Cryptographie

Acquérir les principes de base de la cryptographie
en abordant les fonctions et les mises en application

Présentation

Cette formation permet de bien comprendre les grands principes de base de la cryptographie appliquée, largement utilisée par les banques, les émetteurs privatifs ainsi que les opérateurs téléphoniques. Elle apporte également une compréhension concrète du domaine

Points forts

- Présentation facilement accessible à des non spécialistes
- Démarche pédagogique à base d'illustrations et d'exemples concrets
- Nombreuses définitions et précisions sur le vocabulaire

Public

Cette formation s'adresse à des personnes nouvellement arrivées dans des services dédiés à la sécurité ou à la gestion des clés. Elle est également adaptée aux professionnels monéticiens ayant à faire des choix de sécurité (protection des données…)

Durée

- 1 journée
- Accueil à partir de 9h
- Formation de 9h30 à 17h30

Prochaines sessions

- 14 mars 2018
- 19 novembre 2018

Formation Intra-entreprise

Nous consulter pour connaître les disponibilités. Le contenu de cette formation, organisée au sein de votre entreprise, peut être adapté à vos objectifs particuliers, après analyse de vos besoins et réalisation d'une proposition détaillée

Animateurs

Experts en systèmes de paiement et cryptographie

Langue

Français

Tarif

Nous consulter

Documentation

Support de cours
Liste des sigles monétiques

Lieu

Région parisienne

Galitt - Centre de formation
SAS au capital de 2 667 744€
TVA FR42 329 822 514
RCS Nanterre B 329 822 514

17 route de la Reine
92100 Boulogne-Billancourt

formation.galitt.com
formation@galitt.com
Tél. : +33 1 77 70 28 00
Fax. : +33 1 77 70 28 23

Cryptographie

Programme

Matin

1. Les notions de base : historique et concepts

- Qu'est-ce que la cryptographie ?
- Principaux besoins couverts par la cryptographie
- Historique de la cryptographie

2. Les algorithmes cryptographiques

- Présentation des principaux algorithmes cryptographiques
  - Symétriques : TDES, EAS
  - Asymétriques : RSA, Diffie-Hellman, Courbes Elliptiques
  - Calcul de Hash : SHA-1

3. Les fonctions cryptographiques

- Description des fonctions cryptographiques les plus utilisées
  - Le chiffrement
  - Le scellement
  - Le hachage
  - La signature numérique
  - L'authentification forte
  - ...

Après-midi

4. La cryptographie appliquée : contraintes et solutions

- Description des solutions opérationnelles pour répondre à différents besoins
  - Echanger des clés de session
  - Dériver des clés d'une même clé maître
  - Certifier des clés publiques
  - Tokeniser une donnée numérique

5. Exemples d'utilisation

- Quelques exemples d'implémentation
  - EMV
  - SSL
  - Contrôle du PIN online
  - Echange de clés sur les automates de retrait
  - Cryptogramme visuel pour le paiement sur Internet
  - Cryptogramme Apple Pay
  - Cryptogramme HCE - Cloud Base Payments

6. Les attaques et parades

- Présentation des différents types d'attaques
  - Attaque par force brute
  - Attaque par cryptanalyse
  - Attaque par collision
  - Attaque par rejeu
- Liste des principales parades aux attaques présentées
  - Algorithmes recommandés
  - Longueur des clés à utiliser

Contenu susceptible d'évoluer