Week 2

Lecture 1
Part -1 Extended GCD Algorithm and Related Computations

Part 2 - Symmetric key Cryptography

Lecture 2

Properties of Numbers,

Workshop 2: Workshops start from this week.

Quiz 2

Sym graphy

COMP9

Lecture 2-Part II

Symmetric key Cryptography

Lecture 2 Part II

1.1 Symmetric Cipher Models
- Basic Terminology
- Model and Logical View
- Basic Requirements and Kerckhoffs's principle

1.2 Security
- Characterization of S
- Attacks on Symmetri

1.3 Classical Ciphers
- Substitution Ciphers
  - Caesar and Affine Ciphers
  - Monoalphabetic Substitution Ciphers
- Transposition Ciphers
  - Rail fence cipher
  - Row Transposition Cipher

1.4 Cryptanalysis of Classical Ciphers
- Caesar Cipher
- Affine Cipher
- Monoalphabetic Substitution Ciphers

1.5 Complex Ciphers
Polyalphabetic CiphersVigenère Cipher

1.1 odels

COMP9

Lecture 2-Part II

Symmetric Key Encryption

- Conventional encryption since antiquity-known as single key or private key or **symmetric key** systems.

- A same key is used for both encryption and decryption.

- One of the main ass receiver should have access to the symmetric key used in th

- Widely used in practice.

- Examples: DES, AES etc.

Terminology

- **Plaintext** - Source message
- **Ciphertext** - Encrypted message
- **Cipher** or Encryption Algorithm- Procedure for transforming plaintext to ciphertext

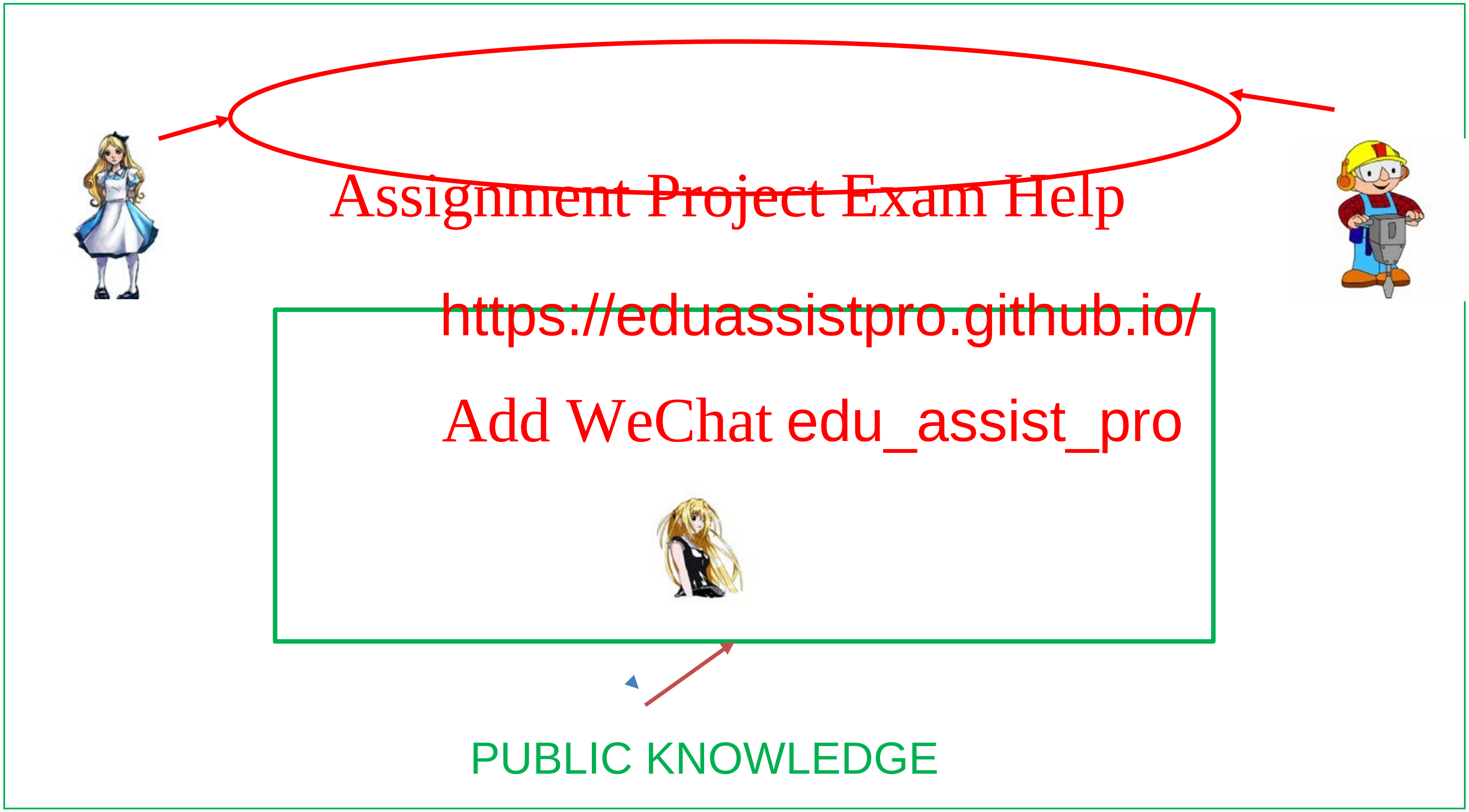
- **Key** – info or secret nder/receiver

