REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

N° d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux

Par: Othman LADJELAT

SUJET

Méthode De Cryptographie basée sur L'ADN « DNA Encryption System»

Soutenu publiquement le : 14/06/2015 devant le jury composé de :

Prof : Bouderah.B	**Université de M'sila**	**Rapporteur**

Promotion : 2014/ 2015

Table des matières

Chapitre II : Le calcul à l'ADN

Chapitre III : Introduction à la cryptographie à l'ADN

Chapitre IV : Algorithme Proposé

Chapitre V : Réalisation & résultats expérimentaux

Depuis le début des civilisations, le besoin en sécurité des communications préoccupe l'humanité. Garantir la confidentialité du contenu de ces communications était le premier problème auquel les gens ont tenté de trouver une solution. Ce besoin à mené à l'apparition de la cryptographie comme moyen puissant pour garantir la confidentialité des informations échangées à travers plusieurs méthodes conçues et améliorées depuis des siècles.

Longtemps, la cryptographie est restée un art réservé aux militaires. C'est au cours de ces quarante dernières années que la cryptographie est devenue une science basée sur les mathématiques et l'informatique. Le développement des moyens de communication à l'échelle planétaire constitue aujourd'hui le moteur de la recherche dans ce domaine. Les applications principales de la cryptographie sont bien sûr le chiffrement des messages pour en garantir la confidentialité, mais aussi l'authentification à distance, la signature des documents numériques, et le contrôle de l'intégrité des messages transmis sur un réseau informatique.

Malgré l'évolution exponentielle de la technologie de l'information et la vitesse atteinte par les supercalculateurs actuels, l'utilisation des circuits électroniques impose plusieurs limites pratiques, ce qui a conduit vers l'apparition de nouveaux paradigmes du calcul tel que le calcul quantique et le calcul à l'ADN. Ce domaine est apparu en 1994, lorsque *Léonard Adleman* a réussi à résoudre le problème du chemin hamiltonien en utilisant des molécules d'ADN.

Le potentiel remarquable du calcul à l'ADN a suscité l'intérêt de chercheurs dans divers domaines, notamment en cryptographie, conduisant ainsi à l'émergence d'un nouvel axe qui est la cryptographie à l'ADN. En effet, grâce au parallélisme massif dans les calculs et la densité de stockage qu'offre cette molécule, l'ADN s'avérer très utile dans un domaine aussi complexe. Cependant, la nécessité d'une technologie de pointe ainsi que l'absence d'une base théorique ralentissent le développement de ce domaine.

Notre travail consiste à proposer une méthode cryptographique inspirée des processus de transformation de l'ADN en ARN puis en protéines appelé le dogme central de la biologie.

Le but n'est donc pas d'utiliser l'ADN mais uniquement de s'en inspirer, et ce en partant de l'idée de *Ning Kang* qui a proposé une méthode cryptographique qui simule les mécanismes du dogme central.

Afin de proposer un algorithme cryptographique offrant un bon degré de sécurité, nous nous sommes basés sur les techniques utilisées dans les algorithmes standards actuels ainsi qu'en suivant les recommandations des agences et instituts de sécurité mondiaux.

Notre mémoire se compose de cinq chapitres organisés comme suit :

Le premier chapitre est une introduction générale à la cryptologie, dans laquelle nous présentons les aspects les plus importants de la cryptographie et de la cryptanalyse.

Dans le deuxième chapitre, nous présentons l'ADN et les outils de la biologie moléculaire, ainsi qu'un bref aperçu sur le calcul à l'ADN.

Le troisième chapitre est dédié à la présentation de la cryptographie à l'ADN dans laquelle nous détaillons la méthode de Ning Kang.

Dans le quatrième chapitre, nous présentons notre algorithme en détaillant ses différentes étapes.

Afin d'évaluer les performances de notre algorithme, des tests expérimentaux ont été effectués, ainsi que l'analyse des résultats obtenus seront l'objet du dernier chapitre de notre mémoire.

Enfin, une conclusion générale clos le mémoire, dans laquelle nous présentons les avantages et les inconvénients de la solution proposée ainsi que des perspectives pour les travaux futurs.

