

Longueur minimale des clefs de chiffrement symétriques afin d'assurer une sécurité commerciale suffisante

Un rapport par un groupe ad hoc de cryptographes
et de scientifiques informatiques

Matt Blaze¹
Whitfield Diffie²
Ronald L. Rivest³
Bruce Schneier⁴
Tsutomu Shimomura⁵
Eric Thomson⁶
Michael Wiener⁷

Janvier 1996

INTRODUCTION

Le chiffrement joue un rôle essentiel dans la protection des informations électroniques contre les menaces d'une variété d'attaquants potentiels. Dans ce dessein, la cryptographie moderne utilise une combinaison de cryptographie *conventionnelle* ou *symétrique* afin de chiffrer les données et des systèmes à *clé publique* ou *asymétriques* pour gérer les *clefs* utilisées par les systèmes symétriques. S'assurer de la force requise par les systèmes cryptographiques symétriques est donc une étape essentielle dans l'utilisation de la cryptographie sur ordinateur et pour la sécurité des communications.

La technologie actuellement disponible (fin 1995) rend les attaques par *force-brute* contre les systèmes cryptographiques rapides et bon marché depuis quelques années. Des ordinateurs à usage général peuvent être utilisés, mais une approche plus efficace est d'utiliser la technologie commercialement disponible des *Field Programmable Gate Array (FPGA)*. Pour des attaquants préparés à réaliser un investissement initial plus important, ces puces fabriquées spécialement et adaptées à réaliser ces calculs de manière rapide amortissent le coût à l'usage.

Ainsi, les cryptosystèmes avec des clefs de 40 bits n'offrent virtuellement aucune protection actuellement contre des attaques de force-brute. Même le standard de chiffrement fédéral américain, le DES, avec ses 56 bits de clefs devient de moins en moins adapté. À mesure que les cryptosystèmes succombent à des attaques "intelligentes" plutôt que la force-brute, il faut se souvenir que les clefs discutées dans ce document sont un minimum contre les menaces de calcul considérées.

Heureusement, le coût du chiffrement fort n'est pas plus important que celui du chiffrement faible. Ainsi, pour avoir une sécurité adaptée à la plupart des menaces sérieuses, des entreprises commerciales aux fonds importants ou des agences de surveillance gouvernementales, les clefs à utiliser pour protéger aujourd'hui les données

¹ AT&T Research, mab@research.att.com

² Sun Microsystems, diffie@eng.sun.com

³ MIT Laboratory for Computer Science, rivest@lcs.mit.edu

⁴ Counterpane Systems, schneier@counterpane.com

⁵ San Diego Supercomputer Center, tsutomu@sdsc.edu

⁶ Access Data, Inc., eric@accessdata.com

⁷ Bell Northern Research, wiener@bnr.ca

doivent comporter au minimum 76 bits. Pour protéger l'information pendant les vingt prochaines années, en estimant les avancées prévisibles de la puissance de calcul informatique, les clefs déployées devront comporter au minimum 90 bits.

1 Le chiffrement joue un rôle essentiel dans la protection de l'information électronique

1.1 Il y a un besoin de sécurité pour l'information

À l'heure où nous rédigeons ce document fin 1995, le développement du commerce électronique et de l'infrastructure globale d'Internet est à un point critique. Les chemins boueux du Moyen Âge ne sont devenus des voies de commerce et de culture que lorsque la sécurité des voyageurs et des biens fut assurée. Il en est de même pour les autoroutes de l'information qui ne seront que des chemins dangereux tant que l'information, le bien de l'âge de l'information, ne pourra être déplacée, conservée, vendue et achetée que de manière sûre. Ni les entreprises commerciales ni les individus ne peuvent réaliser leurs affaires commerciales ou traiter leurs données personnelles au travers de réseaux informatiques sans être assurés de la sécurité des informations.

