

MAS 433: Cryptography

Lecture 1

Introduction

Wu Hongjun

Contents

- Course information
- Cryptography
- Applications

Course information

- Instructor
 - Wu Hongjun (wuhj@ntu.edu.sg)
 - Office hours:
 - Wednesday 2:00PM -- 3:30PM
 - Friday 2:00PM -- 3:30PM

Course information

- Grading
 - Assignments
 - 10% (two assignments, each 5%)
 - Midterm exam (closed book)
 - 20%
 - Final exam (closed book)
 - 70%

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

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 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

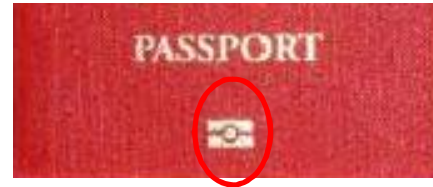


- Mobile phone, wireless internet

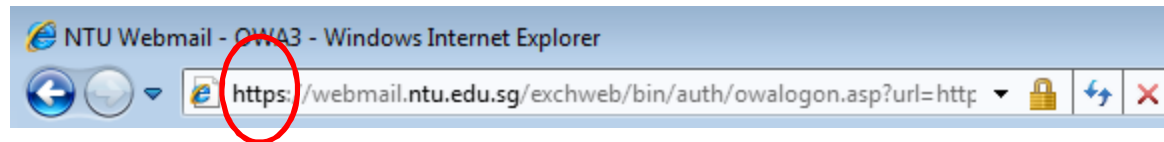


Applications – Daily Life

- Electronic (biometric) passport



- Email



- Security token for authentication