- **Encipher (encrypt)** - Converting plainte

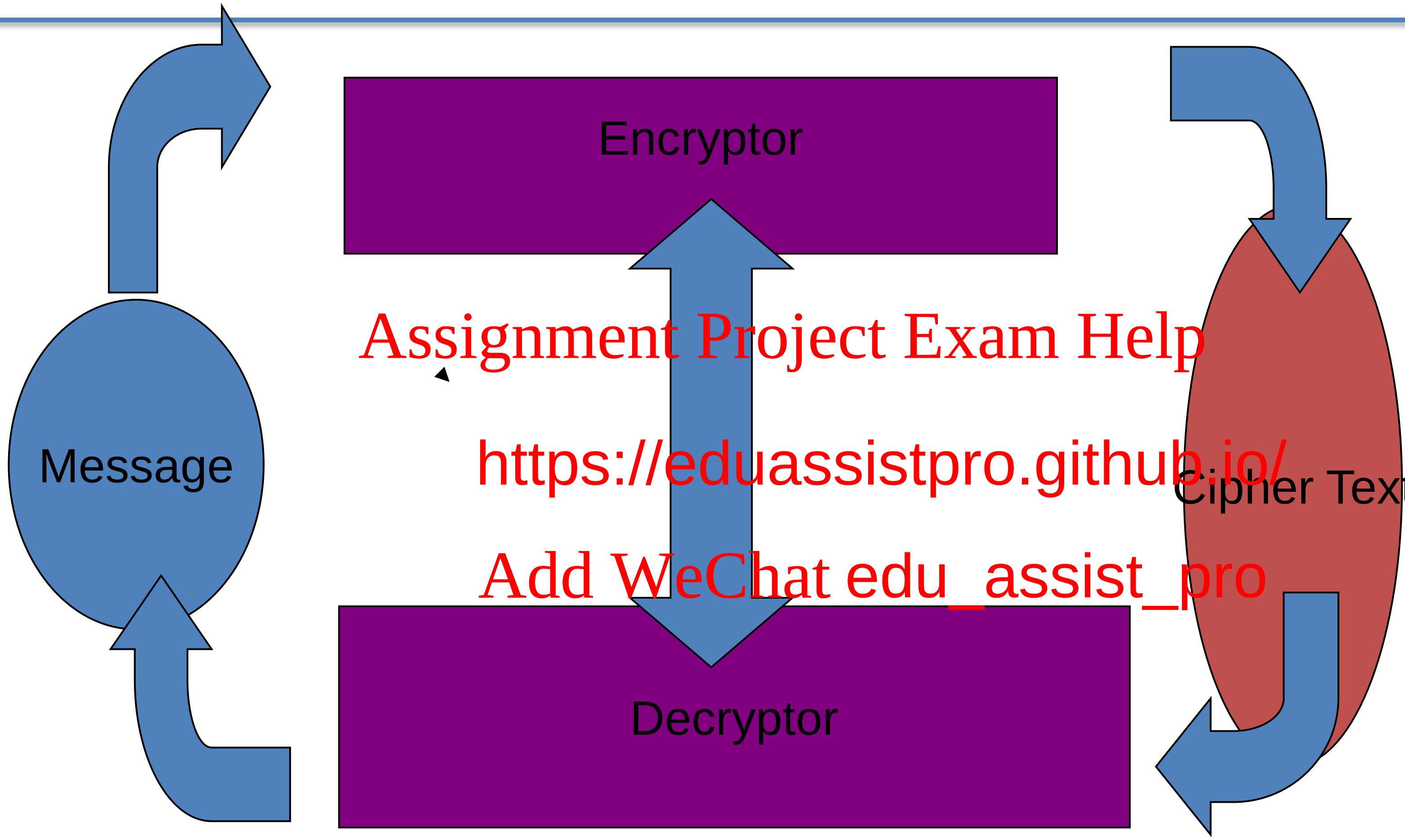
- **Decipher (decrypt)** - Recovering plainte ext
- **Cryptography** - Study of encryption principles/methods
- **Cryptanalysis (codebreaking)** - Study of principles/ methods of deciphering Ciphertext *without* knowing key
- **Cryptology** - Field of both cryptography and cryptanalysis

Model for Symmetric Key Cipher

Modified From:Stallings Figure 2.1:



Logical View of Symmetric Key System



Block diagram of a Symmetric Key System: Logical view

Basic Requirements and Kerckhoffs's principle

- If Cipher Algorithms are kept secret from adversaries, will it help achieving security for the sender and receiver?
- Kerckhoffs's principles argues that security through obscurity is not recommended.
- All algorithm detail should be obtained by using only secrecy
- Stallings recommends two essential req
  - A strong encryption algorithm
  - A secret key known only to participants.
- In symmetric key systems security it is a mandatory requirement that keys are to be kept secret between sender and receiver.

