CRYPTOGRAPHIE POUR LA PROTECTION DES DONNÉES

FFCNCERCERXCS22 | PRIX : 2 550 € | DURÉE : 3 JOURS

Pauses et déjeuners offerts

AVANCÉ | ATELIER | FAISABLE À DISTANCE | RÉALISABLE EN ANGLAIS

CYBERSÉCURITÉ

PRÉSENTATION

La protection des données est un enjeu majeur au cœur des organisations qui, pour l'assurer, doivent mettre en place de nombreuses méthodes issues de la cryptographie.

La formation présente les principaux systèmes cryptographiques indispensables pour la réalisation des services de confidentialité des données, de contrôle d'intégrité et d'authentification.

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
- Utiliser 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
- 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

PUBLIC/PRÉREQUIS

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 cette formation.

RESPONSABLE(S)

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

MODALITÉS PÉDAGOGIQUES

Des exemples et des ateliers illustrent les concepts théoriques.

FORMATIONS INTER-ENTREPRISES