# MAS 433: Cryptography

Lecture 1

## Introduction

Wu Hongjun

# Lecture Outline

- Course information
- Cryptography
- Applications

# Course information

- Instructor
  - Wu Hongjun (wuhj@ntu.edu.sg)
- Lecture (SPMS-TR3)
  - Wednesday 8:30AM--10:30AM
  - Friday 10:30AM--11:30AM
- Tutorial (SPMS-TR3)
  - Friday 11:30AM--12:30PM
- Consultation (SPMS-MAS-05-47)
  - Wednesday 4:30PM -- 5:30PM
  - Friday 4:30PM -- 5:30PM

# Course information

- Grading
  - Assignments (two assignments)
    - 10 marks
  - Tutorials
    - 10 marks
    - submission of tutorial solution is compulsory
      - For each tutorial, about 5 submissions will be chosen (randomly) and marked.
  - Attendance
    - 10 marks
      - If a student does not attend class for *n* times,
        - » If $n \leq 3$, the student gets 10 marks for attendance
        - » If $n > 3$, the student gets 10-5×(n-3) marks for attendance
          - Example: n = 8, then -15 marks for attendance
  - Final exam (closed book)
    - 70 marks

# 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

first half

  - – Public key encryption
  - – Digital signature
  - – Key establishment and management
  - – Introduction to other cryptographic topics

second half

# 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

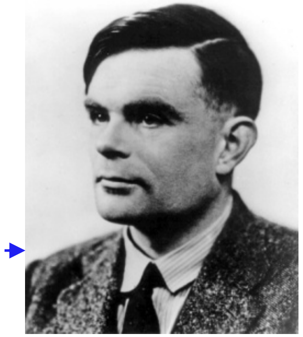
- Cryptography history
  - Closely related to computing devices (cryptography should be computed easily)
    - Paper & pencil
      - simple and normally weak ciphers
    - Electromechanical computing device
      - rotor machines from 1920s to 1960s
    - Electronic computer
      - Modern ciphers: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

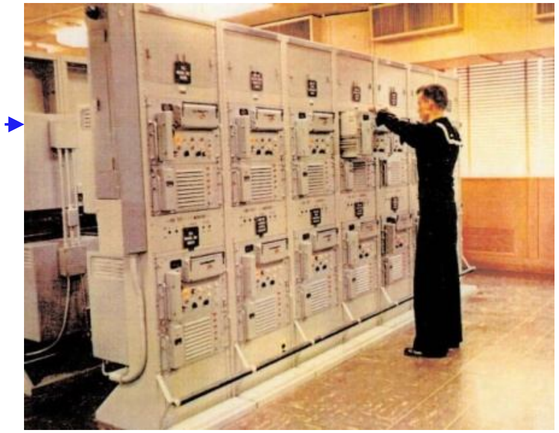
# Cryptography

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

# Applications – Military

- Caesar cipher (Rome Empire)
- Enigma (Germany, WWII)
  - Broken by the Allies
    - Alan Turing
- KW-26 (NATO, 1960s to 1980s)





# Applications – Financial Services

- Interbank transactions
  - Everyday, millions of messages are securely exchanged by over 8,300 financial institutions
- ATM
- Internet banking

