

Cryptographie

Fiche catalogue



— Objectifs pédagogiques :

- └ Assimiler les fonctions propres à la cryptographie (chiffrement, algorithme, etc.)
- └ Appréhender les algorithmes cryptographiques
- └ Recenser les principales attaques et les parades à mettre en oeuvre

— Points forts :

- └ Approche théorique et pratique de l'univers de la cryptographie
- └ Mise en situation avec des exemples concrets
- └ Apport d'un glossaire propre à la cryptographie

— Public : Toute personne souhaitant acquérir les principes de base de la cryptographie en abordant les fonctions et les mises en application

└ **Durée**

└ Présentiel : 1 journée (7h)

└ **Prérequis** : aucune connaissance particulière

└ **Prix** : 1 740 € HT

└ **Nous contacter** :
formation@galitt.com

Cryptographie

Programme

Programme

Les notions de base

- Définition de la cryptographie
- Principaux besoins couverts par la cryptographie
- Historique de la cryptographie

Les algorithmes cryptographiques

- Présentation des principaux algorithmes cryptographiques
- Notions relatives à la cryptographie quantique

Les fonctions cryptographiques

- Description des fonctions cryptographiques (chiffrement, scellement, hachage, signature numérique, authentification forte etc.)

La cryptographie appliquée : contraintes et solutions

- Description des solutions opérationnelles (échange de clés dynamiques ou statiques, etc.)
- Description d'une solution opérationnelle de distribution des clés - RKL TR34 pour la NAC 2020

Exemples d'utilisation

- Exemples d'implémentation (cartes EMV, Cryptogramme Apple Pay, HCE, etc.)

Les attaques et parades

- Présentation de différents types d'attaques (attaque par force brute, par ordinateur quantique, par cryptanalyse, etc.)
- Liste des principales parades aux attaques présentées (algorithmes recommandés, longueur minimale des clés à utiliser)