|  |  |
| --- | --- |
|  | **SIGLE DU COURS** |
| Titre du cours |
| ***Série A, B, C ou D, etc., s’il y a lieu*** |

**Travail noté**

Titre du travail (Pondération)

|  |
| --- |
| ■ Remplissez soigneusement cette feuille d’identité.  ■ Rédigez votre travail, en commençant à la page suivante.  ■ Sauvegardez votre travail de cette façon : SIGLEDUCOURS\_TN1\_VOTRENOM.  ■ Utilisez le *Dépôt des travaux* pour acheminer votre travail à votre professeur ou son délégué. <http://www.teluq.ca/mateluq/> |

Feuille d’identité

Nom       Prénom

Numéro d’étudiant       Trimestre

Adresse

      Code postal

Téléphone Domicile       Travail

Cellulaire

Courriel

Nom du professeur ou son délégué

**Réservé à l’usage du professeur ou son délégué**

Date de réception       Date de retour

Note

Date d’envoi

Projet de fin d’études - Implémentation et comparaison des algorithmes de chiffrage asymétrique

Le présent projet de fin d’études vise à montrer l’efficacité et l’efficience de l’implémentation des trois algorithmes de chiffrement et de déchiffrement asymétriques nommés RSA (Ron Rivest, Adi Shamir et Leonard Adleman), El-Gamal et ECC (Elliptic Curve Cryptography), afin de fournir et offrir des solutions à certains problèmes que surviennent en général, lorsque l’on implémente, en un langage de programmation donné (C, C#, C++, Java, Python etc.), ces trois algorithmes déjà mentionnés ci-dessus.

Afin de satisfaire à cet objectif général, global et primaire, Gonzalo Alfredo Romero Francia a décidé de concevoir la planification de la réalisation de toutes les tâches de toutes les étapes de réalisation du projet qu’il a choisi de réaliser, dans le cadre de la réalisation de son cours INF 1430, ce projet est le projet nommé « Implémentation et comparaison des algorithmes de chiffrage asymétrique ».

Afin de réaliser le projet nommé ci-dessus avec efficacité et efficience, et sans subir aucun retard ni aucun problème de réalisation de ce projet qui pourrait compromettre la réussite de la réalisation de ce projet, Gonzalo Alfredo Romero Francia a conçu, avec une énorme facilité, la planification de la réalisation se son projet nommé « Implémentation et comparaison des algorithmes de chiffrage asymétrique » suivante :

* Phase 1: faire des recherches sur Internet, sur les algorithmes de chiffrement asymétrique RSA, El-Gamal et ECC.
* Phase 2: me familiariser avec la théorie et les notions qu'utilisent ces trois algorithmes de chiffrement asymétrique, sous le plan purement théorique (lecture de pages web et visionnement de vidéos).
* Phase 3: me familiariser avec la théorie et les notions qu'utilisent ces trois algorithmes de chiffrement asymétrique, sous le plan purement mathématique et informatique (modélisation des formules et équations utilisées par ces trois algorithmes de chiffrement asymétrique en utilisant le logiciel Maple 2024, que je vais acheter prochainement).
* Phase 4: commencer à implémenter ces trois algorithmes de chiffrement asymétrique, tout en implémentant avec C++, chacune des formules et équations que ces trois algorithmes utilisent, tant pour chiffrer que pour déchiffrer des messages variés.
* Phase 5: Terminer la programmation de l'implémentation des algorithmes RSA, El-Gamal et ECC, pour rendre les 3 programmes C++ en version finale.
* Phase 6: réaliser des mesures de performance à ces trois algorithmes de chiffrement asymétrique, en utilisant plusieurs critères qui seront déterminées par moi prochainement.
* Phase 7: rédiger le document Word nécessaire pour montrer le résultat de l'implémentation de ces 3 algorithmes, ainsi que les résultats obtenus.