# Applications – Daily Life

- Transportation card

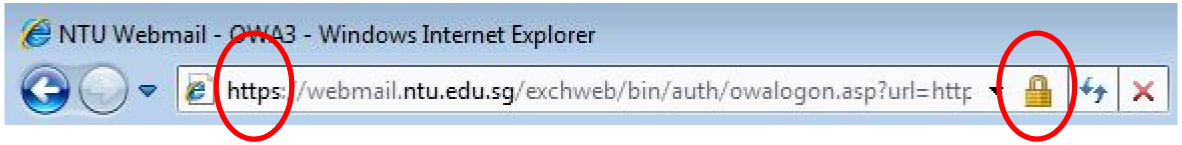
- Access badge

- Mobile phone, wireless internet

# Applications – Daily Life

- Electronic (biometric) passport

- Email



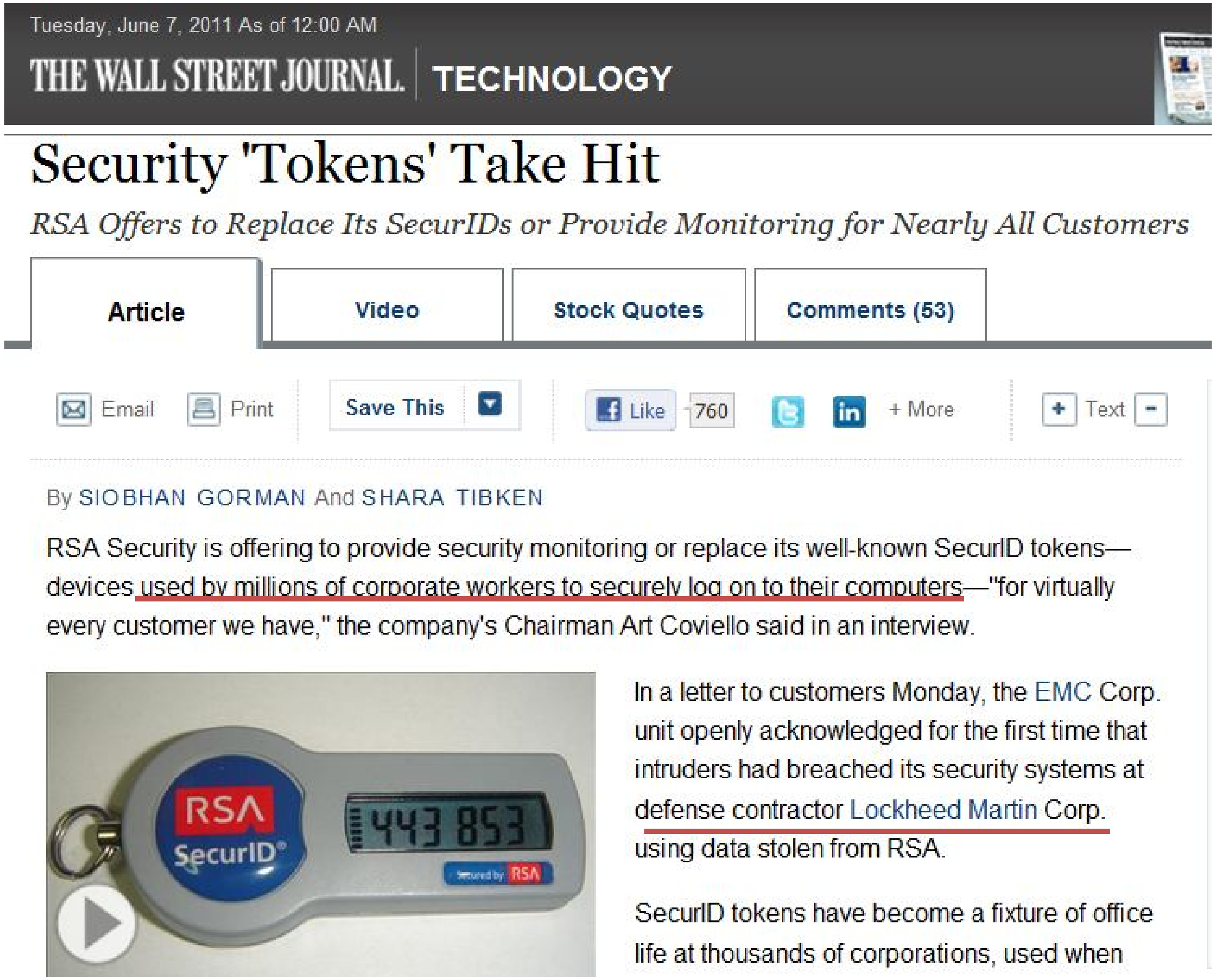
NTU Webmail - OWA3 - Windows Internet Explorer

https://webmail.ntu.edu.sg/exchweb/bin/auth/owalogon.asp?url=http

- Security token for authentication

The latest serious security flaw: RSA security token

(cryptography algorithm is not broken, but key management flaw: database for storing the keys get hacked)



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*

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

# Top 25 software security flaws (Year 2011)

http://cwe.mitre.org/top25/index.html

The following programming errors are related to cryptography:

5. Missing Authentication for Critical Function
7. Use of hard-coded credentials
8. Missing Encryption of Sensitive Data
14. Download of code without integrity check
19. Use of a broken or risky cryptographic algorithm
21. Improper restriction of excessive authentication attempts
25. Use of a one-way hash without a salt

# Significance and limitation of Cryptography

- Significance (necessary)
  - Cryptography is the foundation of information security
    - Weak ciphers => weak information system
- Limitation (but not sufficient)
  - Using strong ciphers does not guarantee that an information system is strong