Le développement remarquable de la technologie de l'information et de la communication et l'utilisation des réseaux non sécurisés pour l'échange des données confidentielles ont rendu l'utilisation de la cryptographie indispensable dans la sécurisation de ces communications notamment dans la garantie de la confidentialité et l'authentification à distance.

Notre travail avait comme objectif la conception et l'implémentation d'une méthode cryptographique inspirée de l'ADN. Pour se faire, il a été nécessaire de comprendre les concepts et outils utilisés aussi bien dans le domaine de la cryptographie, que dans le domaine de la biologie moléculaire.

L'avènement du calcul à l'ADN, proposé par *Adleman* en 1994, a ouvert des portes à l'utilisation de cette molécule comme outils de calcul et de résolution de problèmes complexes. Les cryptographes ont vu en l'ADN un outil très puissant, par son parallélisme et sa capacité de stockage, pour concevoir des méthodes cryptographiques à l'ADN. Ces méthodes utilisent un laboratoire avec les outils biologiques nécessaires (ADN, biologistes, outils de la biologie moléculaire…) pour parvenir à chiffrer/déchiffrer les informations.

Ning Kang a proposé une méthode cryptographique inspirée de l'ADN ***[KAN 09]***. Le principe de chiffrement de cette méthode est inspiré des processus biologiques du dogme central de la biologie moléculaire.

En se basant sur l'idée de *Ning Kang*, et après avoir étudié la conception des méthodes cryptographiques symétriques chiffrant par bloc (en particulier les deux standards l'AES et le DES), nous avons pu proposer une méthode cryptographique appartenant à la famille des *bloc cipher,* agissant par bloc de 128 bits, utilisant des clefs de 128 bits et 256 bits et qui s'inspire du fonctionnement des processus du dogme central.

De plus qu'elles sont simples, rapides en chiffrement, très convenables avec une implémentation hardware, les méthodes de chiffrement par bloc offrent un niveau de sécurité très acceptable.

Dans la conception de cette méthode, nous avons essayé de concrétiser le mieux possible les deux principes de *Shannon,* à savoir, *la diffusion* et *la confusion.* Le premier principe est appliqué à l'aide des permutations et des transpositions conçues en respectant certains critères qui augmentent le niveau de sécurité de la méthode, alors que le deuxième principe est inspiré de l'ADN en simulant les deux processus du *dogme central,* à savoir, *la transcription et la translation.*

En utilisant notre méthode, l'utilisateur peut chiffrer/déchiffrer n'importe quel type de fichiers de n'importe quelle taille avec un taux de chiffrement estimé à *1 méga-octets par seconde* (avec les caractéristiques de la machine utilisée et les paramètres par défaut). Aussi, il peut modifier les paramètres de l'algorithme (nombre de tours, le, mode chiffrement…) selon son besoin en temps et sécurité.

Cependant, le problème principal rencontré dans ce travail est l'évaluation de la sécurité de la méthode proposée. En effet, pour évaluer la sécurité d'une méthode cryptographique symétrique, il faut lui faire subir plusieurs attaques (ou calculer la complexité de ces attaques). Ceci n'est pas évident et nécessite du temps et des connaissances avancées en statistiques et mathématiques. Néanmoins, le choix d'une méthode *bloc cipher* dans notre conception nous garantit un bon niveau de sécurité, puisque nous avons concrétisé la *confusion* et la *diffusion*, et appliqué les recommandations émanant des experts mondiaux en cryptographie tel que la *NSA* et le *NIST.*

Ce travail est ouvert à des perspectives visant à l'enrichir et l'améliorer selon les axes suivants :

- *Axe sécurité :* améliorer la sécurité de la méthode en implémentant des attaques cryptanalytiques, comme l'attaque différentielle ou linéaire et selon les résultats obtenus, optimiser les tables utilisées (les permutations, la table du code génétique).

- *Axe temps de chiffrement* : la parallélisation de certaines parties du code (lorsque ce la est possible) augmentera certainement le taux de chiffrement/déchiffrement.

[1] : H.X. Mel, Doris Baker, *La cryptographie décryptée,* CampusPress 2001.

[2] : Bruce Schneier *« Cryptographie appliquée, Algorithmes, protocoles et codes source en C »* 2e édition Vuibert 1997

[3] : H.X. Mel, Doris Baker, *La cryptographie décryptée,* CampusPress 2001.