Gonzalo Alfredo Romero Francia, l’auteur du présent document, va fournir des informations et des explications sur la forme de réalisation des tâches associées à chacune des phases de la planification de son projet de fin d’études déjà montré ci-dessus. Commençons par la réalisation de toutes les tâches de la phase 1, qui sont les suivantes :

1a. Réalisation de recherches d’informations générales sur la théorie associée à l’algorithme RSA, sans mettre de l’accent sur théorie mathématique associée à cet algorithme.

1b. Réalisation de recherches d’informations générales sur la théorie associée à l’algorithme RSA, tout en mettant l’accent sur théorie mathématique associée à cet algorithme.

1c. Réalisation de recherches de pages web montrant comment réaliser, de manière générale et pas très détaillée, à l’aide d’exemples simples de calcul associés au chiffrement et déchiffrement RSA, les calculs mathématiques permettant d’obtenir les nombres premiers qui permettent de créer les clés publiques et privées utilisées par l’algorithme RSA.

1d. Réalisation de recherches de pages web montrant comment réaliser, de manière générale et pas très détaillée, à l’aide d’exemples complexes de calcul associés au chiffrement et déchiffrement RSA, les calculs mathématiques permettant d’obtenir les nombres premiers qui permettent de créer les clés publiques et privées utilisées par l’algorithme RSA.

1e. Réalisation d’un exercice théorique associé à la création des nombres premiers utilisés pour créer les clés publiques et privées, à la création de clés publiques et privées, et à la réalisation du processus de chiffrement et de déchiffrement de messages clairs et pleins quelconques, pour l’algorithme RSA.

1f. Réalisation de recherches d’informations générales sur la théorie associée à l’algorithme El-Gamal, sans mettre de l’accent sur théorie mathématique associée à cet algorithme.

1g. Réalisation de recherches d’informations générales sur la théorie associée à l’algorithme El-Gamal, tout en mettant l’accent sur théorie mathématique associée à cet algorithme.

1h. Réalisation de recherches de pages web montrant comment réaliser, de manière générale et pas très détaillée, à l’aide d’exemples simples de calcul associés au chiffrement et déchiffrement El-Gamal, les calculs mathématiques permettant d’obtenir les nombres premiers qui permettent de créer les clés publiques et privées utilisées par l’algorithme El-Gamal.

1i. Réalisation de recherches de pages web montrant comment réaliser, de manière générale et pas très détaillée, à l’aide d’exemples complexes de calcul associés au chiffrement et déchiffrement El-Gamal, les calculs mathématiques permettant d’obtenir les nombres premiers qui permettent de créer les clés publiques et privées utilisées par l’algorithme El-Gamal.

1j. Réalisation d’un exercice théorique associé à la création des nombres premiers utilisés pour créer les clés publiques et privées, à la création de clés publiques et privées, et à la réalisation du processus de chiffrement et de déchiffrement de messages clairs et pleins quelconques, pour l’algorithme El-Gamal.

1k. Réalisation de recherches d’informations générales sur la théorie associée à l’algorithme ECC, sans mettre de l’accent sur théorie mathématique associée à cet algorithme.

1l. Réalisation de recherches d’informations générales sur la théorie associée à l’algorithme ECC, tout en mettant l’accent sur théorie mathématique associée à cet algorithme.

1m. Réalisation de recherches de pages web montrant comment réaliser, de manière générale et pas très détaillée, à l’aide d’exemples simples de calcul associés au chiffrement et déchiffrement El-Gamal, les calculs mathématiques permettant d’obtenir les nombres premiers qui permettent de créer les clés publiques et privées utilisées par l’algorithme ECC.

1n. Réalisation de recherches de pages web montrant comment réaliser, de manière générale et pas très détaillée, à l’aide d’exemples complexes de calcul associés au chiffrement et déchiffrement El-Gamal, les calculs mathématiques permettant d’obtenir les nombres premiers qui permettent de créer les clés publiques et privées utilisées par l’algorithme ECC.

1o. Réalisation d’un exercice théorique associé à la création des nombres premiers utilisés pour créer les clés publiques et privées, à la création de clés publiques et privées, et à la réalisation du processus de chiffrement et de déchiffrement de messages clairs et pleins quelconques, pour l’algorithme ECC.

