N° d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DE MATHEMATIQUES ET D'INFORMATIQUE

Département d'Informatique

MEMOIRE

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : système d'information avancée

Par :

Mourad ALILI

SUJET

Mise au point d'un système de cryptage/décryptage pour un client de messagerie électronique

Soutenu publiquement le : 27/06/2012 devant le jury composé de :

Mr. LAMICHE Chaabane	Université de M'sila	Président
Mr. HEMMAK Allaoua	Université de M'sila	Rapporteur
Mr. CHIKOUCHE Nourddine	Université de M'sila	Examinateur
Mr. BOUBAKIR Mouhamed	Université de M'sila	Examinateur

Promotion : 2011 /2012

Table des matières

CHAPITRE 2 : LES MESSAGERIE ELECTRONIQUE ET LEUR CHIFFREMENT

CHAPITRE 3 : ANALYSE ET CONCEPTION

Introduction générale

Les communications ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer un message de façon sécuritaire est probablement aussi ancien que les communications elles-mêmes.

D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif. Dans notre monde moderne, où diverses méthodes de communication sont utilisées régulièrement, le besoin de confidentialité est plus présent que jamais à une multitude de niveaux. Par exemple, il est normal qu'une firme désire protéger ses nouveaux logiciels contre la piraterie, que les institutions bancaires veuillent s'assurer que les transactions sont sécuritaires et que tous les individus souhaitent que l'on protège leurs données personnelles.

Le besoin de communications sécuritaires a donné naissance à la science que nous appelons cryptologie.

Le cryptage (ou chiffrement) est une opération mathématique qui permet de coder le contenu d'un message afin de garantir que seule votre correspondant pourra le déchiffrer (ou le décrypter).

Le courrier électronique, ou courriel par contraction, est un service de transmission de messages envoyés électroniquement via un réseau informatique (principalement l'Internet) dans la boite aux lettres électronique d'un destinataire choisi par l'émetteur.

Lors de son acheminement, un email est relayé par un certain nombre de serveurs où il se retrouve donc copié. Et derrière ces serveurs, ce sont autant d'entreprises commerciales ou d'administratrices curieuses qui peuvent, bien que la loi défende les correspondances privées, fouiner dans vos courriers. Les mails peuvent également être interceptés lors de leurs transferts.

Le chiffrement est réalisé par l'émetteur en utilisant la clé publique du destinataire. En réalité le chiffrement du message est réalisé par un algorithme symétrique, beaucoup plus rapide. La clé publique du destinataire est utilisée pour chiffrer la clé secrète de chiffrement du message. Dans ce cas, seul le destinataire peut récupérer la clé secrète, mais celle-ci est connue de l'émetteur du message.

A partir de ce mécanisme nous proposons une petite amélioration sur ce mécanisme afin d'augmenter le niveau de sécurité et difficulté l'attaque, cette amélioration réside d'ajouter une nouvelle clef d'algorithme symétrique (Rijndael dans notre cas) pour protéger la clef de session avons le crypté avec la clef publique de destinataire.

Pour ce but, nous allons concevoir un logiciel de messagerie électronique permettant de crypter les emails sortant et décrypter les emails entrants selon l'amélioration précédente.

Le besoin de comminations sécurisés sur l'internet, et le vaste stade d'utilisation des messageries électroniques, étaient les motivations majeures à aborder ce travail (client de messagerie électronique) pour le but de sécuriser la communication au cours de l'envoi et de la réception des emails.

L'objectif de ce travail était d'étudier et concevoir un logiciel de messagerie électronique pour la sécurité des courriers électroniques, fonctionne sur le réseau internet, et aussi permettre de la génération des clefs (publiques et privés) des cryptages.

La structure de ce mémoire s'articule autour de quatre chapitres :

Chapitre 01 : présente les définitions et les fondements théoriques de la cryptographie, passe sur les algorithmes modernes de cette dernière et on terminera ce chapitre par la définition de fonction de hachage et le codage de l'information.

Chapitre 02 : concerne la résolution du problème sujet de l'étude : traite les courriers électroniques et sa structure ainsi que les protocoles utilisés lors de l'envoi et la réception des mails, en passant sur l'état de l'art et notre modeste contribution.

Chapitre 03 : la conception de notre logiciel en utilisant UML comme langage de modélisation.

Chapitre 04 : concerne la réalisation de notre logiciel par des interfaces homme machine avec des tests dans le but de faciliter l'utilisation de notre logiciel.

