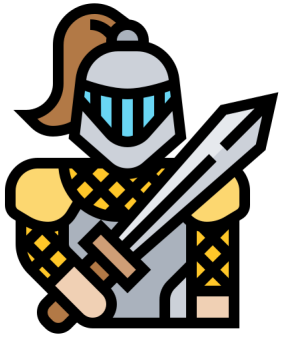
Warmup

- 37 mod 11=
- 00110101 $\oplus$ 10110011 = ($\oplus$ means xor)
- What is the binary representation of 117
- What is the hex representation of 117
- Is 97 a prime number
- Is 143 a prime number
- What is the greatest commond divisor of 117 and 72
- 76696691205 * 345457934806 mod 100 =
- 9^{1023} mod 80 =

Questions?

Why we need cryptography?

Why we need cryptography?

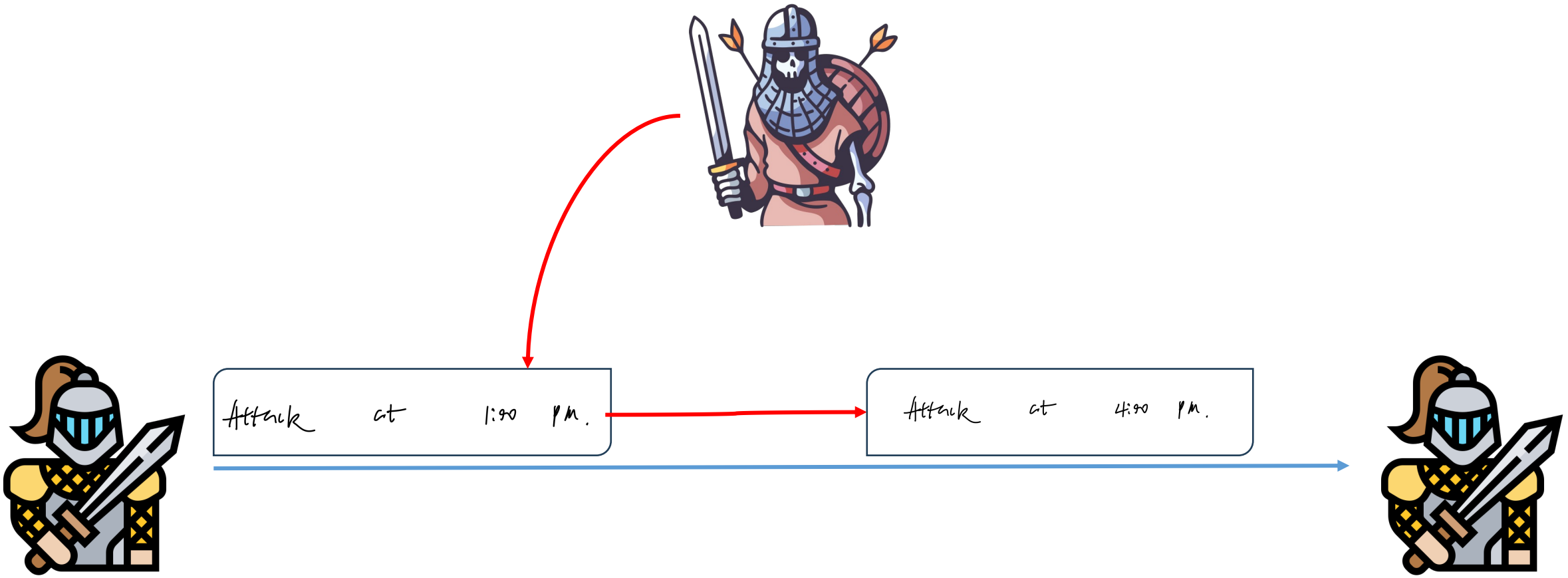


Why we need cryptography?

We need cryptography to protect the confidentiality of information.

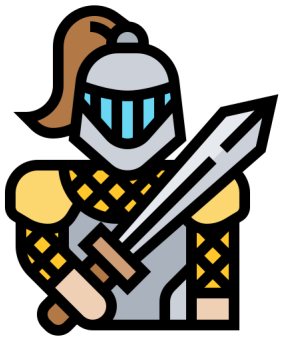
Why we need cryptography?