Afin de réaliser toutes les tâches montrées ci-dessus, Gonzalo Alfredo Romero Francia a réalisé des tas de recherches d’informations sur les algorithmes RSA, El-Gamal et ECC, et il a trouvé des tas de pages web lui enseignant tout sur les théories mathématiques associées à ces trois algorithmes de chiffrement et de déchiffrement asymétrique, le voici la bibliographie montrant toutes les pages web qu’il a trouvés sur Internet, et qu’il a utilisés, pour étudier en profondeur toutes les informations qu’il a trouvées sur les algorithmes RSA, El-Gamal et ECC :

Les algorithmes cryptographiques asymétriques, <https://slideplayer.fr/slide/3260205/>, ISIMA 2014.

La cryptographie , <https://www.mcours.net/cours/pdf/hassbg/hassbgli837.pdf>

La Cryptographie à base des Courbes Elliptiques : Étude Comparative, <http://dspace.univ-jijel.dz:8080/xmlui/bitstream/handle/123456789/12836/Inf.ILM.08-22.pdf?sequence=1>

Professeur Taoufik Serraj, Notes de Cours de Cryptographie, <https://espace-fpn.ump.ma/ftp/etudiants/Cours%20PRT%2020-21/CryptoSMA6%20-%20SERRAJ%20Taoufik.pdf>

Wikipédia, Algorithme d'Euclide étendu,

https://fr.wikipedia.org/wiki/Algorithme\_d%27Euclide\_%C3%A9tendu

Wikipédia, Chiffrement RSA, https://fr.wikipedia.org/wiki/Chiffrement\_RSA

Wikipédia, Inverse modulaire, <https://fr.wikipedia.org/wiki/Inverse_modulaire>

|  |  |
| --- | --- |
|  | Cryptographie moderne > Chiffrement par bloc à clé publique RSA > Démonstration 2/2, |

https://www.hds.utc.fr/~wschon/sr06/crypto/RSA4\_2.htm

Exponentiation rapide, <https://www.labri.fr/perso/betrema/deug/poly/exp-rapide.html>

Cryptographie, https://www.labri.fr/perso/betrema/deug/poly/crypto.html

RSA, A. Dragut, Univ. Aix-Marseille Cours de cryptographie Chapitre III, https://pageperso.lis- lab.fr/andreea.dragut/enseignementCLAA/CryptoChap3RSA2012.pdf

Cryptographie par RSA, <https://www.irif.fr/~emiquey/TP/tp5.pdf>

Introduction à la cryptographie - TP 1, RSA,

https://people.irisa.fr/Jeremy.Metairie/teaching/intro\_crypto/rsa.pdf

Cryptographie asymétrique et courbes elliptiques, Culture Math, https://culturemath.ens.fr/thematiques/lycee/cryptographie-asymetrique-et-courbes-elliptiques

RSA, <https://ataraxy.info/Crypto?Chapitres/RSA>

Cryptographie à clef publique Cours 2, https://lvzl.fr/teaching/2020-21/docs/CP-slides-2.pdf

Introduction au chiffrement asymétrique ElGamal, https://lab.yvesago.net/2015/11/Introduction-au-chiffrement-asymetrique-ElGamal.html

Andreea Dragut (dragut@univmed.fr) Cours de cryptographie Chapitre IV, ELGamal, https://pageperso.lis-lab.fr/andreea.dragut/enseignementCLAA/CryptoChap4ElGamal2012.pdf

Tbowan, ElGamal encryption, <https://www.arsouyes.org/blog/2018/01_ElGamal/>

Anca Nitulescu, Ecole Normale Supérieure, Paris, <https://www.di.ens.fr/~nitulesc/files/crypto4.pdf>