1.2 Security

COMP9

Lecture 2-Part II

Model of Symmetric Key Usage

Opponent

$Y = E(K, X)$

$X = D(K, Y)$

From Stallings Figure 3.2:

Users Perspective:Symmetric key Encryption

Crypto systems have 3 independent Dimensions according to Stallings.

- Algorithm for Ciphers: Transformation details of plaintext to cipher text. They are based on mathematics, heuristics and pragmatic ideas.

- Number of Possibl e better protection.

- Types of Plaintext/Cipher text processi

  - Stream ciphers: plaintexts are streamed to cipher producing stream of ciphertexts element by element.
  - Block Ciphers: plaintext is divided into blocks of data, cipher process one block at a time

Opponent's Perspective: Cryptanalysis

- Main task for him to be able to decrypt ciphertexts without access to keys.
- Usually the objective is to obtain keys by observing plaintext/ciphertext pairs called **Cryptanalysis**. In principle, opponent can get all information about cryptosystem

- Keys should be large enough such that exhaustive key search is impossible.
- There are types of Cryptanalytic attacks based on capability of opponent's model.
- **Ciphertext only, Known plaintext, Chosen plaintext, Chosen ciphertext, Chosen text:**

Computing View of Security

- The attack models described earlier is based on the model of modern Information and Communication that exists today.
- Adversaries are the entities on communication network who can deploy various services to watch, collect, record and process information that flows at the points t entralized o distributed architecture.

- Two important definitions are interest uch of the cryptologic research of modern times are based.

- **Unconditional Security (Shannon):** The security of the cipher is independent of the computing resource available to the adversaries.
- **Computational Security (Turing):** Adversaries are provided with constrained computing resources and the security of the cipher determined by the size of the computations required to break the cipher.

Implications of Brute-force Attack

- To break a ciphertext C = E(K,M), one could try all possible messages, but that is generally futile as the space is large. And if even we break one ciphertext, one may need to repeat the same steps for every ciphertext. Not a feasible approach.
- Next best thing you can hope is to brute-force on every possible keys.
- You realize immedi oportional to the size of the key space.
- Of course you assume you have a metho laintext while trying all possible keys.
- Generally the size of the key space will tell you the complexity of the Brute-force key attack.
- You need at least 128 bit key to protect against this attack in practice based on assumption that adversaries are equipped with classical computing resources.
- We need to increase the key size to protect against Quantum computing attacks (we will deal later)

rs

COMP9

Lecture 2-Part II

Classical Ciphers

- Why do we study?

- They are based on simple properties of plaintext alphabets and are known from antiquity.

- Help us to illustrate ysis in a simple language easy to follow.

- The ideas behind methods and analysis of these schemes have parallels in the design and analysis of modern symmetric key schemes.

Types of Classical Ciphers

- Substitution Ciphers
  - Here plaintext symbols are substituted or replaced with other symbols using an unknown key.
  - The substitutions can be performed as sequence of symbols or symbol by symbol.

  - Eg RANDOM

- Transposition Ciphers
  - Here plaintexts are organized as a sequence of plaintext blocks and symbol positions in each block are permuted or transposed using a key. The same permutation is used for every block
  - Eg. RANDOM LETTER -> MORADN RELETT

Caesar Cipher

- Historically attributed to Julius Caesar
- Assumes letter ordering in a language.

- For example, in English

- The alphabet order STUVWXYZ

- Consider plaintext in sequence, each letter is replaced with the letter that stands in a certain secret(key) places further in the alphabet.
- Example: when k =3, can you decrypt this ciphertext:
- `PHHW PH DIWHU WKH WRJD SDUWB`

Caesar Cipher Mathematically

- P:= Plain Text Space = Z_{26} Space
- C:=Cipher Text Space = Z_{26}

- p: = plaintext c:=ci

- Encryption: E(k,p) = c = p + k mod 26
- Decryption: D(k,p) = c – k mod 26

- What is the size of the key space?

Affine Cipher

- P:= Plain Text Space = Z_{26} Space

- C:=Cipher Text Space = Z_{26}

Key space = (Z_{26}, Z_{26}),

Key k = (a,b, a, b belo $_{26}$

- p: = plaintext c:=ciphertext
- Encryption: E(k,p) = c = ap + b mod 26
- Can you Determine the decryption function?
- Decryption: D(k,p) = Inverse(a)(c – b) mod 26
- What is the size of the key space?

