Publication date : 02/20/2024

Course : Introduction to cryptography

Practical course - 3d - 21h00 - Ref. CYP
Price : 2470 CHF E.T.

4,2 / 5

This course presents the various cryptographic techniques and their main applications. Symmetric and asymmetric encryption, hashing, the most commonly used algorithms and key management methods will be explained in detail.

Teaching objectives

At the end of the training, the participant will be able to:

- Master the vocabulary associated with cryptology: algorithm, hash, key
- Learn about the algorithms most commonly used in cryptology
- Identify methods for exchanging, managing and certifying public keys
- Use symmetric and asymmetric encryption tools

Intended audience

Security managers, developers, project managers.

Prerequisites

No special knowledge required.

Course schedule

1 Introduction

- History of the first encrypted documents.
- Cryptographic services.
- Mathematical concepts.
- Cryptographic security and attack techniques.

PARTICIPANTS

Security managers, developers, project managers.

PREREQUISITES

No special knowledge required.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

2 Stream Ciphers

- Introducing the concept.
- Linear Feedback Stream Register (LFSR): details of operation, Galois LFSR, applications.
- Other forms of flow encryption: RC4, SEAL.

3 Block ciphers

- Introducing the concept.
- The different forms: Electronic CodeBook (ECB), Cipher-Bloc Chaining (CBC), Cipher FeedBack (CFB)...
- Comparison of flow and block encryption.
- Data Encryption Standard (DES).
- Triple DES (3DES): presentation, operating procedures.
- Advanced Encryption Standard (AES).
- Complementary algorithms: IDEA, RC5, SAFER.

4 Asymmetric encryption

- The RSA algorithm in detail. Security and key size. RSA attacks and challenges. Practical applications.
- ElGamel encryption. ElGamel in DSA.

5 Hash functions

- Concept and objectives.
- Algorithmic principles. Mathematical properties.
- Practical justifications for the various properties.
- Security and hash length.
- Simple (Unkeyed) and secure (Keyed) hashing: block ciphering. MD4 function.
- Advanced attacks on hash functions.
- Technical presentation of hash functions: SHA-1, SHA-256 and SHA-512. MD5. Haval. RIPEMD-128...

6 Integrity and authentication

- Presentation. CBC-MAC standards. HMAC.
- Electronic signature. D.S.A. and R.S.A. signature.

7 Key management

- Key exchange with symmetrical and asymmetrical encryption. Exchange details.
- Diffie-Hellman algorithm. Man-in-the-middle attack.
- Public key management and certification.
- Key revocation, renewal and archiving.
- Certificates in X509 format, PKIX standard.
- Key management infrastructure (PKI).

8 Trusted third parties

- Presentation and standards. Architectures.
- Certification authority. Kerberos.

Dates and locations

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

REMOTE CLASS
2026 : 23 Mar., 27 May, 28 Sep., 23 Nov.