

Objectifs

- ▶ Comprendre les algorithmes de chiffrement
- ▶ Comprendre la cryptographie en entreprise
- ▶ Connaître les faiblesses des implémentations cryptographiques

Des travaux pratiques seront effectués tout au long de la formation sur des systèmes Windows et Unix.

Pré-requis

- ▶ Connaissance du langage C
- ▶ Connaissances de base d'arithmétique et d'algèbre

Contenu

- ▶ Introduction à la cryptologie
- ▶ Cryptographie en entreprise
- ▶ Faiblesses des implémentations cryptographiques

Programme détaillé au dos.

Informations pratiques

- ▶ Participants : un maximum de 10 inscrits
- ▶ Formateur : expert sécurité/R&D
- ▶ Matériel : poste individuel, mêmes systèmes et outils que le formateur
- ▶ Locaux : 75 avenue Victor Hugo 92 500 Rueil-Malmaison
5 minutes à pieds du RER Rueil-Malmaison (sortie 5 Victor Hugo)
(Parking disponible sur simple demande)

Durée : 3 jours

Code : CRY

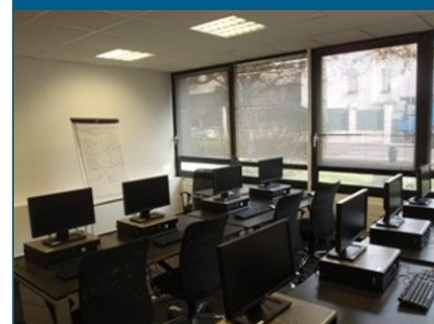
Prix : 2 400 € HT

Catalogue :

www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00



Jour 1 : Introduction à la cryptologie

Concepts et vocabulaire	
Rappels de mathématiques	Probabilités, notions de théorie l'information Théorie des nombres (congruences) Algèbre (polynômes, groupes, corps finis (Z_p , $F_p[x]/P_n(x)$)) Notions de complexité algorithmique
Modes de chiffrement algorithmique	Cesar, Vigenere, Vernam
Cryptographie symétrique	Chiffrement par bloc Chiffrement par flux
Cryptographie asymétrique	Pourquoi la crypto asymétrique ? Inconvénients ? Avantages ? Génération des nombres premiers Factorisation des grands nombres (RSA) Problème du logarithme discret Autres problèmes intéressants (Merkle Hellman, McEliece) Chiffrement à la mode (HFE, Courbes elliptiques)
Hash, signature	Notion de hash Notion de MAC Algorithmes de signature (RSA/DSA) Cas particulier S/MIME

Jour 2 : Cryptographie en entreprise

Notion de PKI	Les différentes briques (AC, AE, CRL) Notion de certificat (x509v3) (DER, PEM/ASN1) Impact de la sécurité des fonctions de hashage sur celle des PKI Distribution des certificats (notion d'annuaire)
Protocoles réseaux de chiffrement	Pourquoi sécuriser les protocoles ? Quels sont les menaces ? 3 protocoles = 3 besoins : SSL, SSH, IPSEC
Authentification, chiffrement de volumes	Cas Unix Cas Windows

Jour 3 : Faiblesses des implémentations cryptographiques

Algorithme de chiffrement et cryptanalyse	
Erreurs classiques d'implémentation en cryptographie	Mauvaise compréhension de la cryptographie Mauvaise gestion des paramètres Les problèmes de padding Les défauts d'entropie
Les cas des attaques par canaux cachés	Les attaques ciblant le software Les attaques contre le hardware