DIPLÔME

Certificat de spécialisation Cryptographie

Code : CS9600A



Niveau d'entrée : Aucun
Niveau de sortie : Aucun
ECTS : 8

Déployabilité
A la carte : Formation pouvant s'effectuer au rythme de l'élève, en s'inscrivant aux unités du cursus
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)

Objectifs pédagogiques

Science du secret, la cryptologie peut sembler être l'apanage des experts et initiés. Cependant, avec l'essor du numérique, son usage s'est répandu et démocratisé, au point qu'elle est devenue la clé de voûte de la sécurisation des données. En dépit de cette omniprésence, ses concepts sous-jacents restent souvent obscurs, entraînant une utilisation aléatoire ou fantaisiste qui peut s'avérer inadaptée et compromettre ainsi la confidentialité, l'authenticité ou l'intégrité de données personnelles, professionnelles ou étatiques. Face à ces risques, la formation des professionnels aux techniques et usages du chiffrement et de la signature numérique est nécessaire pour assurer une sécurisation efficace et pérenne de l'information et des données. Le certificat que nous proposons entend répondre à ce besoin de formation, en permettant d'acquérir une réelle compréhension des mécanismes inhérents aux protocoles actuels de cryptographie ainsi que les compétences et ressources nécessaires pour mettre à jour ses connaissances dans un domaine en évolution permanente.

Compétences et débouchés

Mesurer les enjeux théoriques, techniques et stratégiques liés à la protection de l'information numérique et connaître le cadre juridique relatif à l'utilisation du chiffrement en France et dans le monde.
Acquérir les bases d'algorithmique ; distinguer les différents types de complexité (algorithme polynomial, sous-exponentiel, exponentiel, ...) et en comprendre les implications pratiques.
Connaître et comprendre les notions de chiffrement par blocs et de chiffrement à flot ; maîtriser les concepts de générateur de nombres pseudo-aléatoires (PRNG) et de fonction de hachage.
Connaître les principaux algorithmes de chiffrement à clé secrète et à clé publique (AES, RSA, El-Gamal, ...), leurs fondements théoriques ainsi que les cryptanalyses et attaques connues. Comprendre les différents modèles d'attaque et les niveaux de sécurité d'un protocole de chiffrement.
Comprendre les schémas de signature numérique et infrastructures à clés publiques (PKI).
Comprendre les implications de l'existence d'un ordinateur quantique sur les protocoles de cryptographie actuels et l'importance de préparer la cryptographie « post-quantique ».
Mettre en œuvre la sécurisation des données : connaître les protocoles et les standards actuels ; savoir mettre à jour ses usages et ses pratiques ; utilisation de logiciels de chiffrement/déchiffrement et de signature.
Appréhender l'utilisation des primitives cryptographiques pour d'autres applications : vote électronique, crypto-monnaies, calcul et stockage distribués (« cloud computing »)...

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

Prérequis et conditions d'accès

Personnels d'entreprise et de la fonction publique, ingénieurs, techniciens spécialisés, chefs de projet, managers, journalistes, étudiants souhaitant se former en cryptologie.
Niveau bac +2 /3

MENTIONS OFFICIELLES

Mots-clés

- mathématiques pour l'informatique
- Technique de télécommunications
- Cryptographie
- Sécurité de l'information

Informations complémentaires

Type de diplôme

Certificat de spécialisation

Code NSF

11 - Mathématiques et sciences

114b - Modèles mathématiques ; informatique mathématique
326 - Informatique, traitement de l'information, réseaux de transmission
326m - Informatique, traitement de l'information

Codes ROME

Développeur / Développeuse de sécurité des systèmes d'information[M1805]
Opérateur / Opératrice en cybersécurité[M1810]
Analyste en cybersécurité[M1805]
Directeur / Directrice des services informatiques -DSI-[M1803]
Architecte de sécurité des systèmes d'information[M1802]
Auditeur / Auditrice en sécurité des systèmes d'information[M1802]
Administrateur / Administratrice de serveurs[M1801]
Administrateur / Administratrice sécurité informatique[M1801]

Formacode

Algorithme [11014]
Mathématiques informatiques [11050]
Sécurité télécommunication [24293]
Système information [31008]
Algèbre [11076]

Code du parcours

CS9600A

URL externe

https://www.cnam.fr/certificat-de-specialisation-cryptographie-1132534.kjsp

Modules d'enseignement

→ Cryptographie

→ Projet personnel tutoré

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.
Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.
Chaque bloc de compétences peut être validé séparément.
Information non disponible, pour plus d'information veuillez contacter le Cnam