Fondamentaux Cryptographie

Lien : https://innov-systems.com/formation/fondamentaux-cryptographie

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC72

CATÉGORIE
Sécurité Technique : Cryptographie, Protocoles et Infrastructures

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les différentes techniques cryptographiques
- Identifier les méthodes d’échange, gestion et certification des clés publiques
- Mettre en œuvre les outils de chiffrement symétrique et asymétrique

POUR QUI ?

- Administrateurs
- Chefs de Projet
- Consultants
- Développeurs
- Ingénieurs
- Responsable sécurité

Programme détaillé

1 / Introduction à la Cryptographie

- Histoire de la cryptographie
- Histoire des premiers documents chiffrés
- Services de sécurité fournis par la cryptographie
- Quelques outils et concepts mathématiques
- Types de menaces et vulnérabilités

2 / Le chiffrement de flux (stream cipher)

- Présentation du concept
- Formes de chiffrement de flux :
- LFSR (Linear Feedback Stream Register)
- RC4 (Rivest Cipher 4)

3 / Le chiffrement par blocs (block cipher)

- Présentation du concept
- Formes de chiffrement par blocs :
- ECB (Electronic CodeBook)
- CBC (Cipher-Bloc Chaining)
- CFB (Cipher FeedBack) et CTR (CounTeR)
- Comparer le chiffrement de flux (stream cipher) et par blocs (block cipher)
- L’algorithme Data Encryption Standard (DES)
- 2DES et Triple DES (3DES)
- Advanced Encryption Standard (AES)
- Autres algorithmes courants (Blowfish, Serpent, Twofish…)
- Algorithmes complémentaires : IDEA, RC5, SAFER

4 / Chiffrement asymétrique

- Concepts de fonctionnement
- L’exemple du cryptosystème de Merkle-Hellman
- RSA (Rivest, Shamir et Adleman)
- Sécurité et taille des clés
- Attaques et défi RSA
- Description du protocole ElGamal

5 / Fonctions de hachage

- Définition d’une fonction de hash
- Concept et objectifs
- Principes théoriques et propriétés de base
- Justifications pratiques des différentes propriétés
- Classification des fonctions de hachage
- Degré de difficulté, taille et sécurité du hachage
- Hachage simple (Unkeyed) et sécurisé (Keyed) : chiffrement par blocs. Fonction MD4
- Attaques avancées sur les fonctions de hachage
- La technique : algorithmes MD5, SHA-1, SHA-256...

6 / Intégrité et authentification

- Présentation
- Code d’authentification de message (MAC, Message Authentification Code
- NMAC et HMAC, CBC-MAC
- Signature électronique. Signature DSA et RSA
- Vulnérabilités pour les signatures numériques
- Autorités de certifications et standards
- Les spécifications PKCS de cryptographie à clé publique

7 / Gestion des clés

- Echange de clés avec le chiffrement symétrique et asymétrique. Détail des échanges
- Echange de clés Diffie-Hellman, attaque de l’homme du milieu (man in the middle)
- Architectures PKI (Public Key Infrastructure) pour la gestion des clés
- X.509, structure des certificats
- Révocation, renouvellement et archivage des clés
- Certificats au format X509, norme PKIX
- L'infrastructure de gestion des clés (IGC/PKI)

8 / Tierces parties de confiance

- Présentation et standards. Architectures
- Autorité de certification. Kerberos

9 / Cas Pratiques

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

04 au 07 Août 2026	Présentiel - Casablanca
29 Sep. au 02 Oct. 2026	Distanciel
24 au 27 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com