Aujourd'hui, la plupart des formes de communication peuvent être conservées et traitées de manière électronique. Ceci signifie une grande variété d'information, des valeurs économiques aux aspects privés ainsi qu'une grande variation dans la durée de temps pendant laquelle l'information a besoin d'être protégée sur les réseaux informatiques.

Considérez le spectre suivant :

- les transferts de fonds électroniques représentent des millions ou des milliards de dollars, dont la sécurité à court terme est essentielle, mais dont l'exposition est très courte ;
- les plans stratégiques d'une société commerciale, dont la confidentialité doit être préservée pour un petit nombre d'années ;
- un produit propriétaire (la formule du Coca-Cola, un nouveau médicament) qui doit être protégé pendant toute sa durée de vie utile, souvent des dizaines d'années ;
- l'information privée, propre à un individu (état médical, évaluation d'emploi) qui doit être protégée pendant toute la durée de vie de l'individu.

1.2 Le chiffrement peut fournir une forte protection de la confidentialité

Le chiffrement est obtenu en brouillant les données avec des procédures mathématiques qui rendent la récupération du *texte clair* extrêmement difficile et longue à toute personne autre que les destinataires autorisés, ceux qui disposent des *clefs* de déchiffrement correctes. Un chiffrement correct garanti que l'information restera protégée, même si elle tombe en de mauvaises mains.

Le chiffrement – et le déchiffrement – peuvent être réalisés par logiciel informatique ou matériel dédié. Une approche classique est d'écrire l'algorithme sur un disque afin qu'il soit exécuté par un processeur central ; le placer en ROM ou PROM pour une exécution par un microprocesseur ; isoler le stockage et l'exécution dans une carte pour ordinateur (une carte intelligente ou une carte PCMCIA).

Le degré de protection obtenu dépend de plusieurs facteurs. Ils incluent: la qualité du cryptosystème ; la manière dont il est implémenté en logiciel ou matériel (en particulier sa

fiabilité et la manière dont les clefs sont choisies) et le nombre total de clefs possibles qui permettent de chiffrer l'information. Un algorithme cryptographique est considéré fort si :

1. Il n'y a aucun raccourci qui permet à un adversaire de récupérer le texte clair sans utiliser la force-brute qui consiste à tester chaque clef possible jusqu'à trouver la bonne;
2. Le nombre de clefs possibles est suffisamment grand pour rendre ce type d'attaque irréalisable.

Le principe est ici semblable au verrou d'un coffre. Si le verrou est bien conçu afin que le voleur ne puisse entendre le cliquetis de son mécanisme, une personne qui ne connaît pas la combinaison ne pourra l'ouvrir qu'en essayant chaque combinaison possible, jusqu'à ce qu'il trouve celle qui ouvre le verrou.

Les tailles des clefs de chiffrement sont mesurées en bits et la difficulté à essayer toutes les clefs possibles croît de manière exponentielle avec le nombre de bits utilisés. Ajouter un bit à la clef double le nombre de clefs possibles ; ajouter dix bits augmente le facteur de plus d'un millier.

Il n'y a aucun moyen définitif de regarder un chiffrement et de déterminer si un raccourci existe. Quoi qu'il en soit, plusieurs algorithmes de chiffrement – en particulier le standard de chiffrement fédéral américain (DES) – ont été étudiés en profondeur dans la littérature publique et sont considérés comme de grande qualité. Un élément essentiel de la conception d'un algorithme cryptographique est la longueur de la clef, dont la taille place la limite supérieure de la force du système.

Tout au long de ce document, nous assumerons qu'il n'y a pas de raccourcis et traiterons la longueur de la clef comme représentative du *facteur de travail* du cryptosystème – il s'agit de la quantité minimale de travail à réaliser pour briser le système. Il est important de garder à l'esprit, toutefois, que les cryptographes considèrent cette hypothèse comme brutale et beaucoup recommanderont des tailles de clefs deux fois plus grandes (voire plus encore) afin de résister aux attaques de force-brute, bien que des clefs plus longues demandent plus de travail pour chiffrer et déchiffrer. Un bon exemple de cette approche répandue est l'utilisation du *triple-DES*: le produit du chiffrement d'un DES est chiffré deux fois de suite, en utilisant au total trois clefs différentes.

