COMMONWEALTH OF AUSTRALIA
Copyright Regulation 1969

Fundamental Concepts of Cryptography ISEC2000/5002

Lecture 1: Introduction to Information Security

Lecturer and tutor

- Lecturer/tutor Information
  - Dr. Wanquan Liu
  - Room: 314.329
  - Phone: x2746
  - Email: *w.liu@curtin.edu.au*
  - *Dr Qilin Li (Eric)*
  - *Email:li.qilin@student.curtin.edu.au*
  - *Serena*
  - *Email: Serena.earsman@hotmail.com*

Unit introduction

- With the overwhelming development of computer networks and web applications, information security becomes very important and is a popular research topic. Every year, the loss due to security threats in worldwide is worth billions/millions of dollars.

- Information security is introduced systematically to students in this unit. The formal unit was called Software security 303/300.

- Now cyber-security is a new degree in this department.

Objectives

- This Unit will teach you how cryptographic techniques have been developed and used in protecting information security. Topics will include:

  - Cryptographic technologies.
  - Related mathematical foundations.
  - Standards/protocols being developed/used in practice.
  - Computational Complexity.
  - Key exchange protocols.

Outcomes

- By the end of this unit, you are expected to be able to
  - understand the theory and technology of contemporary cryptography;
  - be aware of the main threats to information system security;
  - familiar with the fundamental international standard cryptographic algorithms and their performance;
  - cryptographic protocols for secure communications;
  - Limitations of some algorithms.

Method of instruction

- 2-hour lecture each week for 12 weeks.
- 12 weeks lecturing followed by a final exam.
- One hour practical in the lab every week from week 2 with tutor supervision.
- Attending lecture is not compulsory **but the lecturer can deny answering questions** which have been explained clearly in your missing lecture.
- Encourage group discussions and independently complete your own assessment.

Assessment

- Assignments – 50%.
  - Two assignments, each worth 25%.
- Finial exam - 50%.
- **How to pass**:
  - Minimum mark of 50% in the final exam.
  - Minimum mark of 50% in all assignments.
- Final Marks
  - Two assignments + final exam marks.

Plagiarism

- The department has a policy to punish students who copy other's work (assignment, finial exam, etc.). If two works are found to be **essentially** identical, then both of the students will receive a **0** mark or may be excluded from the department.

- You should know these rules quite well. If you are not sure of this policy, ask the department secretary or check the rules by yourself for details in the unit outline or university website.

Pre-requisites

- System programming (C/C++ or Java).
- General Computer Science knowledge.
- Strong mathematics background (or interest).
- Consistent hard work will be essential.

Text book and references

- **Text books**
  - W.Stallings, "*Cryptography and Network Security: Principles and Practice*", Prentice Hall, 2011. 6th edition.
- **Reference books**
  - [1] B. Schneier, "*Applied Cryptography*," Second Edition, John Wiley & Sons, 1995. It includes almost every thing.
  - [2]Wenbo Mao, "*Modern Cryptography, Theory and Practice*", Prentice Hall, 2004.
  - [3] C. P. Pfleeger, "*Security in Computing*" (2nd edition), Prentice Hall, 1997. A good reference book in general knowledge of computer, though not comprehensive.

Lecture 1: Introduction to Information Security

- What is information security ?
- Why information security ?
- Security goals and requirements.
- Security Attacks/threats.
- Cryptography.
- Types of cryptosystems over threats.

What is information security ?

- Roughly speaking, it is to protect **information** from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
- In fact it is mainly concerned with the confidentiality, integrity and availability of data. (Called **CIA** in many references).

Why information security ?

- Today is an information age.
- More and more computers/devices are connected to the network.
- Commerce is moving to the network, e.g. multimedia, electronic commerce (e-commerce).
- Security threats are more serious than ever before.
- ATM machines need security protection in one way or another.
- You can add more reasons……
- *Do we have personal information secure now?*

Why information security?

- Employment opportunities. (**You will get better pay if you know security better in IT. Believe or not ?**)
- People are more concerning the data security (e.g. medical record, credit card information, private communication)
  - their confidentiality/secrecy, so that they are not revealed to people who are not allowed to;
  - their integrity, so that they are not modified;
  - their availability, so that they can be retrieved for later use.

