



# Sécurité et informatique, introduction à la cryptographie



## Descriptif

La cryptographie est devenue omniprésente dans la société numérique. Tout système de commerce électronique l'utilise. Le nombre de situations faisant appel aux fonctions de sécurité que la cryptographie assure est maintenant énorme.

Cet exposé des fondements de la Science du secret doit permettre de déterminer la sécurité que la cryptographie peut apporter pour protéger un système d'information et diminuer ses vulnérabilités. Il doit aussi permettre de poser les questions pertinentes aux fournisseurs de solutions de sécurité. Ce séminaire pourra être centré sur certaines questions spécifiques en fonction des attentes des participants.

### Durée :

1 jour

### Objectifs :

- Acquérir les concepts, les méthodes et les outils pour une action de changement efficace au sein d'une conduite de projet
- Lier la décision stratégique à la mise en œuvre d'un projet : mesurer l'importance du facteur humain afin d'évaluer les pièges et les potentialités

### PUBLIC

Décideurs  
Chefs de projets  
Experts métier  
Analystes  
Concepteurs  
Développeurs

### Introduction

- Cryptologie science du secret
- Fonctions de sécurité assurées par la cryptographie
- Authentification des entités
- Intégrité des données
- Chiffrement
- Signature et non-répudiation

### Cryptanalyse

- Principe de Kerckhoff
- Les attaques cryptanalytiques et par force brute

### Cryptographie classique

- Substitution et transposition
- Le chiffre de Vigenère
- La Machine Allemande Enigma
- Les attaques

### Algorithme de chiffrement de données

- Confusion et diffusion
- Algorithmes par bloc : DES, AES
- Les différents modes des algorithmes de chiffrement par bloc
- Chiffrement par flux
- Problème de la génération des aléas

### Algorithme à clef publique

- Problème de la transmission des clés
- Echange de secret à la Diffie-Hellman

- Système RSA
- Courbes elliptiques
- Complexité et sécurité

### Intégrité des données

- Authentification des messages : MAC
- Fonctions de hachage : MD5, SHA
- Fonctions HMAC
- Sécurité des fonctions de hachage

### Signature électronique

- Utilisation de la clef privée
- Nécessité des certificats
- Annuaire électronique

### Application : Authentification dynamique des entités

- Utilisation du temps
- Protocole Aléa-Réponse
- Méthodes incrémentales
- Protocoles à apport nul de connaissance
- Implémentations : Token, Clef USB, Carte à puce

### Panorama de solutions du marché

Commandez votre session inter/intra au tél. 01 44 94 92 50

### Prochaines sessions inter-entreprise :

1 juillet – 2 octobre – 30 décembre