Les systèmes de chiffrement sont classés en deux catégories. Les cryptosystèmes conventionnels ou symétriques – où celui qui dispose de la capacité de chiffrement dispose aussi de celle du déchiffrement – sont ceux qui sont considérés dans ce document. Les cryptosystèmes plus récents à clef publique ou asymétriques ont pour propriété que la clef de chiffrement ne permet pas de déchiffrer : une seconde clef, de déchiffrement, permet le déchiffrement. Dans la cryptographie contemporaine, les systèmes à clef publique sont indispensables pour gérer les clefs des cryptosystèmes conventionnels. Tous les cryptosystèmes à clef publique sont toutefois sujets à des attaques par raccourcis et doivent donc utiliser des tailles de clefs dix fois plus grandes (et souvent plus) que les clefs qui sont ici discutées afin d'obtenir une sécurité satisfaisante.

Bien que les ordinateurs permettent à l'information électronique d'être chiffrée en utilisant de très grandes clefs, les avancées en capacité de calcul des ordinateurs repoussent sans cesse les tailles de clefs qui peuvent être considérées comme grandes et rendent aussi plus facile et bon marché les attaques des informations chiffrées.

1.3 Des menaces provenant d'une variété d'attaquants potentiels

Les menaces sur la confidentialité des informations vient de plusieurs directions et leur forme dépend des ressources des attaquants. Les *hackers* qui peuvent être des étudiants de

grandes écoles comme des programmeurs commerciaux ont souvent accès à des ordinateurs de grande puissance ou des réseaux d'ordinateurs. Ces mêmes personnes peuvent déjà disposer d'étagères peu chères et "maison" contenant des puces *Field Programmable Gate Array (FPGA)* qui fonctionnent comme du "matériel programmable" et qui augmentent radicalement l'efficacité d'un effort cryptanalytique. Une petite compagnie ou même un individu fortuné peuvent s'offrir un grand nombre de ces puces. Une entreprise commerciale de grande taille ou une organisation de crime organisé avec de "l'argent sérieux" à dépenser peuvent acquérir des puces spécialisées et conçues à fins de décryptage. Un service secret, qui consacre une partie de ses efforts à l'espionnage à fins de supériorité économique de son pays, peut disposer d'une machine comportant des millions de ces puces...

1.4 La technologie actuelle rend le coût du chiffrement fort identique à celui du chiffrement faible

L'une des propriétés du chiffrement par ordinateur est qu'une augmentation modeste du coût de la machine permet de disposer d'une grande augmentation de sécurité. Pour chiffrer de l'information de manière très sûre (e.g. avec des clefs de 128 bits) ne demande pas tellement plus de temps de calcul qu'un chiffrement faible (e.g. avec des clefs de 40 bits). Dans beaucoup d'applications, la cryptographie ne compte en soit que pour une faible part du coût de calcul : la majeure partie est consacrée au traitement d'informations comme la voix ou la compression d'image, qui doivent être préparées avant un chiffrement.

Une conséquence de cette uniformité des coûts est qu'il n'y a plus tellement besoin d'adapter la force de la cryptographie en fonction de la sensibilité de l'information à protéger. Même si la plupart des informations dans un système n'ont pas d'implications privées ni de valeur monétaire, il n'y a aucune raison pratique ou économique de concevoir des ordinateurs ou des logiciels qui proposent différents niveaux de sécurité dans le chiffrement : le chiffrement le plus fort doit toujours être utilisé quelle que soit l'information à conserver ou à transmettre au sein d'un système.

