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

© University of Melbourne, 2020
Udaya Parampalli

Symmetric key Cryptography

COMP90043

Lecture 2-Part II

© University of Melbourne, 2020
Udaya Parampalli

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 Symmetric key Encryption
- Attacks on Symmetric key Encryption

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

© University of Melbourne, 2020
Udaya Parampalli

1.1 Symmetric Cipher Models

COMP90043

Lecture 2-Part II

© University of Melbourne, 2020
Udaya Parampalli

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 assumption is that both sender and receiver should have access to the symmetric key used in the encryption.
- Widely used in practice.
- Examples: DES, AES etc.

© University of Melbourne, 2020
Udaya Parampalli

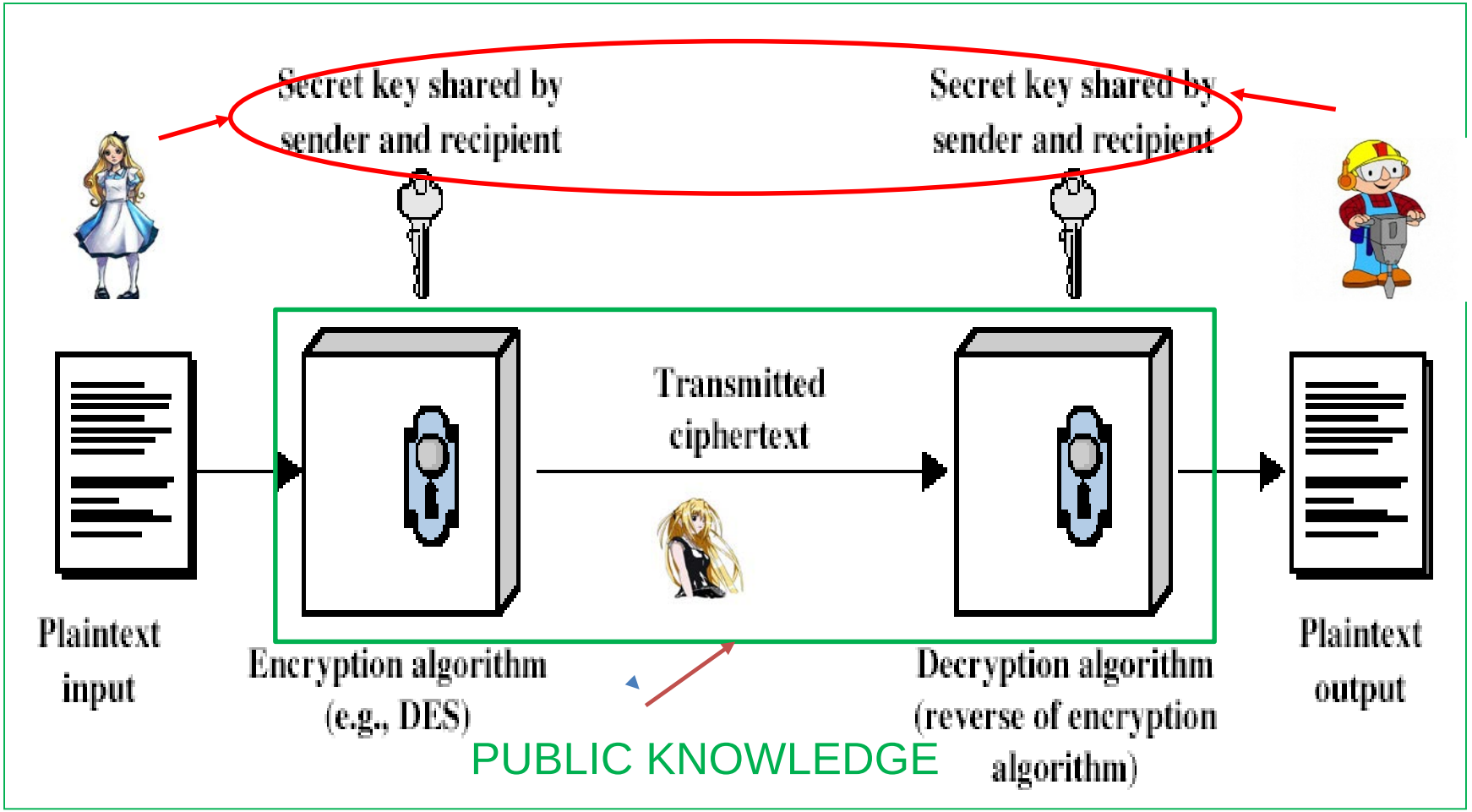
Terminology

- **Plaintext** - Source message
- **Ciphertext** - Encrypted message
- **Cipher** or Encryption Algorithm- Procedure for transforming plaintext to ciphertext
- **Key** – info or secret used in cipher known only to sender/receiver
- **Encipher (encrypt)** - Converting plaintext to ciphertext
- **Decipher (decrypt)** - Recovering plaintext from ciphertext
- **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

