Les algorithmes de chiffrement cassés

Introduction

Depuis des décennies, les algorithmes de chiffrement et de hachage ont sans cesse été découverts, améliorés, et ... cassés !
Le tableau ci-dessous retrace un historique des diverses algorithmes, ceux qui sont cassés, et ce qui ne le sont pas encore. Cela permet de faire le point sur les algorithmes encore considérés comme sûrs.

Récapitulatif des algorithmes de chiffrement

Les Algorithmes de chiffrement cassés

Ces algorithmes, à la pointe des Mathématiques il y a encore quelques années sont devenus complètement obsolètes ! Ils ne sont donc plus à utiliser pour protéger vos données...

Rivest, Shamir and Adleman (RSA)

Cet algorithme est **asymétrique**. Il repose sur l'impossibilité de factoriser un grand nombre par deux nombres premiers. Pour casser l'algorithme, il "suffit" de trouver un moyen de factoriser le nombre, donc de trouver au moins un multiple du nombre.

Année d'apparition	Nom	Type	Taille	Année de cassage	Par qui ?
1974	RSA-100	Chiffrement	100 chiffres	1991	Inconnu
1974	RSA-110	Chiffrement	110 chiffres	1992	Inconnu
1974	RSA-120	Chiffrement	120 chiffres	1993	Inconnu
1974	RSA-129	Chiffrement	129 chiffres	1994	Inconnu. 100$ ont été donnés par RSA Labs à ceux qui ont découvert le moyen de factoriser ce nombre de 129 chiffres.
1974	RSA-130	Chiffrement	130 chiffres	1996	Inconnu
1974	RSA-140	Chiffrement	140 chiffres	1999	Une équipe internationale de chercheurs et la puissance de calcul du SARA Amsterdam Academic Computer Center
1974	RSA-155	Chiffrement	155 chiffres	1999	Une équipe internationale de chercheurs

1974	RSA-160	Chiffrement	160 chiffres	2002	Une équipe internationale de chercheurs du BSI
1974	RSA-576	Chiffrement	560 chiffres	2003	Une équipe internationale de chercheurs (J. Franke, F. Bahr, M. Boehm, T. Kleinjung). 10000$ ont été donnés par RSA Labs à ceux qui ont découvert le moyen de factoriser ce nombre de 576 chiffres.
1974	RSA-640	Chiffrement	640 chiffres	2005	Une équipe allemande du "Federal Agency for Information Technology Security" (BSI). 20000$ ont été donnés par RSA Labs à ceux qui ont découvert le moyen de factoriser ce nombre de 640 chiffres.
1974	RSA-768	Chiffrement	768 chiffres	2010	Une équipe composée de 13 personnes
1974	RSA-704	Chiffrement	704 chiffres	2012	Une équipe de l'Inria

Data Encryption Standard (DES)

Cet algorithme est **symétrique**.

Année d'apparition	Nom	Type	Taille	Année de cassage	Par qui ?
1976	DES-56	Chiffrement	56 bits	1997	Utilisateurs d'Internet sous la bannière de Distributed.net et Electronic Frontier Foundation

Elliptic Curve Cryptography (ECCp)

Cet algorithme est **asymétrique**.

Année d'apparition	Nom	Type	Taille	Année de cassage	Par qui ?
1985	ECCp-79	Chiffrement	79 bits	1997	Inconnu
1985	ECCp-89	Chiffrement	89 bits	1998	Inconnu
1985	ECCp-97	Chiffrement	97 bits	1998	Inconnu. 5000$ ont été attribués par Certicom à ceux qui ont cassé l'algorithme.
1985	ECCp-109	Chiffrement	109 bits	2002	Utilisateurs d'Internet sous la bannière d'Ecc2.com (site disparu depuis). 10000$ ont été attribués par Certicom à ceux qui ont cassé l'algorithme.

Rivest Cipher (RC)

Cet algorithme est **symétrique**.

Année d'apparition	Nom	Type	Taille	Année de cassage	Par qui ?
1987	RC4	Chiffrement	40 bits	1995	Adam Back, Eric Young et David Byers
1994	RC5-56	Chiffrement	56 bits	1997	Utilisateurs d'Internet sous la bannière de Distributed.net
1994	RC5-64	Chiffrement	64 bits	2002	Utilisateurs d'Internet sous la bannière de Distributed.net

CS Cipher (CSC)

Cet algorithme est **symétrique**.