Why information security ?

- Threats to security
  - **Personnel reasons**, e.g. malicious employee; inappropriate management due to lack of knowledge; **vicious attackers and hackers**.
  - Physical reasons, e.g. unexpected fire; earthquake; mouse/mice bite wires.
  - Logical reasons, e.g. insecure operating system; no security mechanism applied in intra networks.

How to enforce information security?

- How to protect them
  - **access control**; security knowledge study; cryptographic techniques;
  - **physical security guard**; use reliable constructing material;
  - use secure operating system and appropriate security technology.

Security goals and requirements

For information, we require

- ***Confidentiality***: Requires that content of information is not revealed to some unauthorized parties.
- ***Integrity***: Requires that unauthorized modification (alternation, insertion, or deletion) is not permitted.
- ***Availability***: Requires that information is available to legitimated users.

Security goals and requirements

For users

- ***Authentication***: Requires that eligibility of users can be verified.
- ***Non-repudiation***: Requires that sender or receiver cannot deny the sending or receiving of a message.
- ***Access control***: Requires that authorization is required for a particular user to get access to a particular data in terms of reading, writing, or modifying.

Cryptography

- What is cryptography?

  It is the study of message secrecy, which includes the following components.
  - *Encryption/decryption* for information confidentiality/privacy.
  - *Message authentication*.
  - *Digital signatures*, for information authentication and non-repudiation.
  - *Authentication protocols*, to manipulate the use of digital signatures.

Cryptography in applications

- Secure management of keys.
- Distributed system security.
- Network security (LAN and Wide area network).
- Secure network protocols.
- Secure electronic commerce (e.g. e-bank, e-cash, smart card).

Cryptosystem classification

- **Symmetric *and* Asymmetric ciphers**
  - (secret key and public key ciphers).
  - (Conventional and public key ciphers).
- **Stream *and* Block ciphers**. (bit operation or block operation)

The concept of security

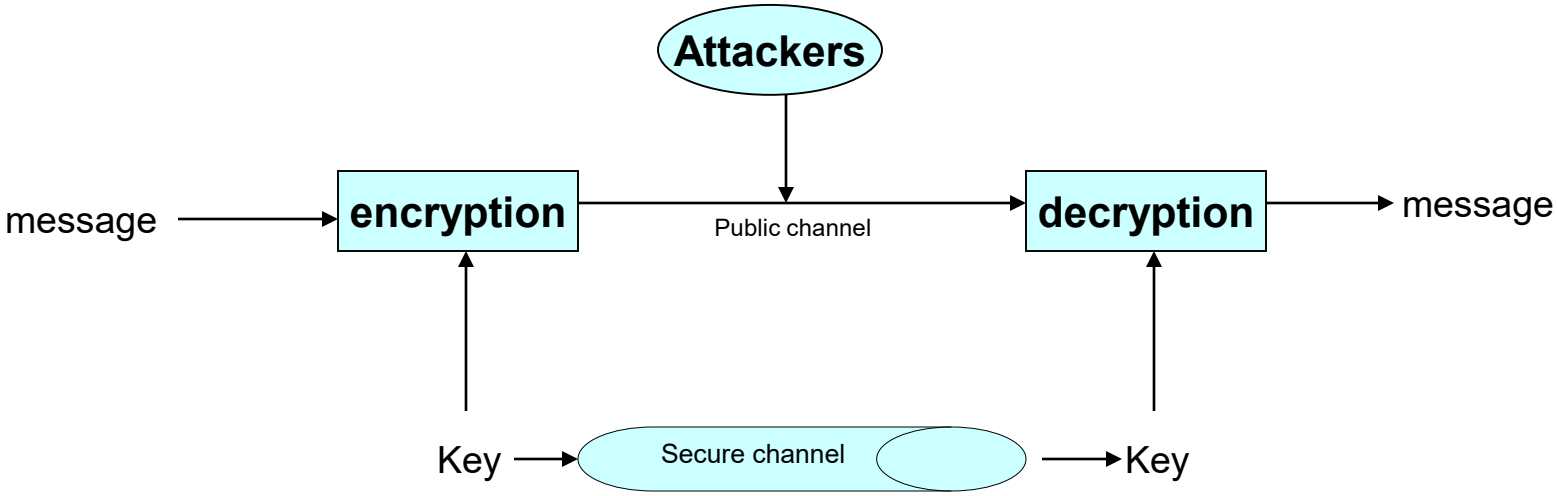
- Unconditional security and computational security.
  - Unconditional: security level is independent of the computational capacity of the attackers.
  - Computational: security is measured in terms of the amount of computing.
- Theoretical security and practical security.
  - Theoretical: security can be proved.
  - Practical: security is based on an assumption.