[4] : Dumont Renaud, *Introduction à la Cryptographie et à la Sécurité Informatique,* Université de Liège, Faculté des Sciences Appliquées, 2007.

[5] : David Pointcheval, *La Cryptographie Asymétrique et les Preuves de Sécurité,* 2003.

www.di.ens.fr/~pointche/Documents/Slides/s2002_cachan.pdf

[6] : François Arnault, Cours *Théorie des nombres & cryptographie,* université de Limoges, mai 2002.

http://www.unilim.fr/pages_perso/francois.arnault/toc.html

[7] : Network Associates International, *Introduction à la cryptographie,* Gatwickstraat 25 NL-1043 GL Amsterdam, http://www.nai.com

[8] : A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1996

[9] : Joan Daemen, Vincent Rijmen, *AES proposal : Rijndael*, 1999.

http://www.daimi.au.dk/~ivan/rijndael.pdf.

[10] : Jacques Stern, Louis Granboulan, Phong Nguyen et David Pointcheval *Conception des algorithmes cryptographiques* Cours de magistère M.M.F.A.I. Ecole normale supérieure Edition 2004.

www.di.ens.fr/~wwwgrecc/Enseignement/CoursCryptoMMFAI.pdf

[11] : J. Capirossi, *La cryptographie. Quelle sécurité ?,* 2003.

http://capirossi.org/info/Securite/Cryptov2.pdf

[12] : : Anne Canteaut, *Cryptanalyse des chiffrements à clef secrète par blocs,* Article paru dans *MISC - Le magazine de la sécurité informatique*, mars 2002.

[13] : Alain Tapp, *Cryptographie*. Laboratoire d'informatique théorique et Quantique Université de Montréal 2004.

http://www.iro.umontreal.ca/~tappa/pages/cours/cryptographie%20camp.ppt

[14] : Florent Gratta, *Les cryptosystèmes déjà cassés,* 2004.

http://p2004ir.free.fr/MA514-Cryptographie/Cryptosystemes_Casses/Cryptosystemes_Casses.pdf

[15] : Leonard.Adleman, *Molecular computation of solutions to combinatorial Problems* , Sience: 266 :1021-1024, 1994.

[16] : Erwin Schrodinger, *« What is life »*. 1944.

http://whatislife.stanford.edu/Homepage/LoCo_files/What-is-Life.pdf

[17] : G.Bourbonnais, *L'information génétique*. Université Cégep de Sainte-Foy

http://www.cegep-ste-foy.qc.ca/profs/gbourbonnais/pasca

[18] : E.G.Berger, T.Hennet, *Le génome humain, Principe fondamental sur l'ADN*. Forum Med Suisse N°23 le 6 juin 2001.

[19] : Hélène Antaya, Isabelle Ascah-Coallier, *L'ordinateur à l'ADN*. Licence d'informatique 2002-2003, Université de Nice Sophia-Antipolis

[20] : Leonard Adleman, *Calculer avec de l'ADN : informatique et biologie* ?, Pour la science-n°252, octobre 1998.

[21] : R.J.Lipton, U*sing DNA to solve NP-complete problems*, In Science: 268:542-545, April 28,1995.

[22] : V.Gupta, S.Parthasarathy and M.J.Zaki, *Arithmetic and Logic Operations with DNA* , 3rd DIMACS Workshop on DNA Based computers, 1997.

[23] : Z.Frank Qiu, M.Lu, *Arithmetic and logic operations for DNA computers.In Parallel and Distributed Computing and Networks,* (PDCN'98),pages 481-486.IASTED, December 1998.

[24] : T.Tateishi, A.Fujiwara, *Data structures for storing binary numbers in DNA computing.* FCS 34-40, 2007.

[25] : XIAO Guozhen , LU Mingxin , QIN Lei & LAI Xuejia , *New field of cryptography: 'DNA cryptography* . Xidian University, Xi'an 710071, China; Chinese Science Bulletin 2006 Vol. 51 No. 12 1413—1420, January 16, 2006

[26] : É.Jouzier, *Une découverte majeure du XXe siècle : La structure de l'ADN, le secret de la vie vue au travers de la philatélie*, Université Victor-Segalen Bordeaux, 2004.

