NATO - Advanced Study Institute, Nork, Yerevan, Armenia, 1-12 October, 2005

(Program as of 1 October, 2005)

1st day	*morning 10:30-13:00*			
	Opening Remarks and Introductions			
	Gruska	Joshef	Czech.	Quantum multiparty cryptography and network security (part 1)
	afternoon 14:00-17:30			
	Solov'eva	Faina	Russia	Switching methods for error correcting codes
	Vasil'eva	Anastasia	Russia	Reconstructive sets of binary words
2nd day	*morning 10:00-13:30*			
	Aydinian	Harout	Germany	On some External Combinatorial Problems Arising in Communication Networks
	D'yachkov	Arkadii	Russia	On DNA codes
	Agaian	Sos	USA	Steganography and Steganalysis: An Overview of Research and Challenges (part 1)
	afternoon 14:30-18:00			
	Anantharam	Venkatachalam	USA	Information theory of covert timing channels (part 1)
	Deppe	Christian	Germany	A Survey of New Results in Coding with Feedback and Searching with Lies
3rd day	*morning 10:00-13:30*			
	Krizanc	Danny	USA	Formal Methods for Proving Security Protocols
	Rykov	Vyacheslav	USA	DNA Code Generation Using an Improved Metric
	Kranakis	Evangelos	Canada	Dynamics of Network Worms (part 1)
	afternoon 14:30-18:00			
	Lebedev	Vladimir	Russia	On (w,r) cover-free codes
	Anantharam	Venkatachalam	USA	Information theory of covert timing channels (part 2)
	Agaian	Sos	USA	Steganography and Steganalysis: An Overview of Research and Challenges (part 1)
4th day	*morning 10:00-13:30*			
	Kranakis	Evangelos	Canada	Dynamics of Network Worms
	Gruska	Joshef	Czech.	Quantum multiparty cryptography and network security (part 2)
	Bouda	Jan	Czech.	Exact and approximative encryption of quantum information (part 1)
	afternoon 14:30-18:00			
	Gevorkyan	Ashot	Armenia	New Mathematical approach for stochastic quantum processes, their manipuation and control
	Kruegel	Christopher	Austria	Advanced Techniques for Malicious Code Detection
	Patera	Jiri	Canada	One and two dimensional aperiodic point sets ("quasicrystals") in cryptography (part 1)
	5th day Excursions			
6th day	*morning 10:00-13:30*			
	Uros	Janko	Germany	Technology Briefing – Pattern Signature Recognition™ (PSR™)
	Gruska	Joshef	Czech.	Quantum multiparty cryptography and network security (part 3)
	Bouda	Jan	Czech.	Exact and approximative encryption of quantum information (part 2)
	afternoon 14:30-18:00			
	Patera	Jiri	Canada	One and two dimensional aperiodic point sets ("quasicrystals") in cryptography
	Kruegel	Christopher	Austria	Advanced Techniques for Malicious Code Detection
	Agaian	Sos	USA	Steganography and Steganalysis: An Overview of Research and Challenges

7th day	*morning 10:00-13:30*			
	Keromytis	Angelos	USA	Self-healing software
	Prelov	Viacheslav	Russia	Asymptotic investigation of mutual information and capacity of certain communication channels
	Gyarmati	Katalin	Hungary	On finite pseudorandom binary sequences (part 1)
	afternoon 14:30-18:00			
	Koval	Oleksiy	Switzerland	Multimedia security: open problems and solutions (Part 1)
	Voloshynovskiy	Sviatoslav	Switzerland	Multimedia security: open problems and solutions (Part 2)
	Haroutunian	Mariam	Armenia	E-capacity of Information hiding systems
8th day	*morning 10:00-13:30*			
	Kotenko	Igor	Russia	Multi-agent Modeling and Simulation of Computer Network Security Processes
	Pogosyan	Edward	Armenia	Simulation of Sttrategy Knowledge for security and competition problems (part 1)
	Ksheveckiy	Alexander	Russia	Public cryptosystems based on linear codes (part 1)
	afternoon 14:30-18:00			
	Desmedt	Yvo	UK	Security when routers are taken over by the adversary
	Burmester	Mike	USA	Using wireless overlay networks for secure management of network resources and to prevent extreme attack
9th day	*morning 10:00-13:30*			
	Preneel	Bart	Belgium	Security of wireless networks: GSM, UMTS, Bluetooth, WLAN
	Kabatiansky	Gregory	Russia	Tracing traitors and collusion-secure fingerprinting via general secret sharing schemes
	Tairyan	Vasil	Armenia	Humanitarian problems in informational security
	afternoon 14:30-18:00			
	Poster Presentations (10 minutes presentations per poster with everyone, before the poster session)			
	Oit	Monica	Estonia	E-voting and other security products at Cybernetica
	Fiore	Basile	Italy	TBD
	10th day Excursions in the morning			
11th day	*morning 10:00-13:30*			
	Ksheveckiy	Alexander	Russia	Public cryptosystems based on linear codes (part 2)
	Gyarmati	Katalin	Hungary	On finite pseudorandom binary sequences (part 2)
	Movsisyan	Yuri	Armenia	Representations of Algebras by Fuzzy Sets
	afternoon 14:30-18:00			
	Arikan	Erdal	Turkey	Guessing and Cryptography
	Haroutunian	Evgueni	Armenia	Reliability Approach in Wiretapper Guessing
	Harutyunyan	Ashot	Germany	On reliably optimal hierarchical transmission
12th day	*morning 10:00-13:30*			
	Pogosyan	Edward	Armenia	Simulation of Sttrategy Knowledge for security and competition problems (part 2)
	Shahbazian	Elisa	Canada	Introduction to Data Fusion
	Gyarmati	Katalin	Hungary	On finite pseudorandom binary sequences
	afternoon 14:30-18:00			
	Sarukhanyan	Hakob	Armenia	Integer to Integer transforms: Synthesis and Applications
	Mkrtumyan	Karen	Armenia	Statistical approach to fight against froud in telecomunication (1 hour)
	Plenary Discussion on Cyber Security Research Future Developments and International Collaboration			
	Closing Remarks			