2 La technologie actuellement disponible rend le décryptage par force-brute rapide et bon marché

Le type de matériel utilisé pour réaliser une attaque de force-brute contre un algorithme de chiffrement dépend de l'envergure de l'opération cryptanalytique et de la quantité de fonds disponibles à l'attaquant. Dans l'analyse qui suit, nous considérons les grands types de technologie qui peuvent être actuellement utilisés par des attaquants, en fonction des ressources dont ils peuvent disposer. Et il n'est pas étonnant de constater que les technologies cryptanalytiques qui demandent les investissements initiaux les plus importants sont aussi celles qui à l'usage (pour chaque clef récupérée) sont les plus rentables, ce qui permet d'amortir le coût sur la durée de vie du matériel.

L'une des propriétés essentielles des attaques de force-brute est la possibilité de les paralléliser de manière infinie. Il est possible d'utiliser autant de machines que disponibles, et d'assigner à chacune une partie distincte du problème. Ainsi, quelle que soit la technologie employée, le temps de recherche peut être réduit en ajoutant plus d'équipements; deux fois plus de matériel permet d'espérer trouver la clef en deux fois moins de temps. L'investissement total aura été doublé, mais si le matériel est utilisé en permanence pour rechercher des clefs, le coût par clef récupérée n'augmente pas.

En bas du spectre technologique disponible se trouvent les ordinateurs personnels ou les stations de travail programmées pour tester des clefs. La plupart, par fait de nécessité ou

disposant d'accès à des machines, sont en position d'utiliser ces ressources à coût réduit voire gratuitement. Toutefois, les ordinateurs à usage général – qui sont fournis avec des équipements auxiliaires comme des contrôleurs vidéo, des claviers, interfaces, mémoire et disques dur – font des machines de recherche très chères. Ils ne seront donc utilisés que de manière occasionnelle par des attaquants qui ne souhaitent pas ou ne peuvent pas investir dans un équipement plus spécialisé.

Une approche technologique plus efficace est d'utiliser les *Field Programmable Gate Array (FPGA)* commercialement disponibles. Les FPGA fonctionnent comme du matériel programmable et permettent des implémentations plus rapides de tâches, comme le chiffrement et le déchiffrement et les réalisent plus rapidement que les processeurs conventionnels. Les FPGA sont très utilisés comme outils simples de calculs devant être réalisés très rapidement, en particulier la simulation des circuits intégrés dans leur phase de développement.

La technologie FPGA est rapide et bon marché. Le coût d'une puce ORCA d'AT&T qui peut tester 30 millions de clefs DES par seconde est de 200 dollars. C'est 1 000 fois plus rapide qu'un PC, ou un dixième du prix ! Les FPGA sont disponibles partout et montés sur des cartes, ces puces peuvent être installées dans un PC standard comme une carte son, un modem ou de la mémoire supplémentaire.

La technologie FPGA peut être optimisée lorsqu'un même outil doit être utilisé pour attaquer une variété de cryptosystèmes différents. Souvent, comme avec le DES, un cryptosystème est suffisamment répandu pour justifier la construction d'une ou plusieurs installations spécialisées. Dans ces circonstances, la technologie au meilleur rapport prix-efficacité mais qui demandent aussi le plus grand investissement initial, sont l'utilisation des circuits intégrés à applications spécifiques: *Application-Specific Integrated Circuits (ASICs)*. Une puce de 10 dollars peut tester 200 millions de clefs par seconde. C'est sept fois plus rapide qu'une puce FPGA pour un vingtième du coût.

Mais parce que les ASICs demandent un investissement plus important que les FPGA et qu'elles doivent être fabriquées en grande quantité pour les rendre économiques, cette approche ne sera envisagée que pour des opérations sérieuses et disposants de fonds importants, comme les entreprises commerciales (ou criminelles) ou les services secrets des gouvernements.

