Cours 1 :

3 règles en crypto :

* Confidentialité : cacher les informations de ceux qui ne doivent pas les voir
* Integrité : Etre sur qu’elles n’ont pas été modifiées par des inconnus
* message authentification : etre sur de la source

Principe de Kerckhoffs : La sécurité d'un système cryptographique ne doit pas dépendre du secret de l'algorithme de chiffrement lui-même, mais plutôt de la sécurité de la clé utilisée. Cela signifie que l'algorithme de chiffrement peut être rendu public sans compromettre la sécurité, tant que la clé reste secrète.

one TIME PAD :

Le processus de chiffrement consiste à appliquer une opération XOR (ou exclusif) entre chaque bit du message et de la clé. Cette opération génère un texte chiffré qui est théoriquement indéchiffrable sans la connaissance de la clé utilisée.

La principale caractéristique du One-Time Pad est qu'il offre un niveau de sécurité parfait, à condition que la clé soit véritablement aléatoire, utilisée une seule fois et détruite après utilisation.

Block ciphers :

Les chiffrements par blocs sont des algorithmes déterministes qui opèrent sur des groupes de bits de taille fixe, appelés blocs. Ils sont utilisés pour chiffrer des messages de longueur variable en les divisant en blocs de taille spécifiée et en appliquant un processus de chiffrement à chaque bloc individuellement.

Two main techniques

Feistel network or Feistel scheme and substitution-permutation networks (SPN network)

blocks ciphers modes:

ECB

CBC

OFB

CTR

iterated structure

DES Data Encryption Standard

Methodes de chiffrement : DES ou AES

Methodes d’opération : blocks ciphers modes:

ECB

CBC

OFB

CTR

AES venu remplacer DES et prend 128 bits

SPN( substitution – permuation networks) structure qui permet de chiffrer symétriquement.

* substitution : on remplace les elements par d’autres
* puis permutation entre les elements ( bits)
* répetition

Hash function

* Pre- image resistant : Si on a f(x)=y et qu’on nous donne y il doit etre impossible de retrouver x.
* second Pre- image resistant : Si on a f(x)=y il doit etre impossible de trouver un x’ tq f(x’)=y
* collision resistance : difficile de trouver deux entrée x et x’ tq f(x)=f(x’)

Plusieurs fonctions ont été inventées :

* MD5 ( ne respecte pas les propriété)
* SHA-1

Construction de Merkle Damgard : utilise une fonction de compression et produit un h sortant grace a la fonction c et a un xor avec la sortie du c precedent

Messgae Authentification Codes ( MAC) : utilisés pour verifier l’integrité et l’authenticité des messages dans un contexte symétrique. 2 méthodes :

* CBC-MAC : inconvenients :

- clé statiques et donc même clé pour cryptage et authentification

- Vulnérable aux attaques par extension de message si la clé est réutilisée.

- Utilisation d'un vecteur d'initialisation prévisible

* HMAC :

Symmetric les limites :

* l’envoyeur et receveur doivent avoir la même clé, ils ont besoin d’un canal securisé pour la distribution des clés
* impossible d’authentifier plusieurs destinataires simultanément

Diffie- Hellman key exchange 🡪 avec les Kb et kb qui appartiennent au groupe cyclique :

Z = YX [N]

Cryptographie a clé publique = chiffrement asymétrique repose sur trois algo principaux :

* algo de géneration de clés ( K)
* algo de Chiffrement ( E)
* algo de dechiffrement ( D)

Processus de generation de clés RSA :

1. generer p et q premiers
2. calculer N= p\*q et la fonction d’euler φ(N)
3. choisir un entier aléatoire e< φ(N) qui est premier
4. calculer d en faisant (e\*d) ≡ 1 (mod φ(N))

Pour chiffrer un message m à l'aide de RSA avec la clé publique de Billel (N, e), Anissa effectue les opérations suivantes :

* Représenter le message m comme un nombre entier compris entre 0 et N.
* Calculer le chiffre de texte chiffré c = m^e (mod N).
* Envoyer le texte chiffré c à Billel.

Pour déchiffrer le texte chiffré c et récupérer le message original m, Billel utilise sa clé privée (d, p, q) :

* Utiliser la clé privée d pour récupérer m = c^d (mod N).

Une trapdoor function c’est une fonction facile a faire dans un sens mais très compliqué a faire dans la direction opposée