MH4311 Cryptography

Lecture 1 Introduction

Wu Hongjun

Lecture Outline

- **Cryptography**
- **Applications of cryptography**
- **Course information**

Cryptography

http://en.wikipedia.org/wiki/Cryptography

- Greek: krypto = secret; graph = writing
- Cryptography
  - Confidentiality
    - Protect the secrecy of message: encryption/decryption
  - Integrity
    - Detect the unauthorized modification of data
  - Authentication
    - Message authentication
      - To check whether a message does come from the sender
    - Identification
- Cryptanalysis
  - Analyze the security of ciphers

Cryptography

- **Cryptography development**
  - **Closely related to computing devices (cipher should be computed easily)**
    - **Paper & pencil**
      - **simple and normally weak ciphers**
    - **Electromechanical computing device**
      - **rotor machines from 1920s to 1960s**
    - **Electronic computing device**
      - **Modern ciphers: DES, AES, RSA …**

Cryptography

- **Cryptography development (cont.)**
  - **Closely related to communication techniques**
    - **Radio telegraph (wireless communication)**
      - **Message interception is easy => strong ciphers needed**
    - **Computer network**
      - **How can two computers communicate secretly, if the two computers do not share any secret key before the communication starts ?**
        - » **public key cryptography in the 1970s (revolution!)**

Applications: Military, Intelligence

- **Caesar cipher (Rome Republic)**
- **Enigma (Germany, WWII)**
  - **Broken by the Allies**
    - **Alan Turing**
    - **this "news" was disclosed in the 1970s**
- **KW-26 (NATO, 1960s to 1980s)**

How NSA and GCHQ spied on the Cold War world

By Gordon Corera
Security correspondent, BBC News

28 July 2015 | UK

American and British intelligence used a secret relationship with the founder of a Swiss encryption company to help them spy during the Cold War, newly released documents analysed by the BBC reveal.

Applications – Financial Services

- **Interbank transactions**
  - **Everyday, millions of messages are securely exchanged by over 8,300 financial institutions (SWIFT system)**
- **Internet banking**
  - **Encrypt data transmitted between client and bank**
  - **Detect the modification of data during transmission**
  - **User authentication: password (+ one-time password)**

Applications – Financial Services

- **ATM**
  - **Encrypt the password being transmitted between ATM machine and bank**
  - **Before 2014, there is no cryptography in the Singapore ATM cards**
    - **easy to forge a ATM card by reading the information stored in the magnetic stripe**
  - **Now there is secret key and strong cipher in the Singapore ATM cards**
    - **much safer to use ATM**

Applications – Daily Life

- **Contactless Payment**

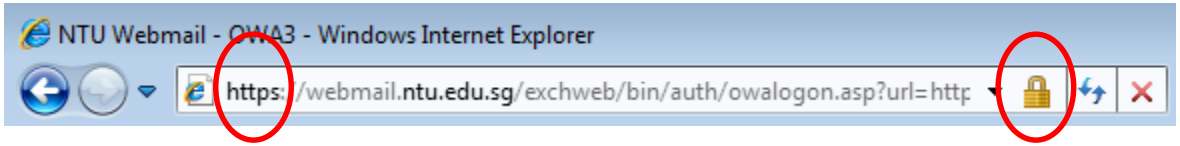
- **Access badge**

- **Mobile phone, wireless network**

Applications – Daily Life

- **Electronic (biometric) passport**

- **Email**



- **Security token for authentication**

Cryptography Flaws

- **Insecure ciphers**
  - **Examples: ciphers in MIFARE (British "Ezlink"), satellite phone, GSM mobile phone, 40-bit key ciphers in all the USA exported products during 1990s, and ciphers with backdoors**
- **Insecure key management**
  - **Key management is a major issue in cryptography applications**
- **Insecure implementation**

Recent Cryptography News

- **RSA security token insecure (key management flaw)**

Tuesday, June 7, 2011 As of 12:00 AM

THE WALL STREET JOURNAL. | TECHNOLOGY

Security 'Tokens' Take Hit

RSA Offers to Replace Its SecurIDs or Provide Monitoring for Nearly All Customers

Article | Video | Stock Quotes | Comments (53)

Email | Print | Save This | Like 760 | + More | Text

By SIOBHAN GORMAN And SHARA TIBKEN

RSA Security is offering to provide security monitoring or replace its well-known SecurID tokens—devices used by millions of corporate workers to securely log on to their computers—"for virtually every customer we have," the company's Chairman Art Coviello said in an interview.

