

Cryptologie

Connaître et comprendre les aspects théoriques et pratiques de la cryptologie pour la sécurité de l'information.

Intitulé officiel : Certificat de spécialisation Cryptographie

Présentation

Publics / 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

Objectifs

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.

Modalités de validation

Projet tutoré.

Compétences

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 ».

Mis à jour le 12-04-2023



Code : CS9600A

8 crédits

Certificat de spécialisation

Responsabilité nationale :

EPN15 - Stratégies / Julia
PIELTANT

Niveau CEC d'entrée requis :

Sans niveau spécifique

Niveau CEC de sortie : Sans

niveau spécifique

Mode d'accès à la certification :

- Formation continue

NSF : Mathématiques et sciences (11) , Modèles mathématiques ; informatique mathématique (114b) , Informatique, traitement de l'information, réseaux de transmission (326) , Informatique, traitement de l'information (326m)

Métiers (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)

Contact national :

EPN15 - Criminologie Psdr3c
2 rue Camille Guérin
22440 Ploufragan
09 72 31 13 12

psdr3c@Lecnam.net

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 »)...

Enseignements

8 ECTS

Cryptographie

CRM219

4 ECTS

Projet personnel tutoré

UAIP20

4 ECTS