LEÇON 1 17.03.2011 17:30

Assurer la confidentialité entre partenaires

Cette première conférence aborde le thème classique d'un échange de messages confidentiels entre deux parties qui se connaissent et qui ont la possibilité de fixer d'un commun accord les procédés et les modalités secrètes de la communication. Il s'agit d'une part du champ de la cryptographie classique et de ses multiples procédés et variantes historiques, d'autre part de son prolongement moderne par la cryptologie basée sur des messages digitaux utilisés dans les communications modernes. Ce volet nous mènera vers les approches scientifiques et les standards de la cryptographie symétrique, en présentant les techniques utilisées actuellement.

LEÇON 2 31.03.2011 attention 17:00 Auditoire Tavenas

Assurer la confidentialité dans la société de l'information

La grande différence avec le contexte de la conférence précédente, c'est que cette fois les intervenants ne se connaissent pas forcément, mais voudraient néanmoins échanger des messages confidentiels, par exemple dans un contexte de commerce électronique ou de messagerie électronique. Ce n'est que depuis une trentaine d'années qu'on connaît des techniques pour le faire : c'est le champ de la cryptographie asymétrique, avec l'utilisation d'une paire de clés, dont l'une seulement est publique. Cette cryptographie à clé publique est à la base de tout le fonctionnement de la société de l'information, en permettant l'échange de clés pour la cryptographie symétrique, mais en fournissant aussi des moyens d'authentification forte, tels que nécessaires pour la signature électronique ou l'identification à distance.

LEÇON 3 14.04.2011 17:30

Communiquer de façon discrète

La communication chiffrée par des techniques cryptographiques fortes ne manque pas d'éveiller l'attention et éventuellement la suspicion d'observateurs externes curieux. Voilà pourquoi il est parfois nécessaire de cacher le fait même de l'échange d'un message confidentiel, en le recouvrant par des messages anodins et non suspects. Il s'agit du champ de la stéganographie, qui étudie les techniques permettant de dissoudre un message à l'intérieur d'un autre message ou ensemble de données : textes, images, sons, films, et de le reconstituer de nouveau en le distillant à destination. Ces techniques, aussi anciennes que l'histoire des communications, ont connu un développement extraordinaire dans le monde digital. D'autres techniques ont pour but de cacher à un observateur curieux le destinataire d'une communication en empruntant des canaux multiples et en brouillant les pistes.

LEÇON 4 05.05.2011 17:30

Signer un document électronique

La signature électronique est un concept dont on parle beaucoup, mais dont bien peu de gens connaissent le fonctionnement véritable, ce qui rend cette signature mystérieuse et amène parfois un doute quant à la sécurité ou la valeur juridique d'une telle signature. Bien que la signature électronique repose sur les fondements scientifiques solides de la cryptographie asymétrique, sa mise en œuvre sur le terrain se révèle délicate, car elle fait intervenir des acteurs nouveaux, tels les tiers de confiance, ou des contextes plus larges, comme l'environnement légal ou les standards internationaux. De plus, il y a aussi des aspects économiques qui interviennent, requérant des investissements énormes de la part des prestataires de services de signature, ce qui engendre de l'autre côté des coûts pour les signataires, réduisant en même temps l'attractivité de ces procédés. La conférence vise à intégrer tous ces aspects au cœur même de la société de l'information.

LEÇON 5 19.05.2011 17:30

Payer électroniquement

Est-il possible de créer par des moyens purement digitaux de l'argent électronique, infalsifiable et non copiable ? La conférence explorera certaines techniques d'argent électronique en présentant les possibilités, mais aussi les limites de ces techniques. Dans un deuxième volet, on passe ensuite aux techniques de paiement électronique sécurisé permettant de satisfaire aussi bien le client, que le commerçant et la banque. Finalement, on abordera aussi les standards EMV utilisés dans les nouvelles cartes de crédit.