Année d'apparition	Nom	Type	Taille	Année de cassage	Par qui ?
1997	CS Cipher (CSC-56)	Chiffrement	56 bits	2000	Utilisateurs d'Internet sous la bannière de Distributed.net

Message Digest Algorithm (MD)

Cet algorithme est **une fonction de hachage**.

Année d'apparition	Nom	Type	Taille	Année de cassage	Par qui ?
1990	Message Digest Algorithm (MD4)	Hachage	128 bits	1996	Hans Dobbertin
1991	Message Digest Algorithm (MD5)	Hachage	128 bits	2004	Xiaoyun Wang

Secure Hash Algorithm (SHA)

Cet algorithme est **une fonction de hachage**.

Les Algorithmes de chiffrement toujours considérés comme sûrs

Voici enfin les algorithmes toujours considérés comme assez robustes pour la protection de vos données

confidentielles.

Rivest, Shamir and Adleman (RSA)

Année d'apparition	Nom	Type	Taille	Informations
1974	RSA-500	Chiffrement	500 chiffres	RSA Labs
1974	RSA-1024	Chiffrement	1024 chiffres	RSA Labs
1974	RSA-2048	Chiffrement	2048 chiffres	RSA Labs

Data Encryption Standard

Année d'apparition	Nom	Type	Taille	Informations
1977	Triple-DES	Chiffrement	192 bits	-

Elliptic Curve Cryptography (ECCp)

Année d'apparition	Nom	Type	Taille	Informations
1985	ECCp-131	Chiffrement	131 bits	Certicom offre 20000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 2.3×10^{10} (estimation Certicom)
1985	ECCp-163	Chiffrement	163 bits	Certicom offre 30000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 2.3×10^{15} (estimation Certicom)
1985	ECCp-191	Chiffrement	191 bits	Certicom offre 40000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 4.8×10^{19} (estimation Certicom)
1985	ECCp-239	Chiffrement	239 bits	Certicom offre 50000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 1.4×10^{27} (estimation Certicom)
1985	ECC2p-359	Chiffrement	359 bits	Certicom offre 100000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 3.7×10^{45} (estimation Certicom)

Elliptic Curve Cryptography (ECC2)

Année d'apparition	Nom	Type	Taille	Informations
Inconnu	ECC2K-130	Chiffrement	131 bits	Certicom offre 20000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 2.7×10^{9} (estimation Certicom)
Inconnu	ECC2-131	Chiffrement	131 bits	Certicom offre 20000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 6.6×10^{10} (estimation Certicom)
Inconnu	ECC2-163	Chiffrement	163 bits	Certicom offre 30000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 2.9×10^{15} (estimation Certicom)
Inconnu	ECC2K-163	Chiffrement	163 bits	Certicom offre 30000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 4.6×10^{14} (estimation Certicom)
Inconnu	ECC2-191	Chiffrement	191 bits	Certicom offre 40000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 1.4×10^{20} (estimation Certicom)
Inconnu	ECC2-238	Chiffrement	239 bits	Certicom offre 50000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 3.0×10^{27} (estimation Certicom)
Inconnu	ECC2K-238	Chiffrement	239 bits	Certicom offre 50000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 1.3×10^{26} (estimation Certicom)
Inconnu	ECC2-353	Chiffrement	359 bits	Certicom offre 100000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 1.4×10^{45} (estimation Certicom)
Inconnu	ECC2K-358	Chiffrement	359 bits	Certicom offre 100000$ à la première personne qui cassera l'algorithme. Nombre de jours/machine nécessaire au cassage : 2.8×10^{44} (estimation Certicom)

Rivest Cipher (RC)

Année d'apparition	Nom	Type	Taille	Informations
1994	RC5-72	Chiffrement	72 bits	Durée estimée de cassage par Distributed.net au 01/09/2014 : 300 ans. Rejoignez notre équipe de cassage de la clé RC5-72

Secure Hash Algorithm (SHA)

