



Course	Data & Network Security																																										
Overview	<p>With the arrival of the Information Age, cryptography has grown to an essential tool for a wide segment of industry and commerce. It can be used to protect all forms of electronic communications such as fax, e-mail, cellular phones and home banking systems. Cryptography can replace the sealed envelope of a paper-oriented system and ensure privacy on electronic media. More important is its ability to prevent forgery of electronic documents, and to supply mutual authentication of senders and recipients of these documents. Without such tools, wide-scale electronic commerce and networks using the Internet would be impossible.</p> <p>The main focus of the course will be to provide background knowledge on the field of cryptography, data and network security to secure electronic commerce since most of today's information technology applications require security as a central system feature. Topics include and are not limited to cryptographic primitives and protocols, key management and access control, network security and electronic commerce. In each area the most important and relevant results will be introduced. Lectures will include basic techniques to provide security, information about the current state of the art and suggestions for further reading for more advanced topics.</p>																																										
Objectives	<p>The aim of this Short Course is to provide attendees with a thorough understanding of the issues associated with the design, provision and management of security services for modern communications and information systems, particularly the Internet. At the end of this course you will acquire a solid background in state-of-the-art cryptography, data and network security and you will become acquainted with up-to-date cryptographic algorithms, network protocols and standards. You will learn the different aspects of information and network security and you will be able to speak about a multitude of security attacks and the defensive strategies used to combat them. In particular, you will see why "textbook" crypto protocols and systems are vulnerable to real-life attacks and understand how to convert them to ones that are "fit for application". Finally, you will have the skills to design and assess data security schemes for given applications. It is designed as an intermediate course on the field although some advanced topics will be covered as well.</p>																																										
Who should attend	<ul style="list-style-type: none"> Engineers and other technical professionals who design, assess, or implement information security applications in software or hardware; system administrators who need to address security issues in computer networks; software engineers involved in e-commerce projects; technical managers who need a solid understanding of data security.. Students and individuals, and in fact for anyone interested in learning about the fascinating and rapidly expanding field of security in data communications. 																																										
Prerequisites	<ul style="list-style-type: none"> Basic Engineering or Computer Science background. 																																										
Dates & Duration	<ul style="list-style-type: none"> February 23,24, 2012 2 days 16 teaching hours 	<table border="1"> <thead> <tr> <th colspan="4">Class Daily Time Schedule</th> </tr> <tr> <th>Hr</th> <th>Starts</th> <th>Ends</th> <th>Intervals</th> </tr> </thead> <tbody> <tr><td>1</td><td>9:30</td><td>10:15</td><td></td></tr> <tr><td>2</td><td>10:15</td><td>11:00</td><td>11:00-11:15</td></tr> <tr><td>3</td><td>11:15</td><td>12:00</td><td></td></tr> <tr><td>4</td><td>12:00</td><td>12:45</td><td>12:45-13:00</td></tr> <tr><td>5</td><td>13:00</td><td>13:45</td><td></td></tr> <tr><td>6</td><td>13:45</td><td>14:30</td><td>14:30-14:45</td></tr> <tr><td>7</td><td>14:45</td><td>15:30</td><td></td></tr> <tr><td>8</td><td>15:30</td><td>16:15</td><td></td></tr> </tbody> </table>		Class Daily Time Schedule				Hr	Starts	Ends	Intervals	1	9:30	10:15		2	10:15	11:00	11:00-11:15	3	11:15	12:00		4	12:00	12:45	12:45-13:00	5	13:00	13:45		6	13:45	14:30	14:30-14:45	7	14:45	15:30		8	15:30	16:15	
Class Daily Time Schedule																																											
Hr	Starts	Ends	Intervals																																								
1	9:30	10:15																																									
2	10:15	11:00	11:00-11:15																																								
3	11:15	12:00																																									
4	12:00	12:45	12:45-13:00																																								
5	13:00	13:45																																									
6	13:45	14:30	14:30-14:45																																								
7	14:45	15:30																																									
8	15:30	16:15																																									
Instructors	Course Led by Tassos D. Dimitriou , AIT Professor																																										
Training Methodology	<ul style="list-style-type: none"> Lectures, International Cases of Hazard Incidents, Lab Demos 																																										
Course outline	<p>Topics include and are not limited to cryptographic primitives and protocols, key management and access control, network security protocols and electronic commerce. In each area, the most important and relevant results will be introduced. Lectures will include basic mathematics, tools, and techniques, as well as information about the current state of the art.</p> <p>The course contents 3 sessions. Changes to the order as well as the topics themselves may occur depending on the previous experience and background of the attendees on these topics.</p> <p>Session 1:</p> <ul style="list-style-type: none"> Basic cryptographic techniques (encryption and data integrity techniques in both the symmetric and public key setting) and formal approaches to security establishment Evaluation of cryptosystems against adversaries of different capabilities. Authentication protocols (notions of authentication, basic techniques, typical attacks, formal methods for authentication) <p>Session 2:</p> <ul style="list-style-type: none"> Evaluation of real-world protocol standards (IPSec, SSH, SSL, Kerberos, etc.) Esoteric protocols (Zero Knowledge, coin flipping over the telephone, quantum cryptography, etc.) Voting Systems, Digital Cash <p>Session 3:</p> <ul style="list-style-type: none"> Virtual Private Networks Intrusion Detection & Firewalls HiperLan & Bluetooth Security 																																										
Expression of Interest	execedu@ait.gr please send your contact info, including program title in email subject line																																										
Registration Form	http://hermes.ait.gr/registrations/multiple.php?prog=325																																										
Venue	AIT, Building B7, INTRACOM Campus, 19 km, Markopoulou Av, Peania 190 02 How to Reach AIT: http://www.ait.edu.gr/ait_web_site/how_to_reach_us.jsp																																										
Tuition Fee	<p>Single Participation: € 530,00</p> <p>This course is also available for in-house training for 4-10 participants @ competitive pricing Oaed funding may reach up to 100%, for more information please contact us.</p> <p>Discount Policy Cancellation Policy</p>																																										
Contact	Katerina Protonotariou, Executive Education Manager, AIT, krpo@ait.gr , 210 6682806, extn 5806																																										

