Initiation à la Cryptographie

1 j (7 heures) Ref : IABC008

Public

Responsables sécurité, développeurs, chefs de projets, responsables de la sécurité des systèmes d'information

Pré-requis

Connaissances de base en informatique
Aucune expérience préalable en cryptographie n'est nécessaire

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Nombreux exercices pratiques et mises en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif. Vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

La formation "Initiation à la Cryptographie" est une session d'une journée conçue pour introduire les concepts fondamentaux de la cryptographie aux professionnels de l'informatique et aux développeurs. Cette formation couvre les bases de la cryptographie, y compris les algorithmes de chiffrement symétrique et asymétrique, les fonctions de hachage, et les signatures numériques. Les participants apprendront comment ces techniques sont utilisées pour sécuriser les communications et les données, ainsi que les applications pratiques de la cryptographie dans la technologie blockchain.

Cette formation d'une journée offre une introduction complète et pratique aux concepts fondamentaux de la cryptographie, permettant aux participants de comprendre et d'appliquer les techniques de base pour sécuriser les informations et les communications dans divers contextes professionnels.

Objectifs

Comprendre les principes fondamentaux de la cryptographie

Apprendre les différences entre les algorithmes de chiffrement symétrique et asymétrique

Utiliser les fonctions de hachage pour assurer l'intégrité des données

Appliquer les signatures numériques pour l'authentification et la non-répudiation

Découvrir les applications pratiques de la cryptographie dans la sécurité des systèmes d'information et la blockchain

Programme détaillé

INTRODUCTION A LA CRYPTOGRAPHIE

HISTORIQUE ET IMPORTANCE DE LA CRYPTOGRAPHIE

La cryptographie, bien que vieille de plusieurs siècles, reste cruciale dans la sécurité des informations sensibles à travers les âges. De l'Antiquité avec les techniques de substitution des lettres aux méthodes modernes basées sur des algorithmes complexes, son évolution continue de façonner la manière dont nous sécurisons les données numériques dans le monde contemporain.

PRINCIPES FONDAMENTAUX DE LA CRYPTOGRAPHIE

CONCEPTS CLES

Nous introduisons les concepts clés de la cryptographie moderne : la confidentialité, qui garantit que seules les parties autorisées peuvent accéder à l'information ; l'intégrité, qui assure que les données n'ont pas été altérées ou corrompues ; l'authentification, qui vérifie l'identité des entités communicantes ; et la non-répudiation, qui empêche les parties d'ignorer ou de nier l'origine ou la réception d'un message.

CHIFFREMENT SYMETRIQUE

ALGORITHMES DE CHIFFREMENT SYMETRIQUE

Nous explorons en profondeur AES (Advanced Encryption Standard) et DES (Data Encryption Standard), deux des algorithmes de chiffrement symétrique les plus utilisés. AES, notamment, est largement adopté pour sa robustesse et son efficacité dans le cryptage de données sensibles à travers le monde.
ATELIER PRATIQUE :
Les participants auront l'opportunité de mettre en pratique leurs connaissances en implémentant un chiffrement symétrique simple à l'aide de Python ou d'un autre langage de programmation. Cet exercice pratique renforce la compréhension des principes de base du chiffrement symétrique et familiarise les participants avec les techniques de sécurisation des données.

CHIFFREMENT ASYMETRIQUE

ALGORITHMES DE CHIFFREMENT ASYMETRIQUE

FONCTIONNEMENT ET EXEMPLES : RSA, ECC.

Nous plongeons dans le fonctionnement des algorithmes de chiffrement asymétrique tels que RSA (Rivest-Shamir-Adleman) et ECC (Elliptic Curve Cryptography), soulignant leurs différences

fondamentales par rapport au chiffrement symétrique. Ces techniques permettent une sécurité renforcée grâce à l'utilisation de paires de clés publiques et privées, facilitant ainsi l'échange sécurisé d'informations entre les parties.

ATELIER PRATIQUE :

À travers des exercices de génération de paires de clés et de chiffrement/déchiffrement de données avec RSA, les participants acquerront une expérience pratique de l'utilisation des algorithmes de chiffrement asymétrique. Cela leur permettra de comprendre comment ces techniques garantissent la confidentialité et l'authenticité des données dans divers contextes d'application.

FONCTIONS DE HACHAGE

UTILISATION DES FONCTIONS DE HACHAGE

Nous explorons l'application des fonctions de hachage telles que SHA-256 et MD5 dans la sécurité des systèmes informatiques. Ces algorithmes génèrent des empreintes numériques uniques pour les données en entrée, garantissant l'intégrité des informations et facilitant leur vérification contre toute altération malveillante.

ATELIER PRATIQUE :

Les participants seront guidés à travers des exercices pratiques de calcul et de vérification de hachages pour des fichiers et des messages. Cette activité démontre comment les fonctions de hachage jouent un rôle crucial dans la détection des modifications non autorisées et dans la sécurisation des données critiques.

SIGNATURES NUMERIQUES

CONCEPT ET UTILISATION DES SIGNATURES NUMERIQUES

Nous étudions le fonctionnement des signatures numériques, essentielles pour la vérification de l'authenticité des données et la non-répudiation des transactions numériques. Ces mécanismes garantissent que les messages proviennent bien de l'émetteur prétendu et n'ont pas été altérés pendant la transmission, renforçant ainsi la confiance dans les échanges numériques.

ATELIER :

Les participants auront l'occasion de créer et de vérifier des signatures numériques, illustrant concrètement comment ces techniques sont mises en œuvre pour sécuriser les communications et valider l'intégrité des données dans les environnements numériques.

APPLICATIONS PRATIQUES DE LA CRYPTOGRAPHIE

CRYPTOGRAPHIE ET BLOCKCHAIN

Nous analysons comment la cryptographie est intégrée dans les blockchains telles que Bitcoin et Ethereum pour sécuriser les transactions, assurer la confidentialité des données et établir un consensus décentralisé. Ces applications démontrent l'importance cruciale de la cryptographie dans la création de

systèmes numériques sûrs et fiables.

AUTRES APPLICATIONS

Nous examinons également d'autres applications de la cryptographie, telles que la sécurisation des communications via les protocoles TLS/SSL et le stockage sécurisé des données sensibles. Ces technologies jouent un rôle essentiel dans la protection des informations personnelles et commerciales contre les menaces de plus en plus sophistiquées.

SESSION DE CLOTURE : SYNTHESE ET Q&R

RECAPITULATIF DES CONCEPTS ET TECHNIQUES APPRIS

Une synthèse des principaux concepts et techniques enseignés permettra aux participants de consolider leur compréhension de la cryptographie et de ses applications essentielles dans la sécurité informatique moderne.

DISCUSSION SUR L'IMPORTANCE DE LA CRYPTOGRAPHIE

Nous explorerons l'importance croissante de la cryptographie dans le monde numérique moderne, en mettant en évidence ses implications stratégiques et ses défis à venir dans un paysage technologique en constante évolution.

QUESTIONS ET RÉPONSES

Une session interactive de questions-réponses permettra aux participants de clarifier leurs doutes, d'approfondir certains sujets spécifiques et de discuter des applications futures de la cryptographie dans divers secteurs technologiques et industriels.