DOCAPOSTE Institute

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- 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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

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

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

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

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France