Monalphabetic Cipher

- We considered two simple functions as Caesar and Affine Ciphers before.
- In fact, we can consider a more general key using a general permutation on 26 alphabets.
- Thus, a key is a p 26 (plaintext letter maps to a differen
- Consider an exam tion:
- **ABCDEFGHIJKLMNOPQRST**
- **DKVQFIBJWPESCXHTMYAU**
- Exercise: Complete the Encryption of the following phrase:
- **Message: newcoronaviruscasescross**
- **Ciphertext: xf…..**
- **How many possible keys?**

Transposition Ciphers

- A permutation of plaintext symbols are employed here as opposed to substitution.

- As a result l ged for every d positions.

- Divide plain text as seq laintext blocks of certain size say, d.
- Then apply a permutation to every d positions of the plaintext. The permutation is the key.

Rail Fence cipher

- A simpler technique where message is written out diagonally over a depth of certain rows (say d). Then ciphertext is read row by row.
- Example from the textbook:

- eg. write me

m e m a t r

e t e f e t e o a a t

- giving ciphertext

MEMATRHTGPRYETEFETEOAAT

- Such ciphers are easy to break if depth is small.

Row Transposition Ciphers

- A more complex Transposition Cipher is by employing a permutation on blocks of columns, when messages are written row by row.
- An example from the textbook:
- Write letters of message out in rows over a specified number of columns
- Then reorder the co efore reading off the rows


```
Key:        3 4 2 1 5 6 7                7 Columns
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: TTNA APTM TSUO AODW COIX KNLY PETZ
```

- Convention for the key
- (1 2 3 4 5 6 7)   Input Order
- (3 4 2 1 5 6 7)   Output Order

1.4 Cryp al Ciphers

COMP9

Lecture 2-Part II

Caesar Cipher

- There are only 26 possible keys, In fact, only 25 non-trivial keys.
- You could mount a simple Brute-force attack.
- Try applying shifts ext from 1 to 25, when you recognize som
- Can you break the ciphertext:
- GCUA VQ DTGCM
- I have provided some magma code on the lms try them.

Affine Cipher

- How many different keys?
- What is the complexity of Brute-force search?
- See a Work eek.

General Monoalphabetic Cipher

- How many different keys?
- 26!

- Brute-force seems i e cipher is safe?

- Language statistics comes into play.

- In English some letters appear more frequent than others, for example “e” appears more frequently followed by “t” etc, A monoalphabetic cipher always maps a distinct alphabet to another symbol. So the mapping preserves the language statistics. With this one can start guessing which is “e” which is “t” etc.

Language Frequencies

From Stallings Fig. 3.5

The original ideas were developed in 9th Century by Arab an

ns.

textbook fo ion

There are now automated methods on Internet rs

COMP9

Lecture 2-Part II

Polyalphabetic Cipher

- How do you make the encryption process more complex so that it is difficult to break?

- Use a set of monoalphabetic ciphers at different time when processing plaintext sequence.

- A key could be used to specify which [illegible]ic cipher to use in a given time context.

- The textbook has some examples, please follow them.

THE UNIVERSITY OF MELBOURNE

Vigenère Cipher

- This is a simple polyalphabetic substitution cipher.
- Here a set of Caesar ciphers is employed.

- ith plaintext symbol key: $k_{(i \bmod d)}$

- The idea is very simple, a key is a multip $= k_1 \, k_2 \ldots k_d$
- $P = p_1 \, p_2 \ldots p_d \, p_{d+1} \, p_{d+2} \ldots p_{2d} \ldots$

- $C = c_1 \, c_2 \ldots c_d \, c_{d+1} \, c_{d+2} \ldots c_{2d} \ldots$
- Encryption: $E(K,P) = C$, where $c_i = p_i + k_i \bmod 26$
- Decrypton: $D(K,C) = P$, where $p_i = c_i - k_i \bmod 26$
- If d is large it offers better security.

Example of Vigenère Cipher

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZHCQYGLMGJ

THE UNIVERSITY OF MELBOURNE

Product Ciphers

- Substitution and Transposition Ciphers are not secure as they are vulnerable to cryptanalysis based on plaintext language characteristics.

- We can think of more general product cipher by applying several substitution and tra n.

- These ideas are were used in German c orld war time-see section on Rotar Machines in the textb

- This is a link to modern ciphers where more complex substitution and transposition ideas are used.

Week 2

Lecture 1

Part -1 Extended GCD Algorithm and Related Computations

Part 2 - Symmetric key Cryptography

Lecture 2

Properties of Numbers-II

Workshop 2: Workshops start from this week.

Quiz 2