Cryptographie avancée

3 j (21 heures) Ref : IABC003

Public

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

Pré-requis

Connaissances solides en cryptographie de base
Expérience en programmation (idéalement en Python, C++, ou Java)
Familiarité avec les concepts de la sécurité des systèmes d'information

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 "Cryptographie Avancée" est un programme intensif de trois jours destiné aux professionnels de l'informatique et aux développeurs souhaitant approfondir leurs connaissances en cryptographie. Cette formation couvre des concepts avancés, y compris les algorithmes de cryptographie moderne, la cryptographie à clé publique avancée, les protocoles cryptographiques, et les applications pratiques de la cryptographie dans la sécurité des systèmes et des communications. Les participants apprendront à implémenter et à évaluer des systèmes cryptographiques robustes et à comprendre les dernières tendances et recherches en cryptographie.

Cette formation de trois jours offre une couverture approfondie des concepts avancés en cryptographie, permettant aux participants de maîtriser les techniques et les algorithmes nécessaires pour assurer la sécurité des systèmes et des communications dans un monde de plus en plus numérique.

Objectifs

Maîtriser les algorithmes de cryptographie moderne et leurs applications
Implémenter des protocoles cryptographiques avancés pour la sécurité des systèmes
Comprendre les principes et les techniques de la cryptographie post-quantique
Analyser les systèmes cryptographiques pour détecter et corriger les vulnérabilités

Appliquer la cryptographie avancée dans des contextes variés, y compris la blockchain et les communications sécurisées

Évaluer les recherches récentes et les nouvelles tendances en cryptographie

Programme détaillé

ALGORITHMES ET PROTOCOLES CRYPTOGRAPHIQUES AVANCES

INTRODUCTION AUX ALGORITHMES CRYPTOGRAPHIQUES AVANCES

Dans cette partie, nous approfondissons les concepts de base de la cryptographie en introduisant des techniques avancées telles que la diffusion des blocs, les permutations et les algorithmes modernes. Ces algorithmes sont essentiels pour assurer la sécurité et la confidentialité des données dans divers environnements, y compris les systèmes blockchain.

CRYPTOGRAPHIE SYMETRIQUE AVANCEE

Nous explorons en détail les algorithmes modernes de chiffrement symétrique tels que l'AES (Advanced Encryption Standard) et ChaCha20. Ces algorithmes sont cruciaux pour sécuriser les communications et les données sensibles en utilisant des modes de fonctionnement avancés comme GCM (Galois/Counter Mode) et CCM (Counter with CBC-MAC). L'accent est mis sur les avantages et les cas d'utilisation spécifiques de chaque algorithme, ainsi que sur leur résistance aux attaques modernes.

CRYPTOGRAPHIE ASYMETRIQUE AVANCEE

Nous examinons les optimisations et les considérations de sécurité liées à RSA, un algorithme clé de chiffrement asymétrique largement utilisé. En outre, nous explorons les courbes elliptiques (ECC), y compris les algorithmes ECC et les courbes spécifiques comme P-256 et P-521. L'atelier pratique comprend l'implémentation et l'optimisation de ces algorithmes, ainsi que la comparaison de leurs performances dans différents contextes d'utilisation.

PROTOCOLES ET APPLICATIONS DE CRYPTOGRAPHIE

PROTOCOLES CRYPTOGRAPHIQUES

Nous étudions en détail les protocoles d'échange de clés comme Diffie-Hellman (DH) et ECDH (Elliptic Curve Diffie-Hellman), qui sont essentiels pour établir des communications sécurisées sur des réseaux non sécurisés. De plus, nous explorons les protocoles d'authentification tels que Kerberos et OAuth, en mettant l'accent sur leurs mécanismes de sécurité et leurs applications dans des environnements distribués.

SIGNATURES ET CERTIFICATS

Nous abordons les aspects avancés des signatures numériques avec des algorithmes comme DSA (Digital Signature Algorithm) et ECDSA (Elliptic Curve Digital Signature Algorithm). En outre, nous discutons de l'infrastructure à clé publique (PKI) et de la gestion des certificats, essentielle pour assurer l'authenticité et l'intégrité des transactions numériques.

CRYPTOGRAPHIE POST-QUANTIQUE

Dans cette section émergente, nous introduisons la cryptographie post-quantique, qui se concentre sur le développement d'algorithmes résistants aux attaques quantiques. Nous examinons des algorithmes comme NTRU et McEliece, qui offrent une alternative aux méthodes traditionnelles en anticipant les capacités potentielles des ordinateurs quantiques à briser les systèmes cryptographiques actuels.
ATELIER PRATIQUE
Les participants sont impliqués dans des activités pratiques telles que l'implémentation de protocoles d'échange de clés sécurisés et des tests de résistance aux attaques quantiques sur des systèmes cryptographiques. Cela inclut des exercices visant à évaluer la robustesse des solutions cryptographiques contre les attaques avancées.

ANALYSE, SECURITE ET TENDANCES ACTUELLES

ANALYSE ET ÉVALUATION DE LA SECURITE

Nous explorons les techniques avancées de cryptanalyse telles que l'attaque par canal auxiliaire et l'analyse différentielle, qui sont utilisées pour évaluer la robustesse des algorithmes et des systèmes cryptographiques. L'objectif est de comprendre les failles potentielles et d'améliorer la sécurité des systèmes en conséquence.

SECURITE DES APPLICATIONS ET DES SYSTEMES

Nous examinons l'utilisation de la cryptographie dans divers systèmes sécurisés tels que TLS/SSL, VPN et autres, en mettant l'accent sur la protection des données en transit et au repos. Cette section explore les meilleures pratiques pour sécuriser les applications contre les menaces modernes et les attaques sophistiquées.

NOUVELLES TENDANCES ET RECHERCHES EN CRYPTOGRAPHIE

Nous concluons par l'exploration des dernières tendances en cryptographie, y compris la cryptographie homomorphique pour le calcul sur des données chiffrées et les protocoles de preuve à divulgation nulle de connaissance (zk-SNARKs, zk-STARKs) utilisés dans les blockchains pour garantir la confidentialité tout en vérifiant les transactions. L'atelier final encourage l'analyse critique des systèmes cryptographiques existants et l'implémentation de solutions basées sur les dernières recherches en cryptographie.

SESSION DE CLOTURE : SYNTHESE ET Q&R

La session finale offre un récapitulatif approfondi des concepts et des techniques appris tout au long du programme. Nous discutons de l'importance croissante de la cryptographie avancée dans le renforcement de la sécurité moderne et explorons les perspectives futures pour l'innovation dans ce domaine crucial. Les participants sont invités à poser des questions et à échanger des idées avec les formateurs pour clarifier les concepts et envisager des applications futures des technologies cryptographiques avancées.
