Introduction à la cryptographie

Cours Pratique de 3 jours - 21h
Réf : CYP - Prix 2024 : 2 390CHF HT

Ce stage présente les différentes techniques cryptographiques ainsi que les principales applications. Les chiffrements symétrique et asymétrique, le hachage, les algorithmes les plus utilisés ainsi que les méthodes de gestion des clés seront expliqués en détail.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Maitriser le vocabulaire associé à la cryptologie : algorithme, hachage, clé

Connaitre les algorithmes les plus utilisé en cryptologie

Identifier les méthodes d'échange, gestion et certification des clés publiques

Utiliser des outils de chiffrement symétrique et asymétrique

LE PROGRAMME

dernière mise à jour : 08/2018

1) Introduction

- Histoire des premiers documents chiffrés.
- Services cryptographiques.
- Concepts mathématiques.
- Sécurité cryptographique et techniques d'attaque.

2) Chiffrement de flux (Stream Ciphers)

- Présentation du concept.
- Linear Feedback Stream Register (LFSR) : détails du fonctionnement, Galois LFSR, applications.
- Autres formes de chiffrement par flux : RC4, SEAL.

3) Chiffrement par blocs (Block Ciphers)

- Présentation du concept.
- Les différentes formes : Electronic CodeBook (ECB), Cipher-Bloc Chaining (CBC), Cipher FeedBack (CFB)...
- Comparaison des chiffrements de flux et par blocs.
- Data Encryption Standard (DES).
- Triple DES (3DES) : présentation, modes opératoires.
- Advanced Encryption Standard (AES).
- Algorithmes complémentaires : IDEA, RC5, SAFER.

4) Chiffrement asymétrique

- L'algorithme RSA en détail. Sécurité et taille des clés. Attaques et défi RSA. Applications pratiques.
- Chiffrement ElGamel. ElGamel dans DSA.

5) Fonctions de hachage

- Concept et objectifs.
- Principes algorithmiques. Propriétés mathématiques.
- Justifications pratiques des différentes propriétés.

PARTICIPANTS

Responsables sécurité, développeurs, chefs de projets.

PRÉREQUIS

Aucune connaissance particulière.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Sécurité et longueur du hachage.
- Hachage simple (Unkeyed) et sécurisé (Keyed) : chiffrement par blocs. Fonction MD4.
- Attaques avancées sur les fonctions de hachage.
- Présentation technique des fonctions de hachage : SHA-1, SHA-256 et SHA-512. MD5. Haval. RIPEMD-128...

6) Intégrité et authentification

- Présentation. Standards CBC-MAC. HMAC.
- Signature électronique. Signature D.S.A et R.S.A.

7) Gestion des clés

- Echange de clés avec le chiffrement symétrique et asymétrique. Détail des échanges.
- Algorithme Diffie-Hellman. Attaque de l'homme du milieu.
- Gestion et certification des clés publiques.
- Révocation, renouvellement et archivage des clés.
- Certificats au format X509, norme PKIX.
- L'infrastructure de gestion des clés (IGC/PKI).

8) Tierces parties de confiance

- Présentation et standards. Architectures.
- Autorité de certification. Kerberos.

LES DATES

CLASSE À DISTANCE
2024 : 03 juin, 04 nov.