© University of Melbourne, 2020

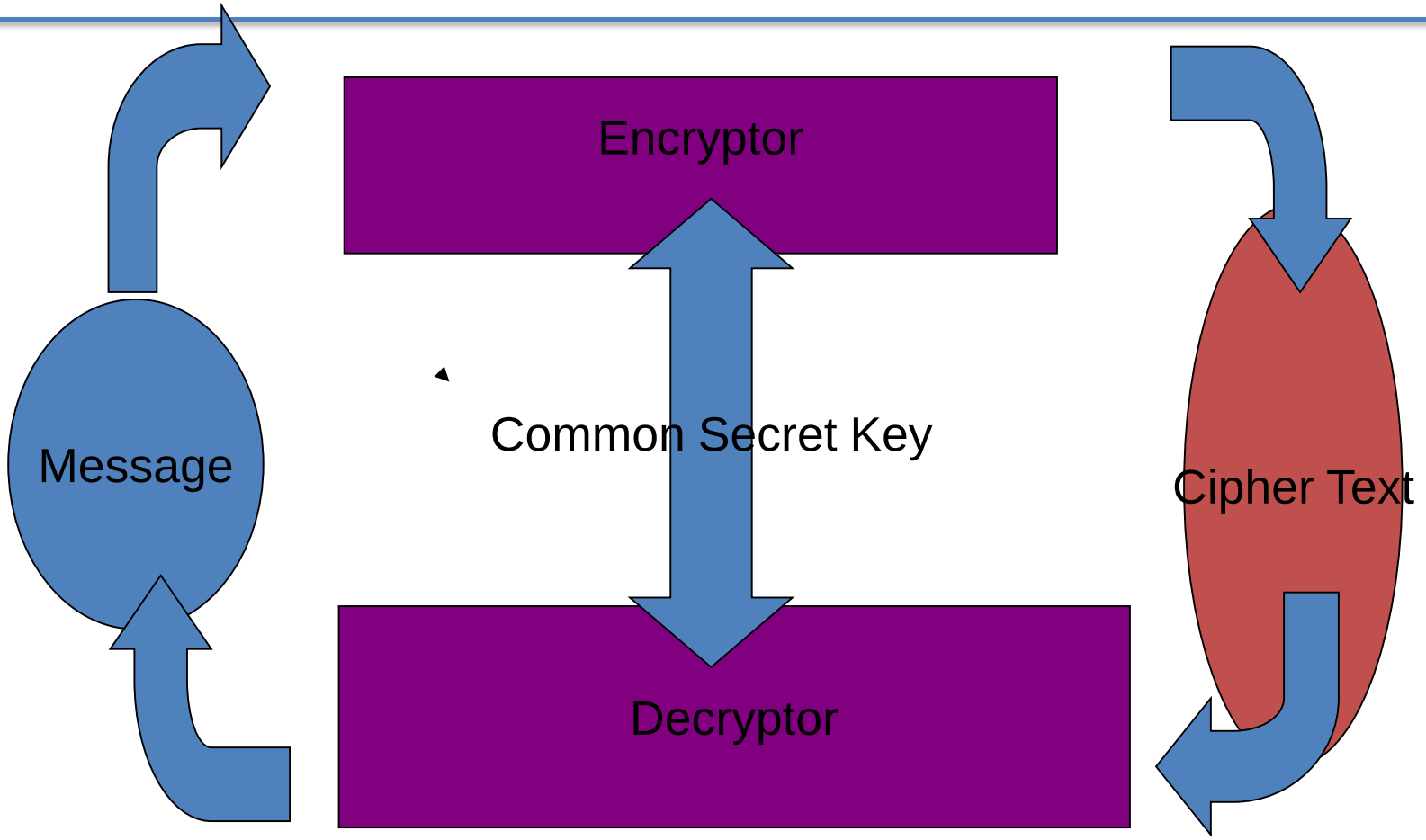
Model for Symmetric Key Cipher

Modified From:Stallings Figure 2.1:



© University of Melbourne, 2020
Udaya Parampalli

Logical View of Symmetric Key System



Block diagram of a Symmetric Key System: Logical view

© University of Melbourne, 2020
Udaya Parampalli

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 details are made public and security should be obtained by using only secrecy of key used in the encryption
- Stallings recommends two essential requirements:
  - 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.