3 Les clefs de 40 bits n'offrent virtuellement aucune protection

La politique du gouvernement américain consiste à limiter l'exportation des logiciels qui incorporent un chiffrement, et n'autorise que les algorithmes RC2 et RC4 avec des clefs de 40 bits. Une clé de 40 bits de longueur signifie qu'il y a 2^{40} clefs possibles. En moyenne, la moitié de ces clefs (2^{39}) devront être essayées pour trouver la bonne. L'exportation d'autres algorithmes et d'autres clefs doivent être approuvés au cas par cas. Par exemple, les DES avec une clé de 56 bits a été approuvé pour certaines applications comme les transactions financières.

L'attaque récente et réussie par deux étudiants français sur l'algorithme RC4 de Netscape ont démontré les dangers de clefs trop courtes. Ces étudiants de l'École Polytechnique de Paris ont utilisé le "temps inutilisé" des ordinateurs de leur école, donc sans le moindre coût pour personne : ni eux, ni leur école. Même avec des ressources aussi limitées, ils ont été capables de récupérer la clé de 40 bits en quelques jours seulement.

Il n'y a pas besoin d'avoir les ressources d'une institution comme les grandes écoles, toutefois. N'importe qui avec un peu d'expertise en informatique et quelques centaines de

dollars peut attaquer le chiffrement 40 bits bien plus vite. Une puce FPGA, pour environ 400 dollars montée sur une carte, cassera une clé de 40 bits en cinq heures. En assumant que la puce FPGA est utilisée pendant au moins trois ans pour trouver des clés, le coût moyen pour trouver une clé est de 8 cents.

Un prédateur commercial plus déterminé, préparé à dépenser 10 000 dollars pour un ensemble de 25 puces ORCA, peut trouver toute clé de 40 bits en 12 minutes, toujours avec un coût de revient de 8 cents par clé. Dépenser encore plus d'argent sur les puces permet de réduire le temps : 300 000 dollars permet d'obtenir une clé toute les 24 secondes, et un investissement de 10 000 000 dollars permet de trouver toute clé en 0,7 secondes.

Comme nous l'avons déjà indiqué, une entreprise commerciale disposant d'assez de ressources peut concevoir et faire fabriquer des puces personnalisées, bien plus rapides. Ainsi, en dépensant 300 000 dollars, une compagnie peut être capable de casser toute clé de 40 bits en 0,18 secondes à 0,1 cent la clé par solution ; une compagnie encore plus grande ou une agence gouvernementale acceptera de dépenser 10 000 000 pour trouver la même clé en 0,005 secondes (toujours à 0,1 cent la clé). Le coût par solution reste constant car nous avons tout le temps assumé que le prix par puce reste constant ; en réalité, plus on achète de puces, et plus le prix par puce se réduit).

Ces résultats sont résumés dans la table I.

4 Même le DES avec ses clefs de 56 bits est de plus en plus inadapté

4.1 Le DES n'est pas la panacée aujourd'hui

Le standard de chiffrement fédéral (DES) a été développé en 1970 par IBM et la NSA, adopté par le gouvernement américain comme standard fédéral de traitement de l'information à fins de chiffrement des données. Il a été prévu pour fournir un chiffrement fort pour les informations sensibles mais non-classifiées du gouvernement. Il a été reconnu par beaucoup que, même lorsque le DES fut développé, les développements technologiques à venir rendraient le DES à clefs de 56 bits très vulnérable avant la fin du siècle.

Aujourd'hui, le DES est probablement le chiffrement le plus répandu, et il continue à être cité dans beaucoup de comparaisons. Malgré cela, le DES et les équivalents ne sont pas la panacée. Les calculs montrent que désormais le DES est incapable de résister à une entreprise commerciale ou à un gouvernement qui disposent de bonnes ressources. En fait, la réalité est que le DES est devenu tellement facile et peu cher à briser...

Comme nous l'avons expliqué ci-dessus, le chiffrement à 40 bits ne fournit qu'une protection faible même contre un attaquant occasionnel, qui dispose du temps libre de quelques machines et de quelques centaines de dollars à dépenser. Contre de tels opposants, utiliser DES avec des clefs de 56 bits ne donne qu'une protection substantielle. Actuellement, il faudrait environ un an et demi à quelqu'un disposant de 10 000 dollars de puces FPGA pour trouver une clé DES. Dans dix ans, un tel investissement permettra de trouver une clé DES en moins d'une semaine.