CONCLUSION

L'objectif de ce travail était d'étudier et concevoir un logiciel de messagerie électronique pour la sécurité des courriers électroniques, fonctionne sur le réseau internet, et aussi permettre de la génération des clefs (publiques et privés) des cryptages.

Nous nous sommes intéressées dans ce mémoire au fonctionnement des messageries électroniques et leurs clients (agents), et les protocoles utilisés lors de l'envoi et l'acheminement des courriers, ainsi les techniques utilisées aujourd'hui pour le cryptage des courriers électronique comme PGP. Aussi on étudier dans ce travail la méthode de cryptographie symétrique Rijndael (standard de NIST), et la cryptographie asymétrique RSA, ces méthodes sont largement utilisées dans nos jours.

Pour un simple but de découvrir les secrets et astuces de la programmation en C#, donc d'apprendre plus, on a volontairement intégré des composantes sur l'environnement de visuel studio (Openpop.dll, irisskin.dll) pour utiliser d'autre fonctionnalités.

Nous considérons que l'essentiel de notre but est atteint même s'il reste des choses à ajouter, et comme perspectives nous proposons :

1- L'implémentation d'un web mail permettant de gérer le chiffrement des emails sortants et le déchiffrement des emails entrants selon l'amélioration qui nous avons ajouté.
2- L'intégration des algorithmes de comprissions des données dans notre client de messagerie pour minimiser la taille des donnés envoyer, et pour le but de difficulté l'attaque.
3- Intégration le service de signature numérique et les autres fonctions de PGP pour l'obtention d'un protocole plus sécurisé.
4- Intégration de chiffrement des fichiers attachés dans notre logiciel.

En fin, on n'a pas présenté un travail exhaustif, hermétique à tout questionnement futur. En élaborant une solution possible parmi tant d'autres, on a voulu contribuer modestement à la résurgence d'autres idées, à même donner une nouvelle impulsion à la science informatique.

BIBLIOGRAPHIE

[1] : Jean-Philippe Gaulier, « *Analyse des algorithmes finalistes concourant pour le futur standard AES* », Mémoire de synthèse soumis dans le cadre d'un probatoire en vue de l'acquisition d'un diplôme en Ingénierie et Intégration Informatique Systèmes d'Information

[2] : Fabien GARGNE, Christian KNOFF, Gaëtan LECOURTOIS, « *Codage Compression et Cryptologie* », 2004–2005, Université de Nice-Sophia Antipolis
http://www.deptinfo.unice.fr/twiki/pub/Linfo/

[3] : Bourgeois Morgan, « *Initiation à PGP : GnuPG* », 19/07/2006
http://www.mbourgeois.developpez.com/articles/

[4] : Jonathan BLANC, Adrien DE GEORGES, « *TECHNIQUES DE CRYPTOGRAPHIE* »
http://www.deptinfo.unice.fr/twiki/pub/Linfo

[5] : Serge Aumont, Roland Dirlewanger, Olivier Porte, « *L'accès sécurisé aux données* », Novembre 1999
http://www.1999.jres.org/tutoriaux/tutorial4-chiffrement.pdf

[6] : David Pointcheval, « *Le Chiffrement Asymétrique et la Sécurité Prouvée* », 17 juin 2002, Université Pris7 Habilitation à Diriger des Recherches.
http://www.www.di.ens.fr/~pointche/Documents/Reports/2002_HDRThesis.pdf

[7] : Stephan Robert, *Eléments de cryptographie,* Septembre 2005
http://www.stephan-robert.ch/attachments/File/Networking/crypto_v10-corr1.pdf

[8] : Destree Lucile, Marchal Mickaël, « *Mini-RSA Programme d'initiation au chiffrement RSA* »
http://www.lesitedemika.org/ressources/cryptographie_rsa.pdf

[9] : Jean-Guillaume Dumas, « *factorisation d'entiers,cryptographie* »
http://www.ljk.imag.fr/membres/Jean-Guillaume.Dumas/

[10] : Emonet jean-Bruno, « *Algorithmes de chiffrement Mesures de performances réseaux* », 24 juin 2005
http://www.www.rd.cri74.org/repository/securite/algo_chiffrement.pdf

[11] : « *Introduction à la cryptographie* », 09/02/01, Support de cours du cabinet Hervé Schauer Consultants (HSC)
http://www.hsc.fr/ressources/cours/crypto/crypto.pdf

[12] : Gilles Dubertret, « *INITIATION A LA CRYPTOGRAPHIE* », octobre 1998, Vibert

