Activity Schedule
For Summer School on Information Security, 2003

Day	Time	Activity
Thursday, May 15th		
	08:30 – 11:45	Yvo Desmedt: *Introduction to Cryptography*
	11:45 – 13:15	**Lunch Break**
	13:15 – 17:00	Mike Burmester: *Introduction to Computer Security*
Friday, May 16th		
	08:30 – 11:45	Yvo Desmedt: *Introduction to Cryptography*
	11:45 – 13:15	**Lunch Break**
	13:15 – 14:30	Mike Burmester: *Provably Secure Versions of El Gamal and RSA*
	14:30 – 15:30	**Afternoon Break**
	15:30 – 17:00	Mike Burmester: *Key Distribution* (*if time permits*) Yvo Desmedt: *Denial of Service and Computer Viruses*
Monday, May 19th		
	08:30 – 11:45	Bart Preneel: *On block ciphers, hash functions, and stream ciphers*
	11:45 – 13:15	**Lunch Break**
	13:15 – 16:00	Jean-Jacques Quisquater/David Samyde: *On all aspects of smart card security and the GQ protocol / ?*
	16:00 – 17:00	Mike Burmester: *Survey of Conference Key Distribution*
Tuesday, May 20th		
	08:30 – 11:45	Bart Preneel: *On block ciphers, hash functions, and stream ciphers*
	11:45 – 13:15	**Lunch Break**
	13:15 – 17:00	Jean-Jacques Quisquater/David Samyde: *On all aspects of smart card security and the GQ protocol / ?*

Wednesday, May 21st

08:30 – 11:45	Pierangela Samarati: *On access control and database security*
11:45 – 13:15	**Lunch Break**
13:15 – 16:00	Pierangela Samarati: *On access control and database security*
16:00 – 17:00	Yvo Desmedt: *Survey of Threshold Cryptography*

Thursday, May 22nd

08:30 – 11:45	Alfred Menezes: *Elliptic curves and their applications in cryptography*
11:45 – 13:15	**Lunch Break**
13:15 – 17:00	Alfred Menezes: *Elliptic curves and their applications in cryptography*

Friday, May 23rd

08:30 – 11:45	Moti Yung: *E-voting, broadcast encryption with/without tracing, and covert channels*
11:45 – 13:15	**Lunch Break**
13:15 – 14:30	Moti Yung: *E-voting, broadcast encryption with/without tracing, and covert channels*
14:30 – 15:30	**Break**
15:30 – 17:00	Alec Yasinsac: *Wireless Security*