La menace réelle aux transactions commerciales et à l'aspect privé d'Internet vient plus de particuliers et d'organisations prêtes à investir assez d'argent et de temps. À mesure que de plus en plus de commerces et qu'une plus grande part d'information personnelle passe dans le monde électronique, les bénéfices que l'on peut tirer augmentent et l'investissement non seulement se justifie, mais serait rentable.

Un effort sérieux, de l'ordre de 300 000 dollars, par un commerce légitime ou illégal, permet de trouver une clef DES avec une moyenne de 19 jours avec la technologie en vente actuellement, et en trois heures avec des puces développées à cette fin. Dans ce dernier cas, le coût par clef reviendrait à 38 dollars (en assumant une durée de vie de trois ans à la puce et une utilisation continue). Une entreprise commerciale ou un gouvernement prêts à dépenser 10 000 000 dollars sur des puces spécialisées pourra récupérer une clef DES en 6 minutes (en moyenne) toujours pour 38 dollars par clef.

Une organisation très fortunée, par exemple une agence gouvernementale, prête à dépenser 300 000 000 dollars pourra récupérer une clef DES toutes les 12 secondes. Le coût de l'investissement est important, mais on en parle dans la communauté des services secrets. Cela coûte moins cher qu'un Explorer Glomar (conçu pour détruire un sous-marin Russe) et beaucoup moins cher qu'un satellite espion. Ces dépenses ne sont pas faciles à justifier pour une seule cible, mais elle est tout à fait appropriée pour un algorithme de chiffrement comme le DES, et profiter de son aspect populaire dans le monde.

Il y a un indice simple du danger que représentent les agences gouvernementales et services secrets qui recherchent l'information non pas à des fins militaires, mais commerciales. Des rapports au Congrès en 1993 ont indiqué que les gouvernements français et japonais espionnent plus de la moitié du commerce au sein de leurs pays. Ainsi, protéger les informations commerciales comme ce type de menaces n'est pas une proposition d'hypothèse.

4.2 Il y a des attaques plus intelligentes que la force brute

Il est facile de marcher jusqu'à un arbre, et d'y grimper. Il n'y a même pas besoin de briser la fenêtre pour entrer si la porte d'entrée n'est pas correctement verrouillée. Les calculs sur la force de résistance des algorithmes cryptographiques font partie des *pires scénarios*. Ils assument que les chiffrements sont dans un sens parfaits, et que les tentatives pour trouver des raccourcis ont échoué. Un point important est l'approche brutale – la recherche parmi les clefs – qui est tout à fait réalisable contre beaucoup de systèmes en cours d'utilisation. Un autre point : les longueurs de clefs discutées ici sont toujours des minimum. Comme nous l'avons indiqué, une conception prudente devrait utiliser des clefs deux ou trois fois plus longues pour s'assurer une marge de sécurité.

4.3 L'analyse d'autres algorithmes est grossièrement comparable

L'analyse ci-dessus s'est focalisée sur le temps et l'argent à consacrer pour décrypter l'information de clef, avec l'algorithme RC4 et des clefs de 40 bits ou l'algorithme DES et ses 56 bits de clef, mais ces résultats ne sont pas spécifiques à ces algorithmes. Bien que chaque algorithme ait ses propres caractéristiques, l'effort requis pour retrouver les clefs des autres algorithmes est comparable. Il peut y avoir des différences dans les procédures d'implémentation, mais elles n'affectent pas le fait que l'on peut casser par force-brute les algorithmes qui disposent de clefs de longueurs proches.

