

## Om NSM

Nasjonal sikkerhetsmyndighet (NSM) beskytter Norge mot spionasje-, sabotasje- og terrorhandlingar. NSM er eit sivilt direktorat under både Forsvars- og Justisdepartementet. Vi driv forebyggjande sikkerheitsarbeid, og har høg kompetanse innan IKT-sikkerheit, dokumentsikkerheit, fysisk sikring og personellsikkerheit. Vi har som mål å vera ein anerkjent og synleg pådrivar for betre sikkerheit i samfunnet. Vi har i dag ca. 140 tilsette, og held til på Kolsås og Akershus Festning.

Nasjonal sikkerhetsmyndighet  
Postboks 14, 1306 Bærum postterminal  
<http://www.nsm.stat.no/>

Telefon 67 86 00 00  
Telefaks 67 86 40 09  
E-post [post@nsm.stat.no](mailto:post@nsm.stat.no)

## Norsk kryptoseminar

13.-14. oktober 2008

Forsvarets høgskolesenter  
Bygning 10  
Akershus festning

Nasjonal sikkerhetsmyndighet

## Måndag 13. oktober

10:00-10:05	Turid Herland <i>Velkommen</i>
10:05-10:20	Bernt Erik Baltzersen <i>Conax CA del I: Noen nøkkelsides</i>
10:25-10:45	Tønnes Brekne <i>Conax CA del II: Inn fra sidekanalen</i>
10:50-11:10	Øystein Thuen <i>Beregning av Hilbert klassepolynom</i>
11:15-12:15	Lars Knudsen <i>Hash funksjoner</i>
12:15-13:00	Lunsj
13:00-13:20	Asgeir Steine <i>UC-Sikkerhet og Ubestemmelige Nøkler</i>
13:25-13:40	Per Harald Myrvang <i>HSM i nettverk</i>
13:45-14:00	Martin Eian <i>Tjenestene i trådløse nettverk</i>
14:05-14:25	Kristian Gjøsteen <i>Anonymitet i mobiltelefonnettverk</i>
14:25-14:40	Pause
14:40-15:10	Trygve Johnsen <i>Om matroidelignende strukturer og visse typer kryptosystemer</i>
15:15-15:35	Tord Ingolf Reistad <i>Multiparty computation</i>
15:40-16:00	Stig F. Mjølunes <i>Undervisningslab i anvendt krypto</i>
16:05-16:15	Pause
16:15-16:30	Rune Steinsmo Ødegård <i>Hash function Edon-R</i>
16:35-16:50	Turid Herland & Olaf Garnaa <i>Harddiskkrypto</i>
16:55-17:00	Turid Herland <i>Info om økonomisk støtte</i>

## Tysdag 14. oktober

09:00-09:25	Adnan Visic <i>[hiddn] Opportunities</i>
09:30-09:45	Son Thanh Nguyen <i>Key Pre-distribution in Wireless Sensor Networks using Combinatorial Design</i>
09:50-10:05	Pause
10:05-10:20	Loren Olson <i>GLV algoritme for rask multiplikasjon på elliptiske kurver.</i>
10:25-10:45	Anton Stolbunov <i>Public-Key Cryptography based on Isogenous Elliptic Curves</i>
10:50-11:10	Hugues Verdure <i>Paringer i EKK</i>
11:15-12:15	Kjell Kjeldsen <i>Elektronisk krypto gjennom 50 år</i>
12:15-13:00	Lunsj
13:00-13:30	Tor Hellesest <i>On recent attacks on the filtergenerator</i>
13:35-13:55	Leif Nilsen <i>Rejewskis rekonstruksjon av Enigmarotorene</i>
14:00-14:20	Anders Paulshus <i>Hvordan knekke Bitlocker</i>
14:25-14:35	Pause
14:35-14:55	Abdul Based <i>Architecture and Characteristics of Internet based Voting</i>
15:00-15:30	Kent Johnny Dokmo & Hans-Petter Gundersen <i>NSM TEMPEST</i>
15:35-16:00	Audun Jøsang <i>Brukervennlighet i informasjonssikkerhet</i>

## Middag

Det blir felles middag til sjølvkost for dei som vil på Olivia på Aker Brygge måndag kveld kl. 19:00.

