

Formation Cryptographie, Introduction et concept clés

Présentation

Ce programme de formation introduit la cryptographie, ses concepts clés et son histoire. Il couvre la cryptographie symétrique et asymétrique, les fonctions de hachage et les signatures numériques. Les participants apprendront également à utiliser des outils cryptographiques et à mettre en place des protocoles de sécurité.

Durée : 14,00 heures (2 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Décrire les principales techniques de chiffrement/déchiffrement
- Garantir l'intégrité des messages

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.

Public

- Administrateurs systèmes et réseaux,
- Chefs de projet,
- Responsables de la sécurité des systèmes d'information (RSSI),
- Développeur

Programme de la formation

Introduction – Fondamentaux de la cryptographie

- Présentation des objectifs de la formation
- Histoire de la cryptographie et premiers systèmes de chiffrement



- Vue d'ensemble de la cryptographie moderne et terminologie
- Distinction entre cryptographie, cryptanalyse et stéganographie
- Concepts clés : chiffrement, déchiffrement, clé, vecteur d'initialisation
- Services de sécurité : confidentialité, intégrité, authenticité, non-répudiation
- Typologie des menaces et vulnérabilités
- Principes fondamentaux : Kerckhoffs et maxime de Shannon
- Acteurs et standards (NIST, AFNOR, RSA Security)
- Algorithmes simples : César, ROT13, Vigenère

Cryptographie symétrique

- Différences entre cryptographie symétrique et asymétrique
- Chiffrement de flux vs chiffrement par blocs
- Algorithmes de flux : LFSR, RC4
- Modes de chiffrement : ECB, CBC, CFB, CTR
- Avantages et limites des approches symétriques
- DES : limites et obsolescence
- 2DES et 3DES : fonctionnement
- Algorithmes modernes : AES, Blowfish, Serpent, Twofish

Fonctions de hachage

- Concept et cas d'usage des fonctions de hachage
- Propriétés fondamentales : collisions, pré-image, résistance
- Classification des fonctions de hachage
- Facteurs de sécurité : taille et robustesse
- Algorithmes : MD5, SHA-1, SHA-256

Cryptographie asymétrique

- Principes de la cryptographie à clé publique
- Exemple du cryptosystème de Merkle-Hellman
- Fonctionnement de RSA
- Principe du protocole ElGamal

Intégrité, authentification et certificats

- MAC : Message Authentication Code
- NMAC, HMAC, CBC-MAC
- Signatures numériques : DSA et RSA
- Vulnérabilités : paradoxe des anniversaires
- Autorités de certification et standards
- Spécifications PKCS
- Échange de clés Diffie-Hellman et attaques MITM
- Architecture PKI (Public Key Infrastructure)
- Certificats X.509

Cas pratiques

- Utilisation de :contentReference[oaicite:0][index=0]
- Calcul d'empreintes et chiffrement de documents
- Création de certificats auto-signés
- Analyse de protocoles (ex. JWT – RFC 7519)
- Mise en place de HTTPS sur serveur Apache
- Chiffrement d'e-mails avec GPG
- Échange de clés et gestion de la confiance

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétence.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.