© University of Melbourne, 2020
Udaya Parampalli

1.2 Security

COMP90043

Lecture 2-Part II

© University of Melbourne, 2020
Udaya Parampalli

Model of Symmetric Key Usage

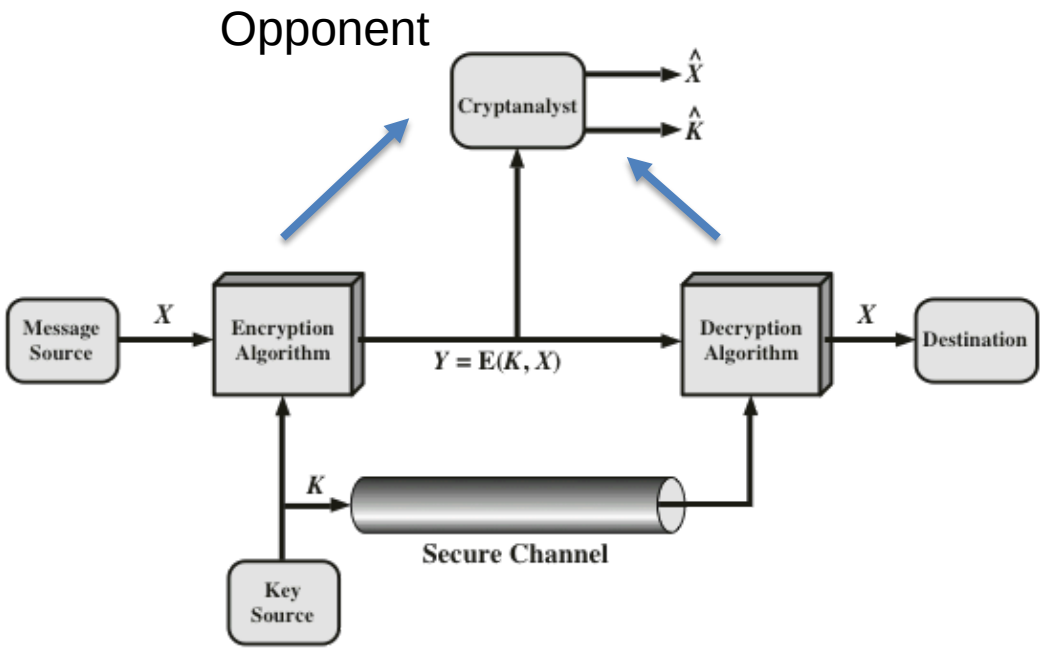


Figure 3.2 Model of Symmetric Cryptosystem

$Y = E(K, X)$

$X = D(K, Y)$

From Stallings Figure 3.2:

© University of Melbourne, 2020

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 Possible Keys used: Higher the key size better protection.
- Types of Plaintext/Cipher text processing
  - 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

© University of Melbourne, 2020
Udaya Parampalli

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 except the key involved.
- Keys should be large enough such that **Brute-force** 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:**

© University of Melbourne, 2020
Udaya Parampalli

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 that they desire. They can use centralized o distributed architecture.
- Two important definitions are interesting on which much 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.

© University of Melbourne, 2020
Udaya Parampalli

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 step for every ciphertext. Not a feasible approach.
- Next best thing you can hope is to brute-force on every possible keys.
- You realize immediately that the attack is directly proportional to the size of the key space.
- Of course you assume you have a method to recognize plaintext 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)

© University of Melbourne, 2020
Udaya Parampalli

1.3 Classical Ciphers

COMP90043

Lecture 2-Part II

© University of Melbourne, 2020
Udaya Parampalli

Classical Ciphers

- Why do we study?
- They are based on simple properties of plaintext alphabets and are known from antiquity.
- Help us to illustrate both encryption and cryptanalysis 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.

© University of Melbourne, 2020
Udaya Parampalli

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 NODE- DITNAP TANF
- 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

© University of Melbourne, 2020
Udaya Parampalli

Caesar Cipher

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

- For example, in English

- The alphabet order is:ABCDEFGHIJKLMNOPQRSTUVWXYZ

- 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`

© University of Melbourne, 2020
Udaya Parampalli

Caesar Cipher Mathematically

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

- p: = plaintext c:=ciphertext

- 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?

© University of Melbourne, 2020
Udaya Parampalli

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 belongs to Z_{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?

© University of Melbourne, 2020
Udaya Parampalli

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 permutation on the alphabet Z_{26} (plaintext letter maps to a different random ciphertext letter)
- Consider an example: key could be a permutation:
- **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
- **DKVQFIBJWPESCXHTMYAUOLRGZN**
- Exercise: Complete the Encryption of the following phrase:
- **Message: newcoronaviruscasescross**
- **Ciphertext: xf…..**
- **How many possible keys?**

© University of Melbourne, 2020
Udaya Parampalli

Transposition Ciphers

- A permutation of plaintext symbols are employed here as opposed to substitution.
- As a result letter are only rearraged for every d positions.
- Divide plain text as sequence of plaintext blocks of certain size say, d.
- Then apply a permutation to every d positions of the plaintext. The permutation is the key.

