CRM219 - Cryptographie

Mis à jour le 07-04-2025

Code : CRM219

Unité d'enseignement de type cours

4 crédits

Volume horaire de référence (+/- 10%) : **40 heures**

Responsabilité nationale : EPN15 - Stratégies / Alain BAUER

Contact national :

EPN 15 Criminologie

40 rue des jeûneurs
75002 Paris

Hapsa DIA
par_criminomastercnam@lecnam.ne

Présentation

Prérequis

Ce certificat de spécialisation s'adresse :

• aux titulaires d'un diplôme bac +2/3.

• aux personnes justifiant d'un niveau de formation bac +3 dans un domaine compatible avec la spécialité du CS et bénéficiant des procédures de Validation d'Etudes Supérieures, Validation d'Acquis Expériences, VAP85...

L'admission des auditeurs se fait sur dossier candidature, sous réserve d'acceptation par les responsables de la formation.

Objectifs pédagogiques

Ce certificat de spécialisation à pour but de former les auditeurs aux aspects théoriques et pratiques de la cryptologie pour la sécurisation efficace et pérenne de l'information et des données. Il aborde les concepts fondamentaux permettant de comprendre en profondeur les différents principes de chiffrement et déchiffrement, de signature numérique, ainsi que l'aspect technique de leur mise en œuvre.

Plus spécifiquement, ce certificat vise à :

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.

Connaître les différents types de chiffrement ainsi que les principaux algorithmes de chiffrement à clé secrète et à clé publique ; maîtriser les concepts de générateur de nombres pseudo-aléatoires (PRNG), de fonction de hachage, de schémas de signature numérique et d'infrastructures à clés publiques (PKI).

Savoir mettre en œuvre la sécurisation des données en utilisant les protocoles et les standards adaptés ; maîtriser l'usage des logiciels de chiffrement/déchiffrement et de signature.

Appréhender les nouvelles applications des primitives cryptographiques, telles que les crypto-monnaies et le calcul et stockage distribués (« cloud computing »).

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.

Connaître les différents types de chiffrement ainsi que les principaux algorithmes de chiffrement à clé secrète et à clé publique ; maîtriser les concepts de générateur de nombres pseudo-aléatoires (PRNG), de fonction de hachage, de schémas de signature numérique et d'infrastructures à clés publiques (PKI).

Savoir mettre en œuvre la sécurisation des données en utilisant les protocoles et les standards adaptés ; maîtriser l'usage des logiciels de chiffrement/déchiffrement et de signature.

Appréhender les nouvelles applications des primitives cryptographiques, telles que les crypto-monnaies et le calcul et stockage distribués (« cloud computing »).

Programme

Contenu

Présentation historique de la cryptologie.
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.
Introduction à la théorie de l'information de Shannon ; présentation des modèles d'attaque et définition des niveaux de sécurité d'un protocole de chiffrement.
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.
Schémas de signature numérique et infrastructures à clés publiques (PKI).
Exemples d'utilisation de primitives cryptographiques : les crypto-monnaies et le calcul et stockage distribués (« cloud computing »).
Introduction à la cryptographie quantique : échange de clés quantiques.
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.

Modalités de validation

- Projet(s)
- Mémoire

Description des modalités de validation

Mémoire sur projet