CATALOGUE DE FORMATION
30/07/2020

KAÏNA-COM
CATALOGUE DE FORMATION

Cryptographie appliquée et communication sécurisée

Nos locaux
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint

Contact
+33(0)9 50 20 91 64

E-mail
info@kaina-com.fr

Site Internet
www.kaina-com.fr

KSE006 – Cryptographie appliquée et communication sécurisée

Réference	KSE006
Niveau	☒ Débutant ☒ Intermédiaire ☐ Expert
Nombre de jours	Programme de formation : • 16 heures (4 heures/jour)
Lieu de la formation	☐ I: e-learning, Formation individuelle (Formation en ligne) ☒ V: v-learning, classe virtuelle ☐ C: c-learning, cours présentiel **KAÏNA-COM** LE CARRÉ HAUSSMANN II, 6 Allée de la Connaissance 77127 Lieusaint - France
Prérequis	Un niveau d'anglais business moyen est requis car la formation sera dispensée en anglais.
Public	Responsables R&D et ingénieurs logiciels, personnels de sécurité informatique, administrateurs sécurité, tout personnel technique intéressée à comprendre les fondamentaux de la sécurité.

Ce sujet continue à la page suivante

KSE006 – Cryptographie appliquée et communication sécurisée, Suite

Objectifs

Le cours est divisé en une journée de présentation des algorithmes de cryptographie utilisés pour la confidentialité et l'intégrité des données et leur utilisation, et la deuxième journée est consacrée aux protocoles de sécurité qui utilisent ces algorithmes. (Remarque : il existe une option pour un séminaire d'une journée sur les algorithmes de chiffrement).

Ce sujet continue à la page suivante

KSE006 – Cryptographie appliquée et communication sécurisée, Suite

Contenu du cours

Contenu du cours :

Table 1: KSE006 - Contenu du cours

Chapter	Description
Introduction	• Confidentiality, Data-Integrity and Non-repudiation – terminology • Attack types • Information security requirements
Encryption & Confidentiality	• Cryptography Fundamentals – One Time Pad – Brute-Force attacks and key-size • Symmetric and non-symmetric encryption • Symmetric stream ciphers – Algorithms (RC4) • Symmetric block ciphers – AES algorithm • Symmetric block encryption modes – ECB – CBC – CTR • Non-symmetric encryption – DH Algorithm – RSA Algorithm • Hybrid Encryption
Digital Signatures and Data-Integrity	• Crypto hash functions and Message Digest • MAC (Message Authentication Code) – HMAC – CMAC & OMAC • Digital signatures

Ce sujet continue à la page suivante

KSE006 – Cryptographie appliquée et communication sécurisée, Suite

Contenu du cours, Suite

Chapter	Description
Authenticated Encryption & GCM	• Authenticated Encryption & GCM
PKI & Authentication	• Certificates (X.509 and extensions) • Certificate Authority – Trusted Root CA – Intermediate CA • CRL • OCSP (RFC 6960) – OCSP Stapling
SSL and HTTPS	• Perfect forward secrecy • SSL design goals • SSL Record Layer protocol • SSL Handshake • SSL Alert protocols • SSL Cipher suites • SSL Vesions
The End	• Summary • Q&A • Evaluation