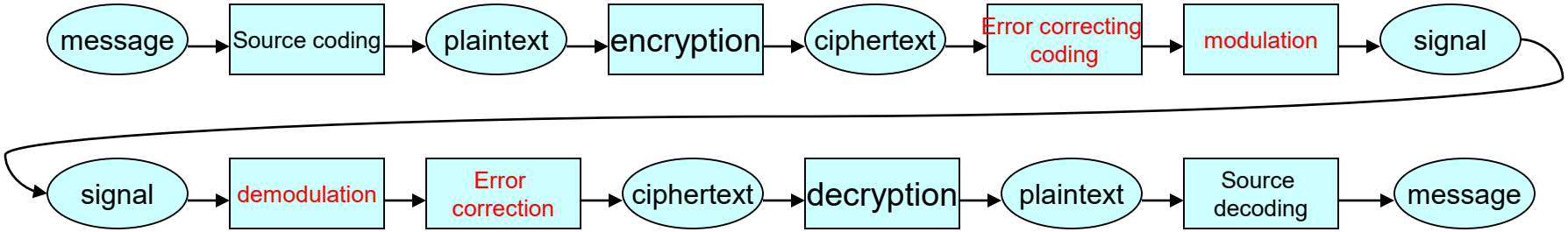
Conventional and public key cryptography

- Public key system for authentication.

  (Public key system is more popular today)
- Public key system is mainly used for session key distribution.
  - *Diffie-Hellman Key Exchange*
- Symmetric block cipher algorithm for secure data encryption.
  - DES or 3DES for data encryption.
  - Symmetric stream cipher algorithm for secure voice communication.

Conventional cryptosystem





Fundamental concepts

- **Plaintext *m***: normally a 0-1 string converted from a message. Sometimes called message.
- **Cipher-text *c***: output of plaintext after encryption.
- **Encryption** c=$E_k(m)$: an algorithm transforms plaintext into cipher-text.
- **Decryption** m=$D_k(c)$: the inverse of $E_k(m)$.
- **Key *k***: secret information used in encryption and decryption.

Fundamental concepts

- **Plaintext space (set)**: the set of all possible plaintext.
- **Cipher-text space (set)**: the set of all possible cipher-text.
- **Key space**: *the set of all possible keys*.
- **Key size**: *size of memory required to store the key.*

Security attacks/threats

- **Passive attacks**
  - release of message contents (cryptanalysis)
  - traffic analysis (a more undetectable attack)
- **Active attacks**
  - **Replay attack**: reuse of message which has been expired or becomes unauthorized.
  - **Masquerade attack**: One entity pretends to be a different entity.
  - **Modification**: Modifies the content of the message illegally.
  - **Denial of service**: System is made to deny services for reasonable requests.

Security attacks/threats

- ***When does an attack become a threat?***
  - For a passive attack: If the attacker gains benefits or
  - For an active attack: If it is undetected.

Shannon's theory

- Shannon's paper: Bell Lab. Journal, 1949. (Foundation paper in Information Theory and Telecommunication)
- Only one-time-pad is theoretically secure (we talk about it later in detail).
  - Any key if used for more than once would leak information.
  - key should be generated at *random.*

Shannon's theory

Security concept/criteria

- **Diffusion**: message should be arranged in a totally random way after encryption;
- **Confusion**: message and key should be mixed completely.

Simple encryption algorithms/ Ancient cipher techniques

- Mono-alphabetic ciphers
  - Caesar cipher
  - Affine cipher
  - Permutation cipher
- Poly-alphabetic ciphers
  - Vignenère cipher
  - Other ciphers, many more

Ancient Ciphers: Letter-to-Number Mapping (simple source coding)

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Operation: modulo 26 based.