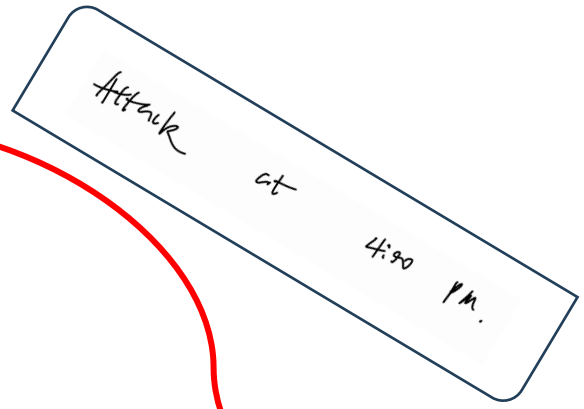
We need cryptography to protect the integrity of information.



Why we need cryptography?

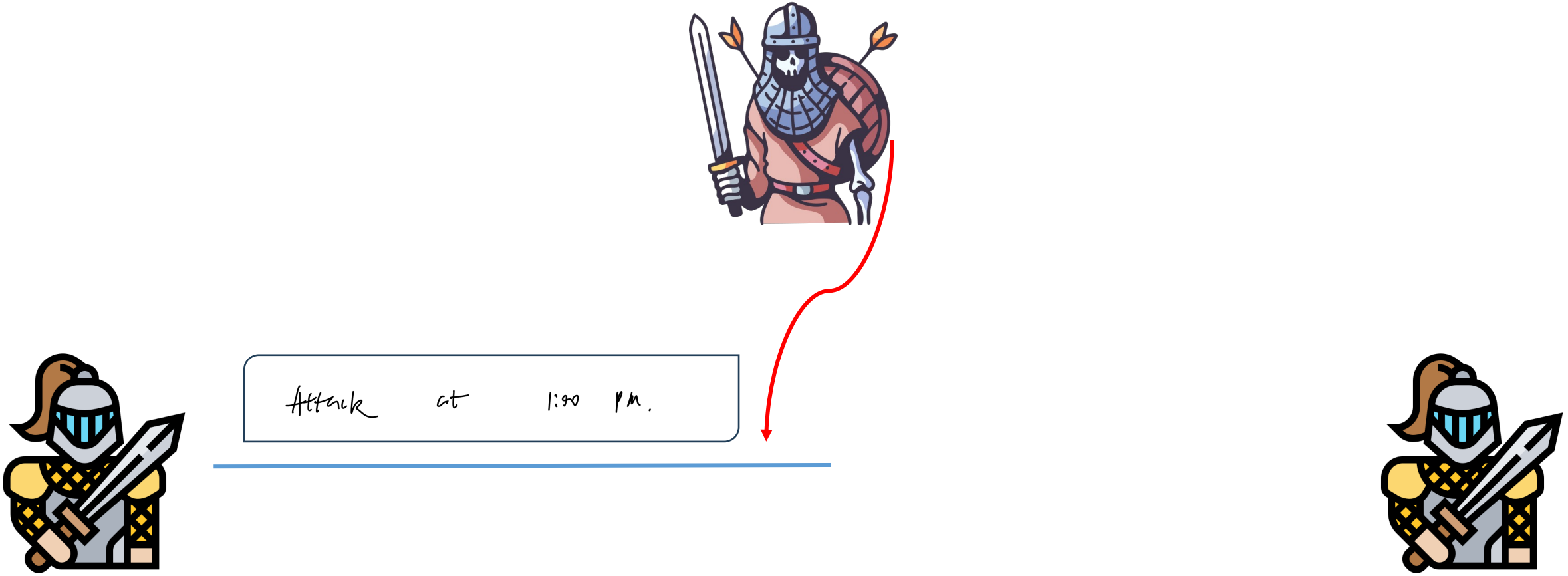
We need cryptography to protect the integrity of information.





Why we need cryptography?

We need to protect the availability of information. Usually, this is outside the scope of cryptography.



