CO7099 Cryptography and Internet Security

Credits: *15* **Convenor:** *Dr. S. Fung and Dr. R. Dimitrova* **Semester:** *2nd*

Prerequisites: *none*

Lectures: *30 hours*
Surgeries: *10 hours*
Laboratories: *10 hours*
Independent Study: *62.5 hours*

Assessment: *Coursework: 40% + Three hour exam in May/June: 60%*

Subject Knowledge

Aims This course will equip students with the knowledge required to build cryptographically secure applications in Java, and the knowledge of common security problems and solutions in Internet applications.

Learning Outcomes Students will be able to: describe the working principles of modern public-key cryptosystems; write cryptographically secure network applications using Java's cryptographic libraries; and describe the basic security principles of some internet applications relying on cryptographic mechanisms.

Methods Class sessions together with lecture slides, recommended textbook, worksheets, printed solutions, and some additional hand-outs and web support.

Assessment Marked coursework, traditional written examination.

Skills

Aims To teach students how to methodically solve problems given the techniques available to them.

Learning Outcomes Students will be able to: breakdown a problem to identify essential elements; apply prior knowledge of subject to analyze problems; design a plan to solve a problem; implement a planned solution and evaluate the implementation.

Methods Class sessions together with worksheets.

Assessment Marked coursework, traditional written examination.

Explanation of Prerequisites

A significant aspect of the module will be the reinforcement of material delivered in lectures with practicals involving students implementing cryptographically secure network applications in Java. Hence a basic knowledge of Java will be essential. A basic knowledge in networks, client-server architecture and Java socket programming, will be very useful. A basic grounding in discrete mathematics will be helpful during the lectures on cryptography.

Module Description

The use of computers and computer networks, in particular the Internet, is becoming an integral part of our lives in different application areas, such as e-banking and e-commerce. This has given us numerous advantages and convenience. However, at the same time, the security of computer systems becomes a critical issue. How can computer systems defend themselves against network attacks? How can we ensure that our data have not been tampered with, or disclosed without our consent? How can we be sure of the identity of the party whom we are communicating with? These are some of the security issues that must be addressed properly. This module will provide students with knowledge of the security issues in computer systems.

A fundamental part of security systems is cryptography, the science of secret writing. There have been rapid advances in cryptography in the past few decades, and cryptography has become an integral part of many commercial computer applications. The module will explain the principles of modern public key cryptography, a cornerstone of many security-enabled network applications in current use. A number of cryptographic primitives, including message digests, digital signatures and certificates, will be discussed. The module will go through all details of how to write secure network applications using these cryptographic primitives.

The course presents the security model of Java introducing elements of its access control model (e.g., Security manager and policies). Also, a few notation and techniques for the analysis of cryptographic protocols commonly adopted in distributed applications are introduced. Such techniques are used to argue about security aspects of some amongst the most popular applications of cryptographic protocols (e.g., Pretty Good Privacy and digital signatures).

Syllabus Cryptography: Security issues and concerns. Key management including generation, translation and agreement protocols (Diffie-Hellman). Principles of classical symmetric ciphers. Modern symmetric and asymmetric ciphers including DES, RSA. Block cipher concepts e.g. chaining and padding. Authentication and integrity with message digests, MAC's, signatures, and certificates. Simple cryptographic protocols, e.g. bit commitment. Java Support: Java Cryptography Architecture (JCA), Java Cryptography Extension (JCE).

Internet Security: Applications of cryptographic techniques in distributed applications. Access control in Java. Enforcement of security properties through cryptography. Pretty Good Privacy (PGP). Digital Signatures. Digital certificates. Kerberos. Secure Electronic Transaction (SET).

Reading List

[B] W. Stallings, *Cryptography and Network Security; ISBN: 0133354695,* Prentice Hall. 2013.

[B] J. Knudsen, *Java Cryptography; ISBN: 1565924029,* O'Reilly. 1998.

[B] S. Oaks, *Java Security; ISBN: 0596001576,* O'Reilly. 2001.

[B] B. Schneier, *Applied Cryptography; ISBN: 0471128457,* John Wiley and Sons. 1996.

[B] S. Garfinkel, *PGP: Pretty Good Privacy; ISBN: 1565920988,* O'Reilly. 1994.

[B] S. Garfinkel with G. Spafford, *Web Security, Privacy & Commerce; ISBN: 0596000456,* O'Reilly. 2001.

Resources Course notes, web page, study guide, worksheets, handouts, past examination papers.

Module Evaluation Course questionnaires, course review.