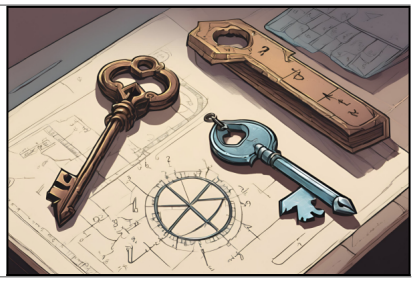
QC3 | Introduction à la cryptographie



Nouvelle Formation

NIVEAU : BASIC

Publics : Professionnels en informatique ou en sécurité informatique souhaitant acquérir des compétences supplémentaires en cryptographie.

Prérequis : Notions en informatique

Responsable(s) pédagogique(s) : Nicolas ARAGON - Maître de Conférences à l'Université de Limoges

Langue de la formation : French

Capacité maximum : 12

Prix : 900€ HT - **Durée :** 1 jour - 7h

Objectifs

- Intégrer les principes fondamentaux de la cryptographie
- Identifier les schémas du chiffrement symétrique, en identifiant les algorithmes courants tels que DES et AES
- Définir les utilisations de la cryptographie asymétrique, que ce soit le chiffrement, la signature numérique ou l'échange de clés
- Déterminer le rôle des certificats numériques et de l'infrastructure à clé publique (PKI)

Dates et lieu des prochaines sessions

- 27 january 2026 au 27 january 2026 - Limoges

Thèmes abordés

Fondamentaux de la cryptographie
Différence entre cryptographie symétrique et asymétrique
Applications de la cryptographie
Fonction de hachage et signature numérique
Implémentation de la cryptographie et attaques side-channel
Certificats et PKI

QC3 | Introduction à la cryptographie

Le programme

Introduction
- Définition de la cryptographie
- Objectifs de la cryptographie en sécurité informatique
- Les trois piliers de la cryptographie : confidentialité, intégrité, authenticité
- Communication cryptographique

Chiffrement Antique
- Le chiffrement de César
- Le chiffrement de Vigenère
- Le chiffrement par substitution

Chiffrement Symétrique
- Principes de base du chiffrement symétrique
- Les algorithmes de chiffrement symétrique (DES, AES)
- Modes de chiffrement (ECB, CBC, GCM)

Cryptographie Asymétrique
- Principes de base de la cryptographie asymétrique
- Échange de clé - Diffie-Hellman
- Les algorithmes de chiffrement asymétrique (RSA, ElGamal)
- Signature numérique

Applications de la Cryptographie
- Les certificats numériques et l'infrastructure à clé publique (PKI)
- Sécurisation des communications (SSL/TLS)
- Protection de la vie privée et anonymat

Méthodologie et évaluation

Questionnaire de positionnement
Exposés et exercices sur ordinateur
Démonstrations interactives
QCM en fin de formation

Formation Continue de l'Institut d'Optique – 2 av. Augustin Fresnel, 91127 Palaiseau. Tél . : +33 1 6453 3236 – fc.institutoptique.fr
PARIS-SACLAY – SAINT-ETIENNE - BORDEAUX