Spécifiquement, il a été suggéré déjà que différences dans les procédures de préparation, comme le long processus de préparation de clef dans le RC4, permet d'avoir dans certains algorithmes des clefs beaucoup plus longues que dans les autres. Dans le cadre de notre analyse, ces facteurs apparaissent sous la forme des longueurs effectives de clefs, mais pas de plus de 8 bits.

5 Les clefs appropriées pour l'avenir – Une proposition

La table I résume les coûts à réaliser ces attaques de force-brute contre les cryptosystèmes symétriques avec des clés de 40 et 56 bits en utilisant des réseaux d'ordinateurs à usage général, des *Field Programmable Gate Arrays* et des puces développées spécialement.

Elle montre que les clés de 56 bits offrent un niveau de protection – environ un an et demi – qui peut correspondre aux usages de nombreux commerces contre un opposant prêt à dépenser 10 000 dollars. Contre un adversaire prêt à dépenser 300 000 dollars, la période de protection tombe à 19 jours. Au-delà, la protection devient vraiment insignifiante. Un investissement très important, et facilement imaginable pour une agence de services secrets, permettrait de récupérer les clés en temps réel (instantanément).

Quel facteur de travail serait requis pour une sécurité aujourd'hui ? Pour un opposant dont le budget peut aller de 10 à 300 millions de dollars, le temps pour rechercher les clés dans un espace de clés de 75 bits demanderait entre 6 ans et 70 jours. Bien que cette dernière image soit comparable au minimum précédent et ses 19 jours, elle représente (en considérant nos hypothèses d'amortissement) un coût de 19 millions de dollars et ne permettrait de récupérer que cinq clés par an. Les victimes d'une telle attaque devront donc être des cibles importantes.

Parce que beaucoup d'informations doivent rester confidentielles pendant de longues périodes de temps, l'hypothèse ne peut se contenter de la sécurité d'aujourd'hui. Encore plus important : les cryptosystèmes – et surtout si ce sont des standards – doivent pouvoir résister pendant des années, voire des dizaines d'années. Le DES par exemple, a été utilisé pendant plus de vingt ans et continuera encore à l'être. En particulier: la durée de vie d'un cryptosystème excède souvent la durée de vie du produit qui le contient.

Une estimation brute de la force minimale requise comme fonction du temps peut être obtenue en appliquant la règle empirique, que l'on appelle la "Loi de Moore", qui indique que la puissance de calcul informatique disponible pour un coût donné double tous les 18 mois. En prenant en compte la durée de vie de l'équipement cryptographique et la durée de vie des secrets à protéger, nous pensons qu'il est prudent d'assurer la sécurité des données chiffrées pour au moins 20 ans. La loi de Moore prédit que les clés devront avoir au moins 14 bits de plus que le nombre requis aujourd'hui pour se protéger contre une attaque.

En gardant à l'esprit que les coûts de calcul additionnels d'une cryptographie plus forte sont modestes, nous vous recommandons fortement un minimum de 90 bits de clé pour les cryptosystèmes symétriques.

Il est instructif de comparer cette recommandation avec le standard fédéral 46 portant sur le traitement de l'information, le standard de chiffrement fédéral américain (DES), le standard fédéral 185 et le standard de chiffrement avec dépôt de clé (EES). Le DES a été proposé il y a 21 ans et disposait d'une clé de 56 bits. En appliquant la loi de Moore et en ajoutant 14 bits, nous découvrons que la force de DES lorsqu'il a été proposé en 1975 est comparable à un système à 70 bits d'aujourd'hui. Qui plus est, il a été estimé à l'époque que le DES n'était pas assez fort et que les clés seraient récupérées au taux d'une par jour pour un investissement d'environ 20 millions de dollars. Notre estimation de 75 bits d'aujourd'hui correspond à 61 bits en 1975, assez pour avoir déplacé le coût de récupération de clé hors de portée. Le standard de chiffrement avec dépôt de clé, bien qu'inacceptable à beaucoup d'utilisateurs pour plusieurs raisons, contient une notion de clé appropriée qui correspond à la nôtre. Il utilise des clés de 80 bits qui se trouvent dans nos estimations entre 75 et 90 bits.