Why we need cryptography

- Cryptography can help us to achieve specific security goals against attacks from adversaries.
- Why does security matter?
  - To protect your money
  - To protect your privacy/secret
  - To protect your intellectual property
  - …
- Who needs security?
  - Governments: To safeguard military or diplomatic communications and to protect national interests.
  - Private sector: To protect sensitive information such as health and legal records, financial transactions, commercial secrets; To protect information ownership.
  - Individuals: To protect sensitive information, and to protect an individual's privacy in the electronic world; Allow E-commerce, internet banking and so on.

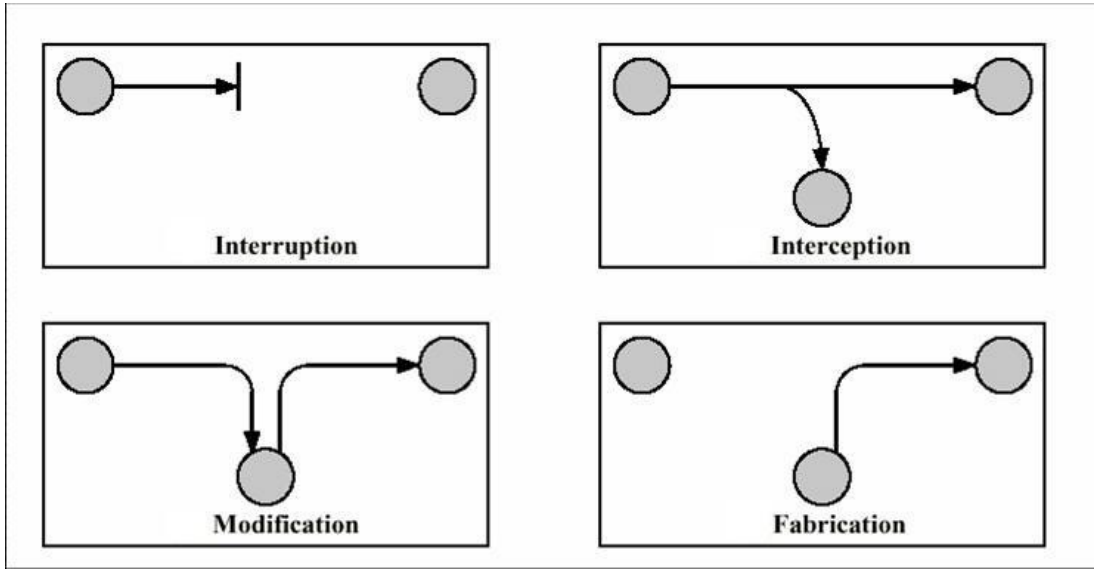
Common Security Goals - CIA

- ***C****onfidentiality*: Information should be inaccessible to unauthorised parties.
- ***I****ntegrity*: Information should be unmodifiable without detection, by unauthorised parties.
- ***A****vailability*: Information should be available to authorised people.

- Some other security goals:
  - Privacy
  - Authenticity
  - Accountability
  - Non-repudiation
  - …

Basic Attack Types

- Interruption: an attack on availability of an asset.
  - Hardware destruction, software erasure.
- Interception: an attack on confidentiality.
  - Wiretapping network, illegal copying of files.
- Modification: an attack on integrity.
  - Modifying stored or transmitted data.
- Fabrication: an attack on integrity /authenticity.
  - Pretending to be someone else.



Passive Attack VS Active Attack

- A passive attack attempts to learn or make use of information from the system but does not affect system resources

- An active attack attempts to alter system resources or affect their operation

Classical Cryptography (Classical Ciphers)

Cryptography

Cryptography (before 1883)

Cryptography = Encryption + Decryption

Encryption= Encryption Algorithm (transform plaintext to ciphertext)
Decryption=Decryption Algorithm (transform ciphertext to plaintext)

Plaintext: the original clear message
Ciphertext: the transformed message that hides the plaintext

Cryptography is only about confidentiality in this stage. The word cryptography is from the Greek words:

- *kryptos*: Hidden
- *graphein*: to write

Can you decode the following?

|_ |= _|

Number	Encoding
1	_|
2	|_|
3	|_
4	=|
5	□
6	|=
7	-|
8	|-|
9	|-

1	2	3
4	5	6
7	8	9

Kerckhoffs' principle

Why?

