

# KAÏNA-COM

## CATALOGUE DE FORMATION

### Cryptographie appliquée et communication sécurisée

---



## KSE006 – Cryptographie appliquée et communication sécurisée

**Référence** 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
<b>Introduction</b>	<ul style="list-style-type: none"> <li>Confidentiality, Data-Integrity and Non-repudiation – terminology</li> <li>Attack types</li> <li>Information security requirements</li> </ul>
<b>Encryption &amp; Confidentiality</b>	<ul style="list-style-type: none"> <li>Cryptography Fundamentals               <ul style="list-style-type: none"> <li>One Time Pad</li> <li>Brute-Force attacks and key-size</li> </ul> </li> <li>Symmetric and non-symmetric encryption</li> <li>Symmetric stream ciphers               <ul style="list-style-type: none"> <li>Algorithms (RC4)</li> </ul> </li> <li>Symmetric block ciphers               <ul style="list-style-type: none"> <li>AES algorithm</li> </ul> </li> <li>Symmetric block encryption modes               <ul style="list-style-type: none"> <li>ECB</li> <li>CBC</li> <li>CTR</li> </ul> </li> <li>Non-symmetric encryption               <ul style="list-style-type: none"> <li>DH Algorithm</li> <li>RSA Algorithm</li> </ul> </li> <li>Hybrid Encryption</li> </ul>
<b>Digital Signatures and Data-Integrity</b>	<ul style="list-style-type: none"> <li>Crypto hash functions and Message Digest</li> <li>MAC (Message Authentication Code)               <ul style="list-style-type: none"> <li>HMAC</li> <li>CMAC &amp; OMAC</li> </ul> </li> <li>Digital signatures</li> </ul>

*Ce sujet continue à la page suivante*



## KSE006 – Cryptographie appliquée et communication sécurisée, Suite

### Contenu du cours, Suite

Chapter	Description
<b>Authenticated Encryption &amp; GCM</b>	<ul style="list-style-type: none"><li>• Authenticated Encryption &amp; GCM</li></ul>
<b>PKI &amp; Authentication</b>	<ul style="list-style-type: none"><li>• Certificates (X.509 and extensions)</li><li>• Certificate Authority<ul style="list-style-type: none"><li>– Trusted Root CA</li><li>– Intermediate CA</li></ul></li><li>• CRL</li><li>• OCSP (RFC 6960)<ul style="list-style-type: none"><li>– OCSP Stapling</li></ul></li></ul>
<b>SSL and HTTPS</b>	<ul style="list-style-type: none"><li>• Perfect forward secrecy</li><li>• SSL design goals</li><li>• SSL Record Layer protocol</li><li>• SSL Handshake</li><li>• SSL Alert protocols</li><li>• SSL Cipher suites</li><li>• SSL Versions</li></ul>
<b>The End</b>	<ul style="list-style-type: none"><li>• Summary</li><li>• Q&amp;A</li><li>• Evaluation</li></ul>