Le système d'ElGamal, <https://igm.univ-mlv.fr/~jyt/Crypto/5/elgamal.html>

Cécile Pierrot, Chargée de Recherche INRIA Nancy, Introduction `a la Cryptographie 6. Cryptographie asymétrique (2), https://members.loria.fr/CPierrot/papers/Telecom\_cours\_06.pdf

LES TECHNIQUES DE CHIFFREMENT ET LEUR ÉVOLUTION Étude du chiffrement El Gamal, https://www-complexnetworks.lip6.fr/~tarissan/enum/2022/Chiffrement-2022-Guyot.pdf

Cryptosystème de ElGamal, De Wikipedia, l'encyclopédie libre, https://www.wikiwand.com/fr/Cryptosyst%C3%A8me\_de\_ElGamal

Hakima Ould-Slimane, École de technologie supérieure (ÉTS) Département de génie électrique ,Cryptographie à clé publique, https://cours.etsmtl.ca/mgr850/documents/cours/Hiver2014/MGR850\_H14\_Cours-06\_cryptoAsym.pdf

Propriétés du chiffrement ElGamal, https://lab.yvesago.net/2015/12/Proprietes-du-chiffrement-ElGamal.html

[Documentation Crypto M1 MIC 2020-2021](https://webusers.imj-prg.fr/~pascal.molin/cours/crypto/index.html), https://webusers.imj-prg.fr/~pascal.molin/cours/crypto/cours\_logdiscret.html#:~:text=Calcul%20d'indice,g%3D11%20g%3D11.

Wikipédia, Logarithme discret, https://fr.wikipedia.org/wiki/Logarithme\_discret

Chiffre RSA, [Cryptographie](https://www.dcode.fr/liste-outils#cryptography), [Cryptographie Moderne](https://www.dcode.fr/liste-outils#modern_cryptography), [Chiffre RSA](https://www.dcode.fr/chiffre-rsa), <https://www.dcode.fr/chiffre-rsa>

Algorithme d'Euclide Étendu**,** [Mathématiques](https://www.dcode.fr/liste-outils#mathematics), [Arithmétique](https://www.dcode.fr/liste-outils#arithmetics), [Algorithme d'Euclide Étendu](file:///C:\Users\Gonzalo%20Alfredo\Downloads\Algorithme%20d'Euclide%20Étendu), <https://www.dcode.fr/euclide-etendu>

Décomposition en Nombres Premiers, [Mathématiques](https://www.dcode.fr/liste-outils#mathematics), [Arithmétique](https://www.dcode.fr/liste-outils#arithmetics), [Décomposition en Nombres Premiers](https://www.dcode.fr/decomposition-nombres-premiers), <https://www.dcode.fr/decomposition-nombres-premiers>

WIKIMATH, [EL GAMAL](https://cours-info.iut-bm.univ-fcomte.fr/pmwiki/pmwiki.php/Crypto/ElGamal), LE CHIFFREMENT D'EL GAMAL, https://cours-info.iut-bm.univ-fcomte.fr/pmwiki/pmwiki.php/Crypto/ElGamal

Judicaël Courant Lycée La Martinière-Monplaisir, Lyon Conférence Algorithmique et Programmation CIRM Le 6 mai 2016, Application de la complexité en cryptographie, <https://www.cirm-math.fr/ProgWeebly/Renc1446/Courant.pdf>

[SYNETIS](https://www.synetis.com/), [SÉCURITÉ](https://www.synetis.com/category/securite/), [NOTIONS DE CRYPTOLOGIE ET ALGORITHME DE CHIFFREMENT](https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/), <https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/>

Cryptosystème de ElGamal, <https://www.slideshare.net/AyoubSIAHMED/cryptosystme-de-elgamal>

Gabriel Chênevert, Département d’Informatique et Mathématiques Appliquées, ISEN Lille, Association mathématique du Québec, Conférence plénière Dimension algorithmique et chiffrement post-quantique, <https://www.amq.math.ca/wp-content/uploads/bulletin/vol59/no3/05-V2-bull.pdf>

