DES

DES signifie Digital Encryption Standard et a été créé en 1975 avec l'aide de la National Security Agency (NSA). En 1981, DES est devenu une norme acceptée et a été largement utilisé. DES est un chiffrement par bloc qui utilise une clé de 56 bits pour créer la table de clés. Ensuite, il passe par le processus de combinaison d'une clé de la table de clés avec le bloc de texte en clair. Une fois la clé et le texte en clair combinés, DES subit 16 modifications supplémentaires (appelées rondes) pour mélanger complètement le texte chiffré. Pour déchiffrer les données, DES passe simplement par tous les changements dans l'ordre inverse.

Étant donné qu'une clé de 56 bits contient environ 72 quadrillions de combinaisons de nombres différentes, la plupart des gens pensaient que DES serait sécurisé pendant très longtemps.

Ce que les gens n'ont pas pris en compte, c'est que les ordinateurs sont devenus plus rapides et moins chers et qu'il ne coûterait pas très cher de créer un ordinateur spécifiquement pour casser DES. En 1999, DES a été cassé en moins de 24 heures sur un ordinateur spécialement construit.

Triple DES De nombreuses années avant que DES ne soit cassé, les cryptographes ont commencé à travailler sur son remplacement. Ce n'était pas que DES était gravement défectueux; c'était que la communauté crypto pouvait voir la fin venir et ils voulaient être préparés. Ainsi, Triple DES (également appelé 3DES) a été créé. Étant donné que de nombreux logiciels et matériels étaient déjà codés avec DES, il était logique d'apporter des modifications à un algorithme déjà utilisé, plutôt que d'en créer un entièrement nouveau. De cette manière, de nombreux produits plus anciens ont pu être mis à niveau vers 3DES (ou une variante très similaire) sans avoir à reconstruire complètement le matériel ou le logiciel.

Comme son nom l'indique, Triple DES fait quelque chose de trois fois plus que le DES normal. Cette triple menace provient de l'utilisation de trois clés sur chaque bloc de texte en clair. Au lieu d'utiliser une clé 56 bits de la table de clés, Triple DES crypte le texte en clair avec la première clé, crypte ce texte chiffré avec une autre clé 56 bits, puis crypte le texte chiffré avec une autre clé 56 bits.

Cela peut sembler exagéré, mais cela fonctionne. 3DES est également capable de travailler avec des clés plus longues pour le rendre plus sécurisé. Les longueurs de clé les plus généralement plus longues (actuellement) sont de 112 bits et 168 bits.

Pour déchiffrer cet algorithme, vous auriez besoin de trouver trois clés distinctes. Non seulement cela, mais le texte chiffré ne sera déchiffré que lorsque les trois clés correctes seront utilisées et dans le bon ordre. Il est peut-être possible de deviner une clé, mais vous ne saurez jamais si elle est correcte tant que vous ne l'avez pas combinée avec les deux autres clés. Le nombre de permutations est scandaleusement élevé et personne ne veut passer autant de temps à attaquer quelque chose de valeur inconnue. Et si vous vous donniez la peine de trouver les trois clés, dans le bon ordre, pour découvrir que les données étaient un e-mail rappelant à tout le monde qu'il reste du gâteau d'anniversaire dans la zone de pause ? Beaucoup d'efforts dépensés pour rien, je dirais

IDEA IDEA signifie International Data Encryption Algorithm, et il est le plus souvent considéré comme un composant de PGP (Pretty Good Privacy, un programme de cryptage de courrier électronique populaire). Cet algorithme commence avec une clé de 128 bits. Il décompose ensuite la clé de 128 bits en un total de 56 sous-clés. Pour ce faire, il divise la clé d'origine en huit clés de 16 bits. Ensuite, les bits de la clé originale de 128 bits sont décalés de 25 bits vers la gauche (un peu comme tout le monde dans un stade de baseball se déplaçant de plus de 25 sièges vers la gauche). Maintenant que la clé d'origine a été décalée et refaite, elle est à nouveau découpée en huit clés de 16 bits. Vous continuez à déplacer et à découper jusqu'à ce que vous ayez un total de 52 touches, chacune d'elles de 16 bits.

Croyez-le ou non, avec toutes ces commutations et coupures, l'algorithme IDEA est traité environ trois fois plus vite que DES. L'une des raisons pour lesquelles il est utilisé est qu'il ne crée pas autant de charge sur le processeur de l'ordinateur. Mais,

comme IDEA est plus récent que DES et 3DES, il n'a pas vraiment été accepté comme standard. Il a été analysé par les militaires, mais ils ne disent pas ce qu'ils ont trouvé. S'il y a des faiblesses dans IDEA, aucun expert extérieur au gouvernement ne les a trouvées - pour le moment.

AES AES signifie Advanced Encryption Standard. Beaucoup s'attendent à ce que cet algorithme soit l'héritier apparent de DES et 3DES. C'est le premier algorithme qui a été créé grâce à une compétition organisée.

Le concours a été annoncé par le NIST (National Institute of Standards and Technology) en 1997 dans le but de trouver un bon algorithme qui deviendrait la prochaine norme gouvernementale. En 1998, la liste des algorithmes concurrents avait été réduite à 15 candidats. Ensuite, les tests intensifs ont commencé. Les concurrents ont commencé à tomber comme des mouches car des faiblesses ont été trouvées dans la plupart des algorithmes à l'étude. En 1999, le casting de joueurs avait été réduit à seulement cinq et une autre série de tests a commencé.

Fin 2000, le NIST a annoncé qu'il avait un gagnant - un algorithme appelé Rijndael (d'après Vincent Rijmen et Joan Daemen, prononcé rine-doll). Il avait survécu à tous les tests et les gens aimaient généralement la façon dont il fonctionnait. Le gouvernement l'a appelé leur Advanced Encryption Standard (AES), mais ce n'est pas encore tout à fait la norme dans le monde réel. Encore une fois, parce que c'est relativement nouveau,

il y a une certaine méfiance et un sentiment qu'il n'a pas été suffisamment testé pour ses faiblesses. Quoi qu'il en soit, il existe des produits sur le marché qui utilisent ouvertement AES et continueront de le faire jusqu'à ce qu'il soit prouvé qu'il est faible ou cassable.