- It is hard to protect the secrecy of the whole algorithm. Sometimes, leaking little inoformation about the algorithm may ruin the whole algorithm.
- It is hard to redesign a new algorithm compeltely.

We need some object that is easier to hide and easier to recreate. This is denoted as a secret key.

Usually, the secret key is a short string.

- It is much easier to keep a short key secret
- If the key is exposed, it is easier to change the key
- It is easier for many people to use the same algorithm but different keys, rather than using different algorithms

The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

Cryptography

Cryptography (1883-1976)

Cryptography = Encryption + Decryption

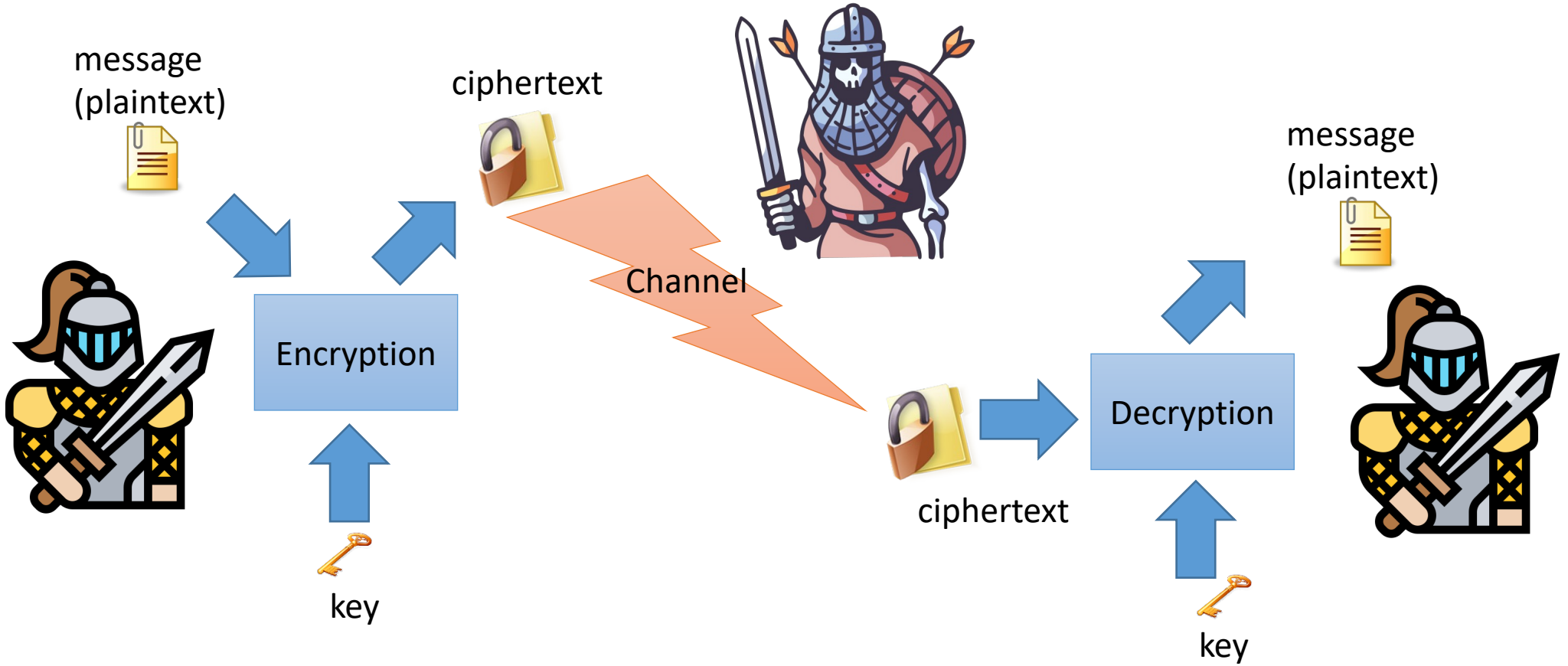
Encryption= Encryption Algorithm + Secret Key (transform plaintext to ciphertext)
Decryption=Decryption Algorithm + Secret Key (transform ciphertext to plaintext)

Plaintext: the original clear message
Ciphertext: the transformed message that hides the plaintext
Secret key: a secret data unit used for encryption and decryption.

