DEPARTAMENTO de MATEMÁTICAS

SEMINARIO

(conjunto con las **Jornadas de Criptografía SCD 2011**)

http://www.matematicas.um.es/

17:00 Sandra Guasch (Scytl, Secure Electronic Voting)

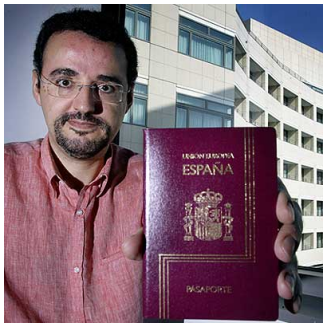
Cryptographic protocols for transparency and auditability in remote electronic voting schemes

Remote electronic voting systems have to meet some security requirements in order to ensure a fair election process. However, the use of electronic means for conducting an election poses some new security risks that have to be taken into account when designing such a system: what happens if software is corrupt or there is a hacker attack? In this scheme, cryptographic algorithms and protocols can be used to provide transparency and auditability means for ensuring the correctness of the system behavior.

In this talk we are going to explain which are the cryptographic tools that can be used in remote electronic voting schemes for ensuring transparency and auditability.

17:30 Jordi Íñigo (Safelayer, Secure Communications S.A.)

Security and PKI



Currently the PKI (Public Key Infrastructure) technology is used extensively on different devices and for different purposes. In this presentation a short summary of current use cases of PKI will be presented, as well as how the different PKI actors and authorities combine to participate in those use cases. A brief comment on cryptographic algorithms in use in PKI will be given, and what the situation will be in the foreseeable future (if a forecast is worth the effort...). Risk and threads on PKI will also be commented.

Jueves 17 de noviembre de 2011

Salón de Actos

A las 16:30 se servirá un café en la Sala Euler

Departamento de Matemáticas, Campus Universitario de Espinardo, 30100 Murcia (España)
Teléf.: 968363519. FAX: 968364182. e-mail: depmat@um.es