La cryptanalyse

Les concepts fondamentaux

Cryptographie : l'art et la science de garder le secret des messages.

(Secret (crypto) writing (graphy))

Cryptanalyse : l'art de décrypter les messages chiffrés.

(Cryptanalistes = Codebreakers)

Cryptologie : la branche des maths qui traite cryptographie et la cryptanalyse

- **Texte en clair noté (M) : suite de bits : suite de caractères, voix numérisée, image vidéo digitale … échangé ou stocké.**
- **Texte chiffré noté (C) : suite de bits : de même taille que M ou compressé ou plus grande taille**
- **La fonction de chiffrement est notée E (crypter) E(M) = C**
- **La fonction de déchiffrement est notée D (décryptions)**

D(C) = D(E(M)) = M

- **Algorithmes cryptographiques : un algorithme cryptographique est une fonction math avec un algorithme de la fonction inverse pour décrypter utilisée pour effectuer E et D.**

Les Attaques

Il existe 6 types génériques d'attaques cryptanalytiques :

1- L'attaque à texte chiffré seulement :

Le cryptanalyste dispose de Données :

C1=Ek(M1), C2=Ek (M2), …, Ci=Ek (Mi) chiffrés avec même algorithme.

Tâche requise : Retrouver soit les Mi, soit k ou l'algorithme permettant de déduire

Mi+1 de Ci+1

2- L'attaque à texte en clair connu :

Le cryptanalyste dispose en plus des messages chiffrés leurs textes en clair correspondants Données :

M1 , C1=Ek (M1), M2 , C2=Ek

(M2), …, Mi , Ci=Ek (Mi)

Tâche requise : Retrouver soit k soit l'algorithme permettant de déduire

Mi+1 de Ci+1

3- L'attaque à texte en clair choisi (statique):

En plus des textes chiffrés et en clair, le cryptanalyste dispose aussi l'accès aux choix de textes en clair à chiffrer Données :

M1 , C1=Ek (M1),

M2 , C2=Ek (M2), …,

Mi , Ci=Ek (Mi) où le cryptanalyste choisit M1,M2 , …, Mi

Tâche requise : Retrouver soit k soit l'algorithme permettant de déduire

Mi+1 de nCi+1 =Ek (Mi)

4- L'attaque à texte en clair chois adaptative (dynamique) :

Ce cas particulier de l'attaque 3, le cryptanalyste peut non seulement choisir les textes en clair mais il peut aussi adapter ses choix en fonction des textes chiffrés précédents.

Pour l'attaque 3, le cryptanalyste est autorisé à choisir un grand bloc de texte en clair au départ

Pour l'attaque 4, il choisit un bloc plus petit et en fonction du résultat il choisira un autre bloc…

5- L'attaque à texte chiffré choisi :

Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer.

Les textes déchiffrés lui seront alors fournis Données :

C1 , M1=Dk (C1),

C2 , M2=Dk (C2), …,

Ci , Mi=Dk (Ci)

Tâche requise : Retrouver k

Très utilisée aux cryptosystèmes à clé publique

6- L'attaque à clé choisie

Attaque + avoir la clé ?!

ce n'est pas très pratique