Table I

Type d'attaquant	Budget	Outil	Temps et coût par clef récupérée		Longueur requise pour protection fin 1995
			40 bits	56 bits	
<i>Hacker</i> habituel	Petit	Temps inutilisé sur ordinateur	Une semaine	Impossible	45
	400 \$	FPGA	5 heures (0,08 \$)	38 heures (5000 \$)	50
Petite entreprise	10 000 \$	FPGA	12 minutes (0,08 \$)	18 mois (5000 \$)	55
Département commercial	300 000 \$	FPGA ou ASIC	24 secondes (0,08 \$)	19 jours (5 000 \$)	60
			0,18 secondes (0,001 \$)	3 heures (38 \$)	
Grande compagnie	10 millions de \$	FPGA ou ASIC	0,7 secondes (0,08 \$)	13 heures (5 000 \$)	70
			0,005 secondes (0,001 \$)	6 minutes (38 \$)	
Services secrets	300 millions de \$	ASIC	0,002 secondes (0,001 \$)	12 secondes (38 \$)	75

À propos des auteurs

Matt Blaze est un scientifique en recherche senior à AT&T Research dans le domaine de la sécurité informatique et la cryptographie. Récemment, Blaze a démontré les faiblesses du système de chiffrement avec dépôt de clef "Clipper". Ses intérêts actuels portent sur la gestion de la confiance à grande échelle et les applications des cartes intelligentes.

Whitfield Diffie est un chercheur reconnu de Sun Microsystems spécialisé dans la sécurité. En 1976, Diffie et Martin Hellman ont créé la cryptographie à clef publique, qui a résolu le problème de la transmission d'informations codées entre deux individus sans rencontre préalable, et qui est la base du chiffrement dans l'âge actuel de l'information.

Ronald L. Rivest est professeur de science informatique au Massachusetts Institute of Technology, directeur associé au laboratoire de science informatique du MIT. Rivest, avec Leonard Adleman et Adi Shamir, ont inventé le cryptosystème à clef publique RSA qui est utilisé de manière importante dans l'industrie. Ron Rivest est l'un des fondateurs de RSA Data Security, Inc. Et le créateur des chiffrements symétriques à longueur de clef variable (e.g. RC4).

Bruce Schneier est le président de Counterpane Systems, une entreprise de consultants spécialisés dans la cryptographie et la sécurité informatique. Schneier écrit et discute fréquemment sur la sécurité informatique et la sécurité des aspects privés de l'existence, l'auteur de "Cryptographie appliquée", livre phare de la cryptographie et le créateur de l'algorithme de chiffrement à clef symétrique Blowfish.

Tsutomu Shimomura est un physicien du calcul employé par le San Diego Supercomputer Center, expert dans la conception d'outils de sécurité informatique. L'année dernière, Shimomura a été responsable du pistage du pirate informatique Kevin Mitnick, qui a volé et altéré des informations électroniques de valeur au travers du pays.

Eric Thompson dirige l'équipe cryptologique de l'entreprise AccessData et c'est un lecteur fréquent des applications cryptographiques. AccessData est spécialisée dans la récupération de données et le décryptage de l'information en utilisant aussi bien les attaques à force-brute que des méthodes "intelligentes". Ses clients réguliers sont le FBI et les autres organisations d'application de la loi, tout comme des entreprises.

Michael Wiener est un conseiller cryptographique à Bell-Northern Research, se focalisant sur la cryptographie, les architectures de sécurité et les infrastructures à clef publique. Son document influent de 1993, "Efficient DES Key Search" décrit en détail comment construire une machine afin de casser le DES par la force-brute (avec des estimations de coût).

REMERCIEMENTS

Les auteurs souhaitent remercier la Business Software Alliance pour avoir fourni un cadre de rencontre d'un jour, qui eu lieu à Chicago le 20 novembre 1995.