Keeper Security, Qu’est-ce que la cryptographie à courbe elliptique ?, <https://www.keepersecurity.com/blog/fr/2023/06/07/what-is-elliptic-curve-cryptography/#:~:text=La%20cryptographie%20%C3%A0%20courbe%20elliptique%20(ECC)%20est%20une%20forme%20de,signatures%20num%C3%A9riques%20et%20le%20chiffrement>,  7 juin 2023

Wikipédia, Cryptographie sur les courbes elliptiques, <https://fr.wikipedia.org/wiki/Cryptographie_sur_les_courbes_elliptiques>

Thibaut Probst, Découvrir les courbes elliptiques en cryptographie, <https://thibautprobst.fr/posts/elliptic-curves/>, 7 mai 2023

Wikipédia, Addition dans le cadre de la théorie des Courbes Elliptiques, https://fr.wikipedia.org/wiki/Addition#Propri.C3.A9t.C3.A9s

Wikipédia, Modular multiplicative inverse, https://en.wikipedia.org/wiki/Modular\_multiplicative\_inverse

Thibault Jouannic, [Un peu de crypto avec les courbes elliptiques](https://www.miximum.fr/blog/cryptographie-courbes-elliptiques-ecdsa/), <https://www.miximum.fr/blog/cryptographie-courbes-elliptiques-ecdsa/>, 17 juin 2014

Marie Lesty, Courbes elliptiques : un nouveau virage pour le chiffrement, <https://www.01net.com/actualites/courbes-elliptiques-un-nouveau-virage-pour-le-chiffrement-143980.html>, 26 mars 2001

Simon Blake-Wilson, Daniel R. L. Brown, Certicom Corp, P. Lambert, Cosine Communications, Groupe de travail Réseau, Traduction Claude Brière de L'Isle, Utilisation des algorithmes de cryptographie de courbe elliptique (ECC) dans la syntaxe de message cryptographique (CMS), <http://abcdrfc.free.fr/rfc-f/rfc3278.html#_Toc218773833>, avril 2002

[Tania Martin](https://www.smalsresearch.be/author/martin/), [Smals Research](https://www.smalsresearch.be/), Elliptic Curve Cryptography for dummies 1: introduction, <https://www.smalsresearch.be/elliptic-curve-cryptography-tutoriel1/>, 25 février 2015.

nina.az, Cryptographie sur les courbes elliptiques, https://www.wikidata.fr-fr.nina.az/Cryptographie\_sur\_les\_courbes\_elliptiques.html

[Hervé LEHNING, agrégé de mathématiques](https://blogs.futura-sciences.com/lehning/), [CRYPTOLOGIE](https://blogs.futura-sciences.com/lehning/category/sciences/cryptologie/), [MATHÉMATIQUES](https://blogs.futura-sciences.com/lehning/category/maths-2/)

COMMENT PEUT-ON CHIFFRER AVEC UNE COURBE ?, <https://blogs.futura-sciences.com/lehning/2019/01/11/comment-peut-on-chiffrer-avec-une-courbe/>, 11 janvier 2019

Valentine A**.**, Chercheure chez Gate.io (page web), Cryptographie à courbe elliptique, <https://www.gate.io/fr/blog_detail/782/elliptic-curve-cryptography>.

Tania Martin, Consultante Recherche chez Smals Research, Elliptic Curve Cryptography for dummies 2: en pratique pour la cryptographie, <https://www.smalsresearch.be/elliptic-curve-cryptography-tutoriel2/>, 12 août 2015

Abdelouahid BEN TAMOU, hamza noursaid, Cryptography, Elliptic Curve Cryptography, Rapport sur les cryptosystèmes utilisant les courbes elliptiques en Tifinagh, https://www.academia.edu/11513925/Rapport\_sur\_les\_cryptosyst%C3%A8mes\_utilisant\_les\_courbes\_elliptiques\_en\_Ti\_finagh

INTChain French Community, Cryptographie sur les Courbes Elliptiques, <https://medium.com/int-chain-fr/cryptographie-sur-les-courbes-elliptiques-74878e5905ca>, 30 juin 2019