Mono-alphabetic ciphers

- **Caesar cipher**
  - Alphabets a - z corresponds to numbers 0 - 25. Key is a number between 0 and 25.
  - Encryption: $c = (m + k) \bmod 26$.
  - Decryption: $m = (c - k) \bmod 26$, or

    $m = (c + (26- k)) \bmod 26$.

    where *m mod p* = the **residue** after *m* is divided by *p*.

Caesar cipher

Example: With k=3, and

- Plaintext: abcdefghijklmnopqrstuvwxyz

The the cipher-text will be

- Cipher-text: DEFGHIJKLMNOPQRSTUVWXYZABC

Number of keys: 26.

E.g. k=3, “security” --> “vhfxulwb”.

Security: Not even secure to hand calculations.

Think about if c-k is negative,

how to compute (c-k)mod 26?

Mon-alphabetic ciphers

- **Affine cipher**
  - Alphabets a - z corresponds to numbers 0 - 25.
  - Key: two numbers 0 <=a, b <= 25, where a is co-prime to 26. (we will talk about coprime in detail later)
  - Encryption: $c = f(m) = (a\ m + b) \bmod 26$.
  - Decryption: $m = f^{-1}(c) = a^{-1}\ (c - b) \bmod 26$.
  - **What is a^{-1} here**?

Mon-alphabetic cipher: Affine Cipher

- Note: a^{-1} is also an integer between [1, 25] satisfying $aa^{-1} \bmod 26=1$.

a	1	3	5	7	11	17	25
a^{-1}	1	9	21	15	19	23	25

- Number of keys: 26 × 12 = 312.
- [Question] Do you know when ***a*** does have an inverse modulo 26?

Mon-alphabetic cipher: Permutation cipher [see textbook for detail]

- A permutation of a finite set of elements **S is an ordered sequence of all the elements of S, with each element appearing exactly once.**
- It is a generalization of Caesar cipher.
  - In Caesar cipher, replace the *Cipher* line by an arbitrary permutation of the 26 alphabets.
- Number of keys: 26! = 403291461126605635584000000
- Key size: $\log_2 26! = 90$ bits.

Mon-alphabetic cipher: Hill Cipher (a block cipher)

- Key K: an m × m nonsingular matrix with respect to modulo 26.
- Plaintext and cipher-text are all blocks of m alphabetics.
- Encryption: $C = KP$.
- Decryption: $P = K^{-1}C$.

