École de Printemps

Cryptographie et sécurité informatique

PROGRAMME

www.laas.fr/crypto-sec/

PROGRAMME

Lundi 24 avril

Matin *Arrivée*

12h30 *Déjeuner*

14h00 *Jean-Jacques Quisquater* (*Université Catholique de Louvain, Belgique*)
La cryptographie par la théorie des graphes

20h30 *Dîner*

Mardi 25 avril

9h00 *Yves Deswarte* (*LAAS-CNRS, France*)
Protection de la vie privée sur Internet

12h30 *Déjeuner*

14h00 *Yannick Chevalier* (*IRIT, France*)
Analyse de protocoles dans un modèle abstrait

20h30 *Dîner*

Mercredi 26 avril

9h00 *Jean-Marc Couveignes* (*GRIMM, France*)
Cryptologie asymétrique, factorisation et logarithme discret

12h15 *Déjeuner*

13h30 *Excursion (visite de Carcassonne)*

18h30 *Paulo Veríssimo* (*Université de Lisbonne, Portugal*)
Architectures tolérant les intrusions : concepts et conception

21h00 *Dîner*

Jeudi 27 avril matin

9h00 *Peter Ryan* (*Université de Newcastle, Grande-Bretagne*)
"Prêt à Voter" : Un système de vote électronique pratique et vérifiable par les votants

12h15 *Déjeuner*

13h30 *Pierre Paradinas* (*CNAM-CEDRIC, France*)
(i) Mesures de performances des systèmes embarqués du type Java Card
(ii) Virtualisation de système et sécurité

17h30 *Sandra Marcello* (*Thales, France*)
Cryptosystèmes basés sur l'identité

20h30 *Dîner*

Vendredi 28 avril matin

9h00 *Serge Vaudenay* (*EPFL, Suisse*)
Comment échanger une clef après 30 ans de Diffie-Hellman ?

12h15 *Déjeuner*

13h30 *Yvo Desmedt* (*University College London, Grande-Bretagne*)
Déni de service et sécurité des réseaux de télécommunication

16h30 *Départ*