In a letter to customers Monday, the EMC Corp. unit openly acknowledged for the first time that intruders had breached its security systems at defense contractor Lockheed Martin Corp. using data stolen from RSA.

SecurID tokens have become a fixture of office life at thousands of corporations, used when

Recent Cryptography News

- **Key generation flaw in Android**
  - **Android is the most popular operating system in smart phones and tablets (roughly 80% market share)**
  - **It was found in 2013 that the secret keys generated in many Android systems can be guessed easily**
    - **It means that the secure communication (email, e-commerce, e-government service …) of the Android devices is insecure**

Recent Cryptography News

- **Heartbleed security bug in OpenSSL**
  - **OpenSSL is a cryptography library.**
  - **OpenSSL is widely used in the implementation of internet secure communication system**
  - **It was found in 2014 that a security bug (software flaw) in OpenSSL allows hackers to retrieve secret information from computers' memory**
    - **Around half a million servers get affected**
  - **Ciphers are strong, but the implementation of the cryptography library is insecure**

Recent Cryptography News

- NSA (National Security Agency, USA) works on information collection, decryption, and analysis
- Edward Snowden and NSA (USA)
  - Snowden is a former NSA contractor who released many secret NSA documents
  - It was revealed that NSA runs numerous global surveillance programs (intercepting email, phone calls …)
  - It was also revealed that NSA deliberately introduces security flaws into the popular software/hardware.
  - NSA is in trouble to explain why a weak NSA cipher becomes a cryptography standard …

http://www.itpro.co.uk/security/23870/ex-nsa-director-support-for-insecure-cryptography-tool-regrettable

http://www.itnews.com.au/News/405833,nist-formally-chops-nsa-tainted-random-number-generator.aspx

Recent Cryptography News

- Tor is a cryptographic software/network that allows a user to browse the internet anonymously
- The dark net in the TOR network is widely used by criminals to sell drugs, illegal documents …

Recent Cryptography News

- **Bitcoin**
  - **A type of cryptocurrency**
    - **Its price is based on speculation**
  - **Decentralized, issued without a central bank**
    - **Issued gradually by computing crypto algorithm**
  - **Bitcoin is widely used for illegal transactions**
- **Bitcoin is somehow 'notorious', but the technology blockchain in Bitcoin is useful to the financial sector**
  - **Example: Singapore government is considering to use block chain to speed up the interbank transactions in Singapore**

Significance and limitation of cryptography

- **Significance**
  - **Cryptography is the foundation of information security**
    - **Weak ciphers => weak information system**
- **Limitation**
  - **Using strong ciphers does not guarantee the security of an information system**
  - **An example: Ciphers used in the interbank messaging system are strong, but hackers stole millions dollars from banks in 2015/2016 (US$81million from Bangladesh central bank, US$10 million from a Ukraine bank, … , 12 banks get affected)**

Course Information

Course information

- **Instructor**

  Wu Hongjun

  Email: wuhj@ntu.edu.sg

  Office: SPMS-MAS-05-47

- **Lecture**

  Monday 15:30--17:30 SPMS-LT4

  Friday 09:30--10:30 SPMS-LT4

- **Tutorial**

  Friday 10:30--11:30 SPMS-LT4

- **Consultation**

  Friday 11:30--12:30 (MAS-05-47)

Course information

- **Grading**
  - **Two graded assignments: 10 marks**
    (each assignment is 5 marks)
  - **Midterm exam: 30 marks**
  - **Final exam: 60 marks**

Midterm and Final exams are restricted open book exam: you can bring one double-sided A4 paper to the exam (write or print anything on the paper)

Course information

- **Textbook: CTP**
  - **Cryptography Theory and Practice, Third Edition**
  - **Doug Stinson**
- **Reference book: HAC**
  - **Handbook of Applied Cryptography, First Edition**
  - **A. J. Menezes, P. C. van Oorschot, S. A. Vanstone**
  - **Free online version at:**

    http://www.cacr.math.uwaterloo.ca/hac/

Course information

- Syllabus
  - Classical ciphers
  - Symmetric key encryption
  - Hash function and Message Authentication Code
  - Public key encryption
  - Digital signature
  - Key establishment and management
  - Introduction to other cryptographic topics

first half

second half