INFORMATION AND COMMUNICATION SECURITY: ENCRYPTION & INFORMATION HIDING

by

Jonathan Blackledge

Distinguished Professor
Centre for Advanced Studies
Warsaw University of Technology

http://jmblackledge.web.officelive.com

A five day short course (4 hours per day)
Monday, 10th October – Friday, 14th October, 2011
10:00am - 12:00am & 2:00 - 4:00pm

ABOUT THE COURSE

This course has been designed for delegates who require an introduction to modern techniques of information and communication security with applications to areas such as computer network security, wireless communications, e-banking and cloud computing. Delegates should have a reasonable grasp of basic mathematics and some experience of computer programming but no prior knowledge of Cryptology is required. The course begins with a brief introduction to signals and systems and gives a short history of cryptography looking at the principal developments of the subject over the past fifty years and instructing delegates on the primary algorithms, standards and products that form the basis of modern secure communications technology. The course then explores current and future developments in Cryptology including methods of information hiding and *Steganography* for application in areas such as e-document authentication and digital rights management. Finally, the course looks at issues commonly ass

Lecture co-financed by the European Union in scope of the European Social Fund

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

EUROPEAN UNION
EUROPEAN
SOCIAL FUND

ociated with the management of information in terms of security protocols and procedures and addresses current problems such a securing data on the Cloud. The course is based on the book *Cryptography and Steganography,* by J M Blackledge published by the Centre for Advanced Studies, Warsaw University of Technology, 2011, and involves 20 contact hours, including presentations and tutorials and will require interested delegates to complete an examination and undertake self-study assignments equivalent to 5 ECTS.

DELEGATES WILL LEARN TO

Understand the underlying concepts and computational methods associated with data encryption and communications in a unified way; understand the basis upon which standard (and some non-standard) algorithms are constructed; design computer algorithms to investigate the encryption of different data fields; apply their knowledge to design encryption systems for specific problems; develop information hiding applications.

COURSE CONTENT

Signals and Systems	**Basic Encryption Methods**
Fundamental signal models. Temporal and spectral representations. Basic signal processing algorithms. Inverse problems and digital filters. Modulation and coding. Information entropy and statistical models. Statistical analysis and Bayesian models. Spread spectrum methods.	Brief history of cryptography. Transposition and substitution ciphers. Symmetric and Asymmetric encryption. Diffusion and Confusion based models. Stochastic field generation. Coding methods. Cryptanalysis. Cribs and attack strategies.
Computational Background	**Algorithms and Standards**
Iterative Function Systems. Random Number Generators. Randomness and Complexity. Cryptographically secure systems. Chaotic systems and signals. Encryption using Deterministic Chaos. Multi-algorithmic encryption.	Digital Encryption Standards. RSA algorithm. Advanced Encryption Standard algorithm. Key exchange algorithms. Hash functions. Public Key Infrastructure. Example applications.
Information Hiding	**Information Security Management**
Covert cryptography and watermarking. *Steganography and Steganalysis.* Watermarking methods for digital signals. Chirp coding methods. Fractal modulation. Watermarking techniques for digital images. Stochastic diffusion methods. e-to-e watermarking schemes. e-to-print watermarking methods. Authentication and self-authentication. e-Freud prevention and temper proofing. Digital Rights Management.	The human factor. Common mistakes and some case studies. Disinformation and camouflage. Network encryption algorithms. Architectures and applications. E-commerce security systems. Application in banking and finance. Mobile communications security. Statistical signature data analysis. Networking tomography. Networking topology. Cloud Computing and data security.