Cryptography is only about confidentiality in this stage. The word cryptography is from the Greek words:

- *kryptos*: Hidden
- *graphein*: to write

The Basic Model



The Basic Secrecy Channel

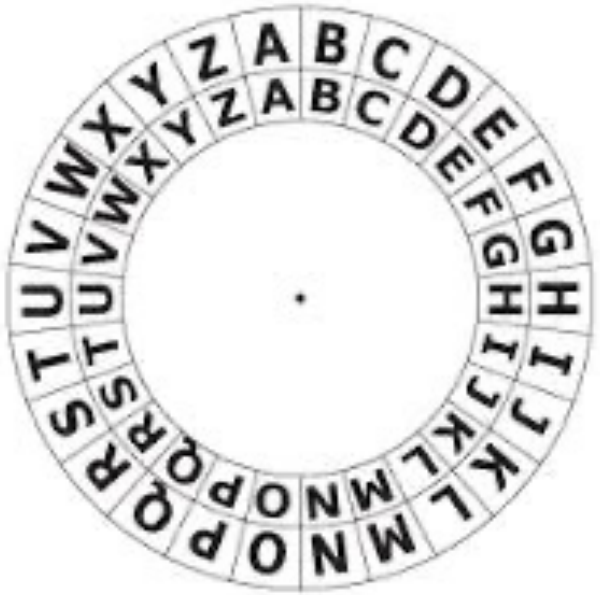
- The channel can be a communication channel or a storage channel
- Sender (Alice) wants to send a message M to the Receiver (Bob), through this channel, such that the opponent/enemy/intruder/adversary (Eve) cannot access M.
- Alice applies a transformation, known as **encryption**, to M, referred to as the **plaintext**, to produce a garbled message C, referred to as the **ciphertext.**
- Then Alice sends the **ciphertext** C to Bob via the insecure channel.
- Bob applies another transformation, known as **decryption**, to the **ciphertext** C to obtain the **plaintext** M again.
- The adversary Eve should not learn any information about the **plaintext** M from the **ciphertext** C even if it controls the channel.

Classical Ciphers

- Caesar Cipher
- Shift cipher
- Substitution Ciphers
- …

Caesar Cipher

- Julius Caesar 2000 years ago
- Substitution: a letter is replaced by another letter (the original Caesar cipher is a shift cipher)



What is the original message?

Fubswrjudskb lv dq lqwhuhvwlqj vxemhfw

Cryptography is an interesting subject

Caesar Cipher – An additive cipher

- 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
```

- Algorithm can be expressed as:

$$c = E(3, p) = (p + 3) \bmod (26)$$

Shift Cipher

- 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

- A shift may be of any amount, so that the general Caesar algorithm is:

$$C = E(k, p) = (p + k) \bmod 26$$

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

$$p = D(k, C) = (C - k) \bmod 26$$

- Is shift cipher secure?

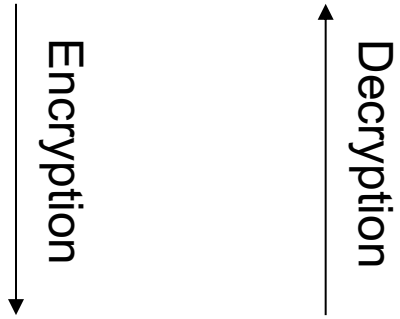
Monoalphabetic Substitution Ciphers

- Make a substitution table

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XZYABCDWFGHIJSLMNOPQRKTUVE
```

- Example

Plaintext: **HELLO**
Ciphertext: **WBIIL**



- How Many Possible Keys are there?

$$26! \approx 4 \times 10^{26} \approx 2^{88}$$

- Does Monoalphabetic Substitution Cipher Secure? NO!

Summary

- Why we need cryptography
  - Security goals
  - Basic attack types
- Classical Ciphers
  - Kerckhoffs' principle
  - The basic model
  - How the ciphers work