Introduction à la cryptographie

-Réference: **PL-76** -Durée: **3 Jours (21 Heures)**

Les objectifs de la formation

- 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

A qui s'adesse cette formation ?

POUR QUI :

- Responsables sécurité, développeurs, chefs de projets.

PRÉREQUIS :

- Aucune connaissance particulière.
- .

Programme

- **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).

Programme

- 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.

- **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.

Programme

- 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.


(+212) 5 22 27 99 01


(+212) 6 60 10 42 56


Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc