Program for Norsk Kryptoseminar 2003

10. - 11. november, 2003

Navn	Org	Tittel	Tid (min)
Mandag 10.00 - 12.00: Oversikt			
Tor Helleseth	Selmersenteret, UiB	Åpning og presentasjon av Selmersenteret	20 min
Kjell Jørgen Hole	Selmersenteret, UiB	Forskning på trådløse nett ved Selmersenteret	30 min
Helge Lægreid	Nasjonal Sikkerhetsmyndighet	Forprosjekt PKI i Forsvaret	30 min
Øyvind Eilertsen	Senter for informasjonssikring (SIS)	SIS - ett år senere	30 min
Lunsj			
Mandag 13.00 - 15.00: Kryptografi og andvendelser			
Lars R. Knudsen	Dansk Teknisk Universitet	Message Authentication Codes	60 min
Leif Nilsen	Thales Communications AS	Multippel kryptering	25 min
Tønnes Brekne	Q2S, NTNU	Monoalfabetisk substitusjon for Turing maskiner	30 min
Kaffe			
Mandag 15.30 - 17.00: Elliptiske kurver			
Loren Olson	IMS, Univ. i Tromsø	Forsvarsmekanismer i ECC	30 min
Tormod K Sivertsen	Universitetet i Tromsø	Klassegrupper og kryptografi	20 min
Hilja Lisa Huru	UiTø/UiB		20 min
Hugues Verdure	IMS, Univ. i Tromsø	Torsjons undergrupper på elliptiske kurver	15 min
Mandag 19.00 - : Sosialt arrangement			
Tirsdag 09.00 - 10.20: Algebra og kryptologi			
Terje Jensen	Nasjonal Sikkerhetsmyndighet	Den algebraiske strukturen til AES (BES)	25 min
Kristian Gjøsteen	IMF, NTNU	Undergruppeproblemer	20 min
Berner Larsen	Høgskolen i Bodø	Number Field Sieve	15 min
Øyvind Grinde	Universitetet i Tromsø	Irredusible Polynomer	20 min
Kaffe			
Tirsdag 10.40 - 12.00: Kryptografi og anvendelser			
Anders Paulshus	Nasjonal Sikkerhetsmyndighet	Kompleksitetsteori og kryptografi	25 min
Tore Mortensen	FO/E	Harddiskkryptering	20 min
Espen Torseth	NISLAB og ErgoIntegration		15 min
Christian Veigner	HiS	Sequrity challenges during transition to NGI	15 min
Lunsj			
Tirsdag 13.00 - 14.40: Kryptografi og kryptoanalyse			
Håvard Molland	Selmersenteret, UiB	Attakcing additive Stream Ciphers	30 min
Håvard Raddum	Selmersenteret, UiB	Sparse ligningssystemer over endelige ringer	30 min
Vebjørn Moen	Selmersenteret, UiB	Weaknesses in WPA	20 min
John Erik Mathiassen	Selmersenteret, UiB	Linear Cryptanalysis	20 min
Kaffe			
Tirsdag 15.10 - 16.15: Kryptografi og anvendelser			
Geir Johansen	Thales Communications AS	Trusted VPN	20 min
Gunnar Alendal	FO/E	got crypto? Om misbruk av krypto	30 min
Dag Arne Osvik		Effektiv implementasjon av blokkchiffer	15 min