FFCNCERC 2 520 € 3 jour(s)
ERXCS22

[Formation] Cryptographie pour la protection des données

ATELIER RÉALISABLE À DISTANCE AVANCÉ

OBJECTIFS

- Donner une vision globale des enjeux liés à la protection des données
- Identifier les principaux algorithmes de chiffrement à clé secrète et à clé publique
- Maîtriser la mise en œuvre des mécanismes pour offrir les services de confidentialité, d'intégrité et d'authentification
- Expliquer la cryptanalyse et les attaques connues
- Présenter les implications des ordinateurs quantiques et expliquer l'importance de la cryptographie post-quantique

PROGRAMME

Introduction

La Cryptographie

- Principes généraux et vocabulaire
- Cryptographie symétrique, asymétrique
- Fonction de hachage
- La cryptanalyse
- API cryptographique

Atelier : mise en œuvre et benchmark

Chiffrement homomorphe

- Introduction au chiffrement homomorphe
- Avantages et principaux défis
- Utilisation

Atelier : mise en œuvre

Infrastructure de confiance et de sécurité

- Signature digitale
- Certificats numériques
- Infrastructure de gestion de clés publiques (PKI) : Architecture, composants et mise en œuvre

DATES ET LIEUX

Du 03/11/2025 au 05/11/2025 à Paris

PUBLIC / PREREQUIS

Ingénieurs techniques, DSI ainsi que toute personne impliquée dans les systèmes d'information ou souhaitant acquérir des connaissances en cryptographie pour garantir les différents services de sécurité.

Des connaissances générales en mathématiques et en algorithmique sont souhaitables afin de tirer pleinement profit de la formation.

COORDINATEURS

Rida KHATOUN

Enseignant chercheur à Télécom Paris au sein du département Informatique et Réseaux. Ses domaines de recherche actuels comprennent la sécurité du Cloud Computing, la sécurité de l'Internet des objets, la sécurité des réseaux véhiculaires, l'architecture de sécurité, les systèmes de détection d'intrusion et la technologie Blockchain.

Weiqiang WEN

Enseignant chercheur à Telecom Paris dans l'équipe Cybersécurité-Cryptographie. Ses recherches s'intéressent principalement à la cryptographie basée sur les

- Contraintes de déploiement
- Exemples concrets d'applications sécurisées : sécurité des réseaux mobiles GSM/3G/4G, SSL, messagerie sécurisée, vote électronique, paiement EMV, téléprocédures, Big Data, etc.

Atelier : signature et PKI

Cryptographie post-quantique

- Ordinateur quantique et ses implications
- Importance de la cryptographie post-quantique
- Focus sur les candidats finaux du NIST

Synthèse et conclusion

réseaux, et plus particulièrement à la difficulté des problèmes algorithmiques sur les réseaux euclidiens et les réseaux algébriquement structurés.

MODALITES PEDAGOGIQUES

Des exemples et des ateliers illustrent les concepts théoriques.