[27] : Constanza Lampasona, *DNA Computers Applications Cryptography.*Innovative Computer Architectures and Concepts Computer Architecture Department - University of Stuttgart June 2002.

[28] : Ashish Gehani, Thomas H. LaBean, John H. Reif, *DNA based cryptography* 5th Annual DIMACS Meeting on DNA Based Computers (DNA 5), MIT, Cambridge, MA, June 1999.

[29] : Dr.Makri-Mokrane Samia, Pr.Tazir Meriem, *Introduction à la génétique moléculaire* , Université d'Alger Département de médecine, année 2006.
http://www.sante.dz/adrmng/cours02.pdf

[30] : E.G.Berger, T.Hennet, *Le génome humain, Principe fondamental sur l'ADN*. Forum Med Suisse N°23 le 6 juin 2001.

[31] : B.Houchmandzadeh, *Ballade autour de quelques thèmes de biologie*. 10 octobre 2005.

[32] : Pr.Lafleur, *Les traits s'héritent et se transforment,* Université Pierre et Marie Curie – UFR de Biologie, 2006, www.snv.jussieu.fr

[33] : Ning Kang, *A Pseudo DNA Cryptography Methode,* DBLP:journals/corr/abs-0903-2693, 2009.

[34] : V.Gupta, S.Parthasarathy and M.J.Zaki, *Arithmetic and Logic Operations with DNA* , 3rd DIMACS Workshop on DNA Based computers, 1997.

[35] : site internet www.codeproject.com.

ملخص

تغيرت طرق نقل المعلومات بعد أن أصبحت تكنولوجيا المعلومات و الاتصالات تغزو جميع ميادين الحياة سواء العملية او الخاصة ، وهذا النقل غير مضمون عبر الشبكات الغير محمية، فمثلا شبكة الانترنت توفر مستوى عالي من الحماية و من بين الوسائل المستخدمة لذلك التشفير و هو الأكثر استعمالا ولايمكن الاستغناء عنه لا سيما في ضمان سرية المعلومات المتبادلة .

تشفير ADN هو محور جديد في ابحاث التشفير ،و الذي يعتمد على مختلف تقنيات علم الاحياء من اجل ابتكار طرق تشفير حديثة.

يهدف عملنا لاقتراح طريقة التشفير على أساس تقنيات التشفير المستخدمة في خوارزميات التشفير الاساسية ومستوحاة من آليات العقيدة المركزية لعلم الأحياء الجزيئي.

الكلمات المفتاحية: حماية المعلومة،التشفير، حساب ADN،تشفر ADN، العقيدة المركزية، علم الأحياء الجزيئي

Abstract

The new technologies of information and communication are present in all aspects of modern life. These various transmission means of information through non secured networks, as internet, impose the guarantee of a high security level. Among the used means, the cryptography is one of the most efficient and most indispensable, notably in the guarantee of the confidentiality of the exchanged information.

The DNA cryptography is a new axis of research in cryptography that calls on the different tools of the biology in order to conceive some new methods cryptography implemented in biologic laboratories.

Our work aimes to propose a cryptographic method based on the techniques of ciphering used in the standard cryptographic algorithms, and inspired from the mechanisms of the central dogma of the molecular biology.

Key words: Computer Security, Cryptography, DNA Computing, DNA Cryptography, central Dogma, molecular Biology.

Résumé

Les nouvelles technologies de l'information et de la communication sont présentes dans tous les aspects de la vie moderne. Ces divers moyens de transmission de l'information à travers des réseaux non sécurisés, comme internet, imposent la garantie d'un niveau de sécurité élevé. Parmi les moyens utilisés, la cryptographie est l'un des plus efficaces et les plus indispensables, notamment dans la garantie de la confidentialité des informations échangées.

La cryptographie à l'ADN est un nouvel axe de recherche en cryptographie qui fait appel aux différents outils de la biologie afin de concevoir des nouvelles méthodes cryptographiques implémentées dans des laboratoires biologiques.

Notre travail a pour objectif de proposer une méthode cryptographique basée sur les techniques de chiffrement utilisées dans les algorithmes cryptographiques standards, et inspirée des mécanismes du dogme central de la biologie moléculaire.

Mots clés : Sécurité Informatique, Cryptographie, Calcul à l'ADN, Cryptographie à l'ADN, Dogme central, Biologie moléculaire.