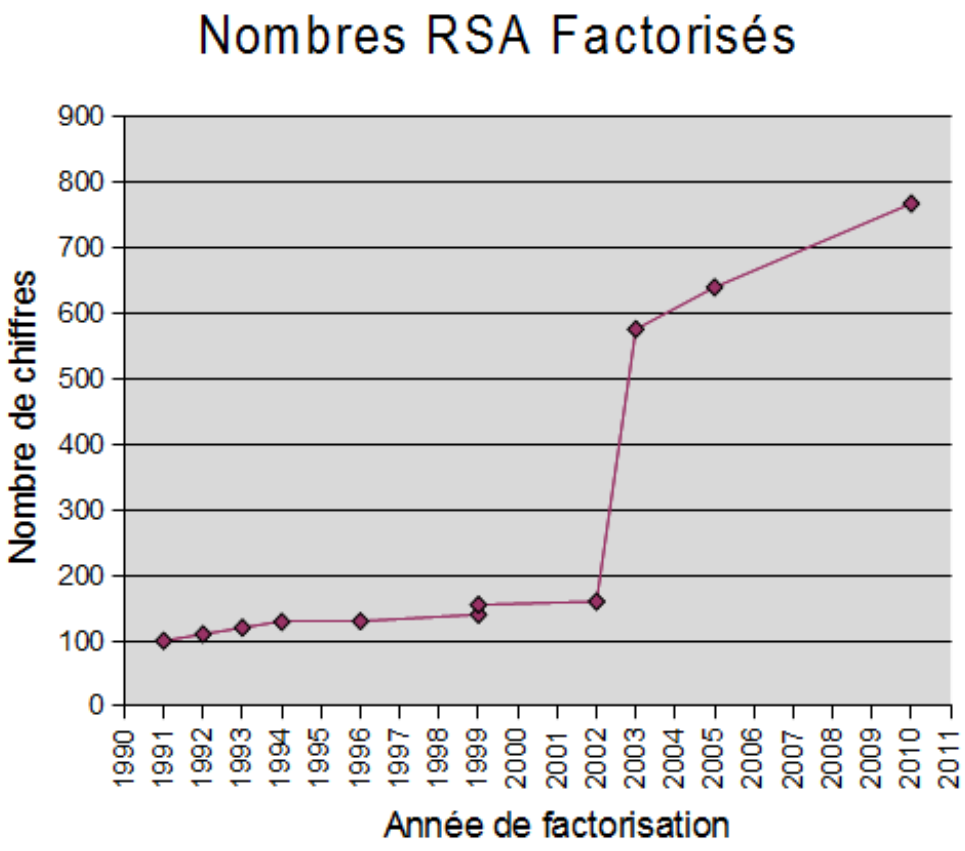
Année d'apparition	Nom	Type	Taille	Informations
1995	SHA-224	Hachage	224 bits	-
1995	SHA-256 (SHA-2)	Hachage	256 bits	-
1995	SHA-384	Hachage	384 bits	-
1995	SHA-512 (SHA-2)	Hachage	512 bits	-
2012	SHA-3	Hachage	512 bits	-

Advanced Encryption Standard (AES)

Année d'apparition	Nom	Type	Taille	Informations
1999	AES-128	Chiffrement	128 bits	-
1999	AES-192	Chiffrement	192 bits	-
1999	AES-256	Chiffrement	256 bits	-

Et l'évolution dans tout ça...

Si on regarde de prêt le cassage de l'algorithme RSA, voici ce que l'on a :



Voici ce que l'on remarque :

- De 1990 à 2002 : Une courbe très linéaire ! Pourquoi ? La difficulté à casser un algorithme est une courbe exponentielle d'un algorithme à l'autre. Cependant, cette courbe est fortement aténuée par cette autre courbe exponentielle que tout le monde connait : la puissance des ordinateurs d'une année à l'autre !
- En 2003 : Une rupture ! Pourquoi cette rupture ? Parce qu'à la courbe exponentielle de la puissance de calcul s'ajoute l'évolution des Mathématiques ! Des avancées énormes en terme de théories de factorisation des grands nombres ont permit de bondir vers le cassage des algorithmes RSA pour des nombres de 576 et 640 chiffres !

Nous vous conseillons

Pour vos applications cryptographiques (VPN, chiffrement de documents, etc...) nous vous conseillons actuellement de choisir **AES** et **RSA-1024** pour le chiffrement et **SHA-256** pour le hachage. Triple-DES vit certainement ses dernières années de robustesse...
Attention néanmoins à la législation en cours de votre pays en terme de cryptographie !

Conclusion

Avec la Loi de Moore qui spécifie que, depuis les années 70, la puissance des ordinateurs double tous les 2 ans, il faut s'attendre à une boucle sans fin : d'anciens algorithmes seront cassés, de nouveaux devront apparaîtres.

Si tous les algorithmes de chiffrement et de hachage sont cassés sans qu'il n'y ait de nouveaux, alors, fini le VPN, fini HTTPS, fini les mails cryptés, il n'y aura plus de sécurité possible dans l'informatique...

Heureusement, dans l'état actuel des choses, il y a encore quelques dizaines (centaines ?) d'années devant nous avant que cela arrive !

Arnaud Jacques
4 Octobre 2004, mis à jour Septembre 2014