kaïna-COM ACADEMY

PILAT EUROPE
Leading a new era of human resources

Boost Program

SUMMER EDITION 2020

Cyber Security Package: Enigma

- ✓ Don’t Let the Hackers In
- ✓ Applied Cryptography & Secure Communication

WWW.KAINA-COM.FR

Training Catalogue
02/07/2020

KAÏNA-COM
TRAINING CATALOGUE

Don't Let the Hackers In

KSE003 – Don’t Let the Hackers In

Reference	KSE003
Experience	☒ Beginner ☒ Intermediate ☐ Advanced
Duration	Training Program: • 24 hours (4 hours/day)
Training Method	☐ I: i-learning, individual training (web-based training) ☒ V: v-learning, virtual class ☐ C: c-learning, classroom training **KAÏNA-COM** LE CARRÉ HAUSSMANN II, 6 Allée de la Connaissance 77127 Lieusaint - France
Prerequisite	Understanding computer software and architecture.
Audience	Anyone who needs to learn about anti-hacking techniques.

Continued on next page

KSE003 – Don’t Let the Hackers In, Continued

Objective	Computer and information security is of utmost importance in today’s technological (and political?) environment. The threats imposed by viruses, Trojan horses and other software malware is well known, as is the problem of the hackers – both those programmers who breaks into computer systems because of the challenge imposed and those who break in for criminal or terrorist purposes – to steal, change or destroy information. In this “anti-hacker” course, participants learn about the basic threats hackers pose and what is needed in order to protect computer systems from them.

Continued on next page

KSE003 – Don't Let the Hackers In, Continued

Course Contents

Course Contents :

Table 1: KSE003 - Course Contents

Chapter	Description
Introduction	• What's there to worry about
Organizational Threats	• Users • Host • Server • Perimeter
Defense Methodologies	• Defense in depth • IATF • ISSE • Technology environment defined
Defense Tools	• Users • Host • Server • Perimeter
Security Assessment Demonstration	• Concepts • Tools
The End	• Summary • Q&A • Evaluation

Training Catalogue
02/07/2020

KAÏNA-COM
TRAINING CATALOGUE

Applied Cryptography & Secure Communication

KSE006 – Applied Cryptography & Secure Communication

Reference KSE006

Experience

☒ Beginner
☒ Intermediate
☐ Advanced

Duration

Training Program:

- 16 hours (4hours/day)

Training Method

☐ I: i-learning, individual training (web-based training)

☒ V: v-learning, virtual class

☐ C: c-learning, classroom training

KAÏNA-COM
LE CARRÉ HAUSSMANN II,
6 Allée de la Connaissance
77127 Lieusaint - France

Prerequisite None

Audience

R&D managers and software engineers, IT security staff, security administrators, any technical staff interested in understanding security fundamentals.

Continued on next page

KSE006 – Applied Cryptography & Secure Communication, Continued

Objective	The course is divided to one day of overview on the crypto algorithms used for data confidentiality and data integrity and their usage, and the second day is devoted to security protocols that are using these algorithms. (Note: there is an option for a one-day seminar on encryption algorithms).

Continued on next page

KSE006 – Applied Cryptography & Secure Communication, Continued

Course Contents

Course Contents :

Table 1: KSE006 - Course Contents

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

Continued on next page

KSE006 – Applied Cryptography & Secure Communication, Continued

Course Contents, continued

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 Versions
The End	• Summary • Q&A • Evaluation