Formation Introduction à la cryptographie

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	CYP
Durée	3 jours (21h)
Tarif	2 290 €HT
Repas	repas inclus

Objectifs

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

Public

| responsables sécurité
| développeurs
| chefs de projets

Prérequis

| aucune connaissance particulière

Programme de la formation

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

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.

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.

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

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 3 au 5 juin 2024
du 4 au 6 novembre 2024

PARIS
du 27 au 29 mai 2024
du 28 au 30 octobre 2024

LYON
du 3 au 5 juin 2024
du 4 au 6 novembre 2024

VOIR TOUTES LES DATES

Fonctions de hachage
| Concept et objectifs.
| Principes algorithmiques. Propriétés mathématiques.
| Justifications pratiques des différentes propriétés.
| 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...

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

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).

Tierces parties de confiance
| Présentation et standards. Architectures.
| Autorité de certification. Kerberos.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.