Date: Mercredi 26 avril 2006 à 18:45:47
Sujet: 7 Cryptographie

La cryptographie DES (Data Encryption Standard)

La cryptographie ou la steganographie consiste à cacher quelque chose à quelqu'un, par exemple un message en le modifiant de manière à ce que seul une personne conaissant le moyen de le faire puisse le ramenner à son état d'origine. Le D.E.S. (Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données) est un standard mondial depuis plus de 20 ans. Bien qu'il soit un peu vieillissant, il résiste toujours très bien à la cryptanalyse et reste un algorithme très sûr.

Au début des années 70, le développement des communications entre ordinateurs a nécessité la mise en place d'un standard de chiffrement de données pour limiter la prolifération d'algorithmes différents ne pouvant pas communiquer entre eux. Pour résoudre ce problème, L'Agence Nationale de Sécurité américaine (N.S.A.) a lancé des appels d'offres.La société I.B.M. a développé alors un algorithme nommé Lucifer, relativement complexe et sophistiqué. Après quelques années de discussions et de modifications, cet algorithme, devenu alors D.E.S., fut adopté au niveau fédéral le 23 novembre 1976. Le D.E.S. est un système de chiffrement par blocs. Cela signifie que D.E.S. ne chiffre pas les données à la volée quand les caractères arrivent, mais il découpe virtuellement le texte clair en blocs de 64 bits qu'il code séparément, puis qu'il concatène. Un bloc de 64 bits du texte clair entre par un coté de l'algorithme et un bloc de 64 bits de texte chiffré sort de l'autre coté. L'algorithme est assez simple puisqu'il ne combine en fait que des permutations et des substitutions. On parle en cryptologie de techniques de confusion et de diffusion. C'est un algorithme de cryptage à clef secrète. La clef sert donc à la fois à crypter et à décrypter le message. Cette clef a ici une longueur de 64 bits, c'est-à-dire 8 caractères, mais seulement 56 bits sont utilisés. On peut donc éventuellement imaginer un programme testant l'intégrité de la clef en exploitant ces bits inutilisés comme bits de contrôle de parité. L'entière sécurité de l'algorithme repose sur les clefs puisque l'algorithme est parfaitement connu de tous. La clef de 64 bits est utilisée pour générer 16 autres clefs de 48 bits chacune qu'on utilisera lors de chacune des 16 itérations du D.E.S.. Ces clefs sont les mêmes quel que soit le bloc qu'on code dans un message. En effet la sécurité du D.E.S. avec ses 16 rondes est grande et résiste à l'heure actuelle à toutes les attaques linéaires, différentielles ou par clefs corrélées, effectuées avec des moyens financiers et temporels raisonnables (i.e. moins de 10 millions de dollars et moins d'un mois). La grande sécurité repose sur ses tables de substitutions non linéaires très efficaces pour diluer les informations. De plus le nombre de clefs est élevé (256=7,2*1016) et peut être facilement augmenté en changeant le nombre de bits pris en compte. D'autres avantages plus techniques au niveau cryptanalyse existent. De plus, cet algorithme est relativement facile à réaliser matériellement et certaines puces chiffrent jusqu'à 1 Go de données par seconde ce qui est énorme :

c'est plus que ce qu'est capable de lire un disque dur normal. Pour les industriels c'est un point important notamment face à R.S.A.

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
http://www.zmaster.fr

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=180