[13] : A.Gosselin, « *Le courrier électronique* », Janvier 1998
http://www.etab.ac-caen.fr/montchamp/enseign/documnts/ uti_mail.pdf

[14] : Stéphane Lohier, Dominique Présent, « *internet : services et réseaux* », paris, 2004, Dunod

[15] : CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS, « *SECURITE DE LA MESSAGERIE* », Septembre 2005
http://www.clusif.asso.fr/fr/production/ouvrages/pdf/Securite_Messagerie.pdf

[16] : « *Le courrier électronique* »
http://www.another-teacher.net/IMG/pdf/05_Le_courrier_electronique__mis-en-forme_custom.pdf

[17] : Carherine Szaibrum, « *Internet initiation* », paris 2000, DUNOD

[18] : DOMINIQUE LACHIVER, « *Courrier électronique* », Septembre 2010
http://lachiver.fr/supports/opale/tic/internet/courrier/courrier_papier.publi/paper/courrier_papier.pdf

[19] : GAADI Mohamed, ABDRUBO MOHAMED BAKER Gehad, *« Conception et Réalisation d'un Système de Messagerie Electronique dans un Intranet »*, 2009-2010, Mémoire de fin d'études.

[20] : *« Crypter le courrier »*
http://www.competencemicro.com/supplements/inetsecu/pgp.pdf

[21] : LAES : Advanced Encryption Standard, May 17, 2012
http://w ww.securiteinfo.com/cryptographie/aes.shtml

[22] : http://www.commentcamarche.net/contents/base/base64.php3

[23] : http://office.microsoft.com/fr-ch/outlook-help/chiffrer-des-messages-electroniques-HP010355559.aspx

[24] : Fabián Rodríguez, *« Chiffrer son courriel avec Enigmail »*, 28 septembre 2004, Guide d'installation et d'utilisation pour Mozilla Thunderbird, Enigmail et WinPT
http://www.framasoft.net/IMG/tb-enigmail.pdf

[25] : *http://www.commentcamarche.net/contents/base/ascii.php3*

Résumé

La communication est un aspect essentiel de la vie humaine, de nouvelles technologies de l'information et de la communication se développent continuellement en offrant de nouvelles potentialités. Notre travail, se situe dans le cadre du développement d'un système de cryptage pour un client de messagerie électronique dans internet permettant ainsi une bonne communication sécurisée entre les sociétés et les personnes. Pour ce faire, on a conçu un logiciel de messagerie électronique permettant de gérer le cryptage des emails sortants et décryptage des emails entrants, utilisant le mécanisme de PGP avec quelque amélioration. La conception est a été réalisée par le langage UML. L'implémentation a été développée par le langage orienté-objet C# dans l'environnement de Visual studio 2010.

Mots clés : Cryptographie, Messagerie électronique, Cryptage Messagerie électronique, Algorithme de Cryptage, Protocoles de messagerie électronique, UML.

Abstract

The Communication is an essential aspect of human life, new technologies of information and communication develop continually offering new potentialities. Our work is situated in the development of a system of encryption for e-mail client in Internet allowing secure good communication between companies and individuals. To do this, we designed an e-mail software used to manage the encryption of outgoing emails and decryption of incoming emails, using the PGP mechanism with some improvements. The design was carried out by the UML. The implementation was developed by the object-oriented language C # in Visual Studio 2010 environment.

Keywords: Cryptography, Email, E-mail Encryption, Encryption Algorithm, email protocols, UML.

ملخص

الاتصال هو أحد الجوانب الأساسية للحياة البشرية، والتكنولوجيات الجديدة للمعلومات والاتصالات تتطور باستمرار لتقديم إمكانات جديدة .ويتمثل عملنا في تطوير نظام التشفير لعميل البريد الإلكتروني في الإنترنت، كما يسمح بالتواصل الجيد و الآمن بين الشركات والأفراد .للقيام بذلك، قمنا بتصميم عميل بريد إلكتروني يسمح بتشفير الرسائل الصادرة وفك تشفير الرسائل الواردة ، وذلك باستخدام تقنية PGP مع بعض التحسينات .وقد تم التصميم بواسطة لغة التمثيل UML. كما تمت البرمجة بواسطة لغة السي شارب في محيط العمل فيجول ستوديو2010.

الكلمات المفتاحية :التشفير، البريد الإلكتروني، تشفير البريد الإلكتروني ، خوارزميات التشفير، بروتوكولات البريد الإلكتروني، UML.