MScIT43 – Security and Cryptography

Instructor: Ziad Sakr (Dr)
Class Schedule: Monday and Wednesday, 5:00 - 6:30
Location:
E-mail: ziad.sakr@utt.edu.tt
Course URL: www.u.tt/ict

Course Objective

Understanding the goals, issues, technologies, algorithms, protocols, systems, and design criteria used in cryptography and data security. Developing basic system analysis and solution synthesis skills.

Assessment

- **Midterm Exam: 30%**
- **Project**
  - **Oral Presentation: 10%**
  - **Project Report: 20%**
- **Final Exam: 40%**

Compulsory Textbook:

- William Stallings, Cryptography and Network Security: Principles and Practice, Fourth Edition, Prentice Hall, 2006.

Reference Textbooks:

- Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons, 1996.
- Douglas R. Stinson, Cryptography: Theory and Practice, Second Edition, Chapman & Hall/CRC, 2002.

Topics

System Security: security policies, security goals, security mechanisms, security principles, physical security, hackers, risk management.

Introduction to Cryptography: classical cryptography, one-time pad (OTP).

Computational Cryptography: symmetric encryption, block ciphers, Feistel ciphers, DES, attacks on DES, 2-DES, 3-DES, IDEA, AES, encryption of long texts, stream ciphers, linear feedback shift registers.

Authentication Functions: by symmetric encryption, by asymmetric encryption, by hash functions, one-time-signatures.
Hash Functions: uses of hash functions, design of hash functions, birthday paradox, birthday attack, MD5, SHA-1, HMAC.

Public-Key Cryptography: basics number theory, Diffie-Hellman Key-Exchange protocol, DSS signatures, RSA algorithm.

Authentication: passwords and pass phrases, cryptographic authentication, authentication protocols, challenge response protocols, mutual authentication, authentication attacks.

Symmetric Key-Exchange Protocols: Key-Distribution Centers (KDC), Kerberos.

Asymmetric Key-Distribution: public-key certificates, certificate authorities, X.509 certificates, public key cryptographic standards, public-key infrastructure (PKI).

Network Layer Security: Internet Protocol Security (IPSec), Internet Key Exchange (IKE).

Transport Layer Security: SSL and TLS. Application Layer Security: Pretty Good Privacy (PGP), Email security, Web security, Electronic commerce.