APT 3090: CRYPTOGRAPHY AND NETWORK SECURITY

Prerequisite APT 2050: Computer Network and Telecommunication

3 Credit Units

Rationale

The ability to protect the confidentiality of information, to prevent unauthorized access to data or services and to prevent the unauthorized modification of data is fundamental elements of security. Similarly, the ability to know who you are talking to and where something has come from, and to be able to bind parties to previous commitments or actions, is essential for trust. In the electronic world, these services typically rely on the use of cryptographic techniques. However, it is imperative that these techniques are used in the correct fashion if they are to satisfy their objectives. In particular, it is crucial that cryptographic keys are managed in an appropriate way.

Course Description

The course introduces the core techniques of cryptography around which security and trust can be constructed, and highlights the implications of using such techniques. It also looks at the entire key management lifecycle, and examines the differing requirements and methodologies for managing cryptographic keys of different types. The course ends by looking at how these techniques are applied in various applications and standards, from VPNs to secure email. The applications and techniques described are accompanied by a description of their strengths and limitations and the necessary supporting infrastructure.

Learning outcomes

Upon successful completion of this course, the students should be able to:

1. Appreciate the different services provided by the various cryptographic techniques, and understand their differences and how they are constructed
2. Describe the implications of using such techniques
3. Appreciate the different key management requirements and methodologies
4. Demonstrate how these techniques are applied in various applications and standards, from VPNs to secure email

Course Content

The cryptographic services: Symmetric key ciphers, from historical examples through to modern ciphers, and including: Asymmetric key techniques, including: Identification techniques Cryptographic key management: the life-cycle of cryptographic keys from generation through to destruction, and including digital certificates and Certification Authorities Cryptographic applications.

Teaching and learning Methodologies

Lectures, Presentations by members of the class, Case discussions, Tutorials, Assignments, Continuous assessment tests, Practical, Library, appropriate software, manual/notes,

Instructional Materials/Equipment

Course text, Handouts, White board, Presentation slides, Journals

Methods of evaluation

Class assignments, take-home assignments, tests, small projects to demonstrate use of software tools

Laboratory Work	20%
Project	20%
Assignments	10%
Mid-semester	20%
Final semester exams	30%
Total	**100%**

Main Textbooks-journals:

Computer security and Cryptography by Konheim, A.G 2007

Computer Security by Gollmann, D. 2nd Edition 2006

Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell 2007

Image Pattern Recognition: Synthesis and Analysis in Biometrics S. Yanushkevich, M. Gavrilova, P. Wang and S. Srihari (Eds), World Scientific Publishers, 2007

Handbook of Face Recognition Editors: Stan Z. Li and Anil K. Jain Springer, New York, 2005

Handbook of Multibiometrics (International Series on Biometrics) Arun A. Ross, Karthik Nandakumar, and Anil K. Jain, Hardcover - May, 2006