Engue Gillier, Ingénieur Sécurité chez Facebook,

[Sécurisez vos données avec la cryptographie, Utilisez le chiffrement asymétrique, https://openclassrooms.com/fr/courses/1757741-securisez-vos-donnees-avec-la-cryptographie/6031872-utilisez-le-chiffrement-asymetrique, 3 janvier 2024](file://C:\\Users\\Gonzalo Alfredo\\Downloads\\Sécurisez vos données avec la cryptographie, Utilisez le chiffrement asymétrique, https:\\openclassrooms.com\\fr\\courses\\1757741-securisez-vos-donnees-avec-la-cryptographie\\6031872-utilisez-le-chiffrement-asymetrique, 3 janvier 2024)

AVI Networks, Elliptic Curve Cryptography, Elliptic Curve Cryptography Definition, <https://avinetworks.com/glossary/elliptic-curve-cryptography/>, année 2024

Cédric Murdica. Physical security of elliptic curve cryptography. Cryptography and Security [cs.CR]. Télécom ParisTech, 2014. English. ffNNT : 2014ENST0008ff. fftel-01179584

D. Sravana Kumar, CH. Suneetha, A. ChandrasekhAR, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 DOI : 10.5121/ijdps.2012.3125 301 ENCRYPTION OF DATA USING ELLIPTIC CURVE OVER FINITE FIELDS, <https://arxiv.org/ftp/arxiv/papers/1202/1202.1895.pdf>, Janvier 2012

n software, IPWorks Encrypt 2020 C++ Edition, ECC Class, <https://cdn.nsoftware.com/help/IEF/cpp/ECC.htm>

Crypto Stack Exchange Forum, Cryptography, [521-bit ECC keys are the same strength as RSA 15,360-bit keys](https://crypto.stackexchange.com/questions/79944/521-bit-ecc-keys-are-the-same-strength-as-rsa-15-360-bit-keys), <https://crypto.stackexchange.com/questions/79944/521-bit-ecc-keys-are-the-same-strength-as-rsa-15-360-bit-keys>, 2021

Renaud Dumont, Université de Liège Faculté des Sciences Appliquées, Cryptographie et Sécurité informatique INFO0045-2, Notes de cours provisoires 2009 – 2010, https://doc.lagout.org/security/Crypto/2010\_cours\_crypto.pdf

Awouzouba Esso-Essinam, Cours cryptographie, Gran guru Computador, Magister Informatica, <https://www.slideshare.net/KarlAwouzouba/cours-cryptographie>, 1 décembre 2017

[Alegsaonline.com](https://fr.alegsaonline.com/) - [Effet avalanche](https://fr.alegsaonline.com/art/7672) - Leandro Alegsa - 2021-05-09 21:13:44 - url: https://fr.alegsaonline.com/art/7672

Geeks for Geeks page web (<https://www.geeksforgeeks.org>), Avalanche Effect in Cryptography, <https://www.geeksforgeeks.org/avalanche-effect-in-cryptography/>,14 Mars 2022

Freeman Law page web (<https://freemanlaw.com/>), WHAT YOU NEED TO KNOW ABOUT THE “AVALANCHE” EFFECT, THE CRITERIA OF THE STRICT AVALANCHE EFFECT, <https://freemanlaw.com/what-you-need-to-know-about-the-avalanche-effect/>, année 2022

[Satish Kumar](https://www.tutorialspoint.com/authors/satish-kumar-166980035458), [Computer Network](https://www.tutorialspoint.com/articles/category/Computer-Network), [Digital Signature](https://www.tutorialspoint.com/articles/category/digital-signature), [Cryptography](https://www.tutorialspoint.com/articles/category/cryptography), Avalanche Effect in Cryptography, <https://www.tutorialspoint.com/avalanche-effect-in-cryptography>, 6 Février 2023

Affan Malik, page web educative.io (<https://www.educative.io/>), What is the avalanche effect?, <https://www.educative.io/answers/what-is-the-avalanche-effect>, année 2024