© University of Melbourne, 2020
Udaya Parampalli

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 message out as:

  m e m a t r h t g p r y

  e t e f e t e o a a t
- giving ciphertext

  MEMATRHTGPRYETEFETEOAAT

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

© University of Melbourne, 2020
Udaya Parampalli

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 columns according to some key before 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

© University of Melbourne, 2020
Udaya Parampalli

1.4 Cryptanalysis of Classical Ciphers

COMP90043

Lecture 2-Part II

© University of Melbourne, 2020
Udaya Parampalli

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 on the alphabets in the ciphertext from 1 to 25, when you recognize some meaningful plaintext stop,
- Can you break the ciphertext:
- GCUA VQ DTGCM
- I have provided some magma code on the lms try them.

© University of Melbourne, 2020
Udaya Parampalli

Affine Cipher

- How many different keys?
- What is the complexity of Brute-force search?
- See a Workshop question next week.

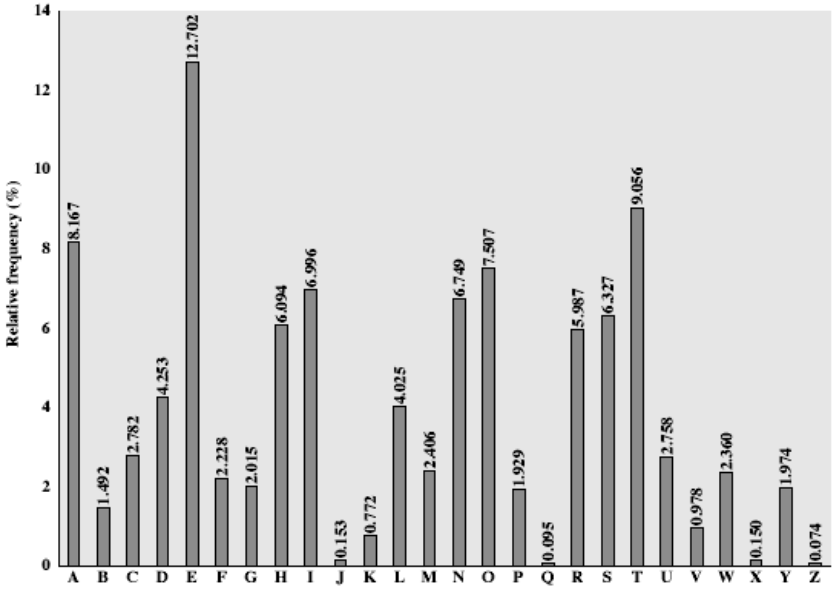
© University of Melbourne, 2020
Udaya Parampalli

General Monoalphabetic Cipher

- How many different keys?
- 26!
- Brute-force seems impossible. But do you think the 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.

© University of Melbourne, 2020
Udaya Parampalli

Language Frequencies



From Stallings Fig. 3.5

The original ideas were developed in 9th Century by Arabian mathematicians.

Refer to the textbook for more discussion

There are now automated methods on Internet

© University of Melbourne, 2020

1.5 Complex Ciphers

COMP90043

Lecture 2-Part II

© University of Melbourne, 2020
Udaya Parampalli

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 monoalphabetic cipher to use in a given time context.
- The textbook has some examples, please follow them.

© University of Melbourne, 2020
Udaya Parampalli

Vigenère Cipher

- This is a simple polyalphabetic substitution cipher.
- Here a set of Caesar ciphers is employed.
- ith plaintext symbol is handled by Caesar cipher with key: $k_{(i \bmod d)}$
- The idea is very simple, a key is a multiple letter word: $K = k_1\ k_2\ \ldots\ k_d$
- $P = p_1\ p_2 \cdots p_d\ p_{d+1}\ p_{d+2} \cdots p_{2d}\ldots$
- $C = c_1\ c_2\ \ldots\ c_d\ c_{d+1}\ c_{d+2}\ \ldots\ c_{2d}\ldots$
- 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.

© University of Melbourne, 2020
Udaya Parampalli

Example of Vigenère Cipher

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

© University of Melbourne, 2020
Udaya Parampalli

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 transposition ciphers in succession.
- These ideas are were used in German cipher during world war time-see section on Rotar Machines in the textbook.
- This is a link to modern ciphers where more complex substitution and transposition ideas are used.

© University of Melbourne, 2020
Udaya Parampalli

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

© University of Melbourne, 2020
Udaya Parampalli