

Formation Cryptographie : apprendre à protéger l'information

Réf. SF33648

Une formation de 2 jours pour comprendre les grands principes et algorithmes cryptographiques

2 j Durée	1 500 € HT Inter / participant	4 100 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ S'approprier les enjeux et concepts fondamentaux de la cryptographie moderne
- ✓ Identifier les méthodes et outils de chiffrement, déchiffrement, authentification ou encore garantie d'intégrité des messages
- ✓ Connaître les techniques cryptographiques les plus utilisées

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Chefs de projet, Développeurs, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis Connaissances de base sur les systèmes d'information, quelques notions en algèbre linéaire et en arithmétique aideront à la compréhension des différents algorithmes étudiés, mais ce cours est accessible aux non-mathématiciens.

Programme détaillé

Introduction à la formation Cryptographie

Présentation générale et objectifs de cette formation d'introduction à la cryptographie
Petite histoire de la cryptographie et des premiers documents chiffrés
Vue d'ensemble de la cryptographie moderne, terminologie
Bien distinguer cryptographie, cryptanalyse et stéganographie
Définitions et concepts clés : chiffrement/déchiffrement, clé, vecteur d'initialisation...
Services de sécurité fournis par la cryptographie : confidentialité, authenticité, intégrité et non-répudiation
Types de menaces et vulnérabilités
Quelques outils et concepts mathématiques
Le principe de Kerckhoffs et la maxime de Shannon
Organismes et acteurs à connaître : NITS, AFNOR, RSA Security
Exemples d'algorithmes cryptographiques simples : code de César, ROT13, chiffrement de Vigenère

Cryptographie symétrique (à clé secrète)

Cryptographie symétrique et cryptographie asymétrique
Comparer le chiffrement de flux (stream cipher) et par blocs (block cipher)
Formes de chiffrement de flux : LFSR (Linear Feedback Stream Register), RC4 (Rivest Cipher 4)
Formes de chiffrement par blocs : ECB (Electronic CodeBook), CBC (Cipher-Bloc Chaining), CFB (Cipher FeedBack) et CTR (CounTeR)
Avantages et inconvénients de la cryptographie symétrique
L'algorithme Data Encryption Standard (DES), pourquoi n'est-il plus recommandé aujourd'hui ?
2DES et Triple DES (3DES) : fonctionnement et mise en œuvre
Advanced Encryption Standard (AES) et autres algorithmes courants (Blowfish, Serpent, Twofish...)

Fonctions de hachage cryptographiques

Qu'est-ce qu'une fonction de hash ? Concept et cas d'utilisation
Principes théoriques et propriétés de base : attaques, collisions, pré-images
Classification des fonctions de hachage
Degré de difficulté, taille et sécurité du hachage
La technique : algorithmes MD5, SHA-1, SHA-256...

Cryptographie asymétrique (à clé publique et privée)

Concepts de fonctionnement, l'exemple du cryptosystème de Merkle-Hellman
RSA (Rivest, Shamir et Adleman), fonctionnement détaillé
Description du protocole ElGamal

Intégrité, authentification : signatures et certificats numériques

Code d'authentification de message (MAC, Message Authentication Code)
NMAC et HMAC, CBC-MAC
Signatures DSA et RSA
Vulnérabilités pour les signatures numériques : le paradoxe des anniversaires
Autorités de certifications et standards
Les spécifications PKCS de cryptographie à clé publique
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

Exemples de cas pratiques réalisés durant la formation

Manipulations des outils cryptographiques d'OpenSSL
Calculs d'empreintes, chiffrement, déchiffrement de documents
Certificats auto-signés
Méthodes pour la vérification de protocoles cryptographiques, exemple avec JWT (RFC 7519)
Mise en place d'HTTPS sur un serveur Apache
Transmission d'e-mails avec GPG
Echange de clés, travail sur la notion de confiance

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Michael G. — Formateur Cybersécurité

Michael intervient sur des formations portant sur la sécurité défensive et l'architecture de sécurité (Blue Team). Les sujets abordés incluent notamment la cybersécurité. Son activité de formation remonte à 2023.

Ils nous font confiance

Cette année notre filière Sécurité Défensive & Architecture (Blue Team) a accompagné plus de 25 entreprises dont :

ADVENTIEL ALTEN SA AMCS TECHNOLOGIES ARPEGE BIRDZ CA-GIP CHAPSVISION CHELA + CONSORT FRANCE ECONOCOM SERVICES & SOLUTION +15 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com