Hill cipher: an example

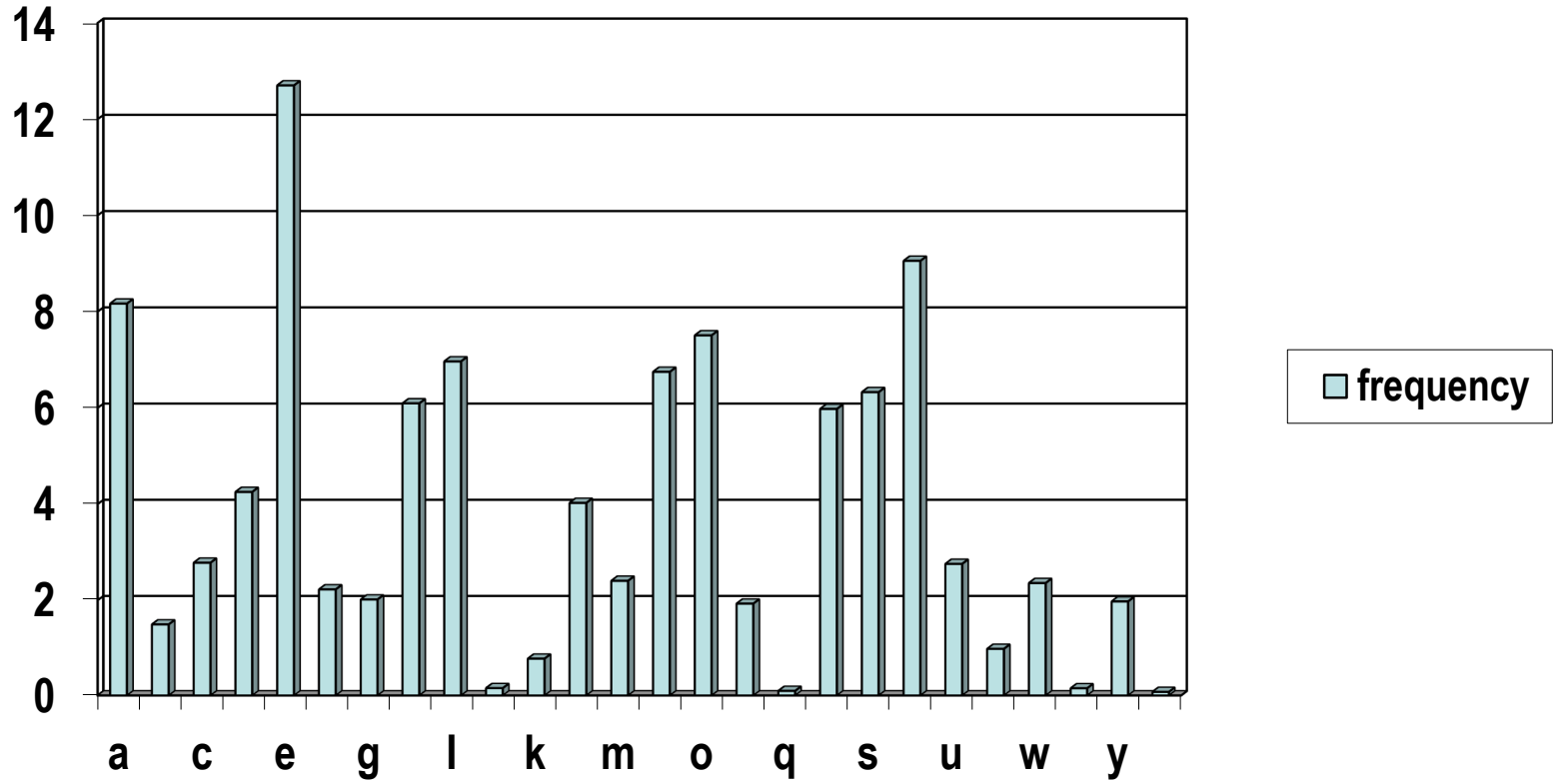
- $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ $K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$
- M="and" = $(0\ 13\ 3)^T$; X^T means the vector is a column one.
- $C=KM = (2\ 11\ 5)^T$ = "clf".

- Check: $M == K^{-1}C = (0\ 13\ 3)^T$?

Mon-alphabetic Cipher: Properties

- **Vulnerable to statistical analysis**.
  - Because different alphabets appear in a text at different frequency, it is possible that one can guess which letter is encrypted from a particular letter. For example, the letter with the highest frequency is likely the cipher-text of letter *e*. (see [2] for detail)

Relative frequency of Letters in English text



Example: Design of Cryptosystem

- **Message *m***: is divided as a sequence of characters.
  - *m* = *"information*" = (*i n f o r m a t i o n*).
- **Key *k*=*"key"*** (seed): is repeated to at least the same length as *m*.
- **Key *K* (used):** is the segment of repeated *k* with the same length of *m. K="keykeykeyke".*

Example

- **Conversion:**

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- **Encryption** ($c = m + k$):
  - Convert characters into integers less than 26: then
  - m' = 8 13 5 14 17 12 0 19 8 14 13
  - K'= 10 4 24 10 4 24 10 4 24 10 4

Example

- **Encryption**
  - **Cipher text *c′*,** the addition of *m′* and *k′* per-character modulo 26. *c′* = 18 17 3 24 21 10 10 23 6 24 17.
  - **Cipher text *c***: convert *c′* into characters, then *c* = *“srdyvkkxgyr"*.
- **Decryption** (*m* = *c* - *k*):
  - *c* --> *c′: c′* = 18 17 3 24 21 10 10 23 6 24 17.
  - *m’* is the modulo 26 subtraction of *c′* and *K*.
  - *m′* = 8 13 5 14 17 12 0 19 8 14 13.
  - *m* is converted fro*m m′: m = “information".*

Conclusions

- Encryption is the inverse of decryption.
- The way in converting letters into numbers are not essential (this is called source coding, refer to signal processing).

Summary

- Information security.
- Basic requirements for information security.
- Shannon information theory.
- Simple encryption techniques.
- Encryption algorithm design and key size computation/estimation.