13262 BAHOUS Youness

La sécurisation des messages à l'aide de la cryptographie sur les courbes elliptiques

J'ai rencontré sur internet une publicité d'une application de messagerie qui proposa un chiffrement bout à bout de l'information , ceci m'as mené à questionner le déroulement d'un tel procédé, et comme étant passionné par l'informatique et l'algorithmique, j'ai choisi ce sujet pour mon TIPE.
La confidentialité des données, au sens large, à l'ère numérique repose sur l'incarnation moderne de l'art ancien des codes et des chiffres la cryptologie , cette branche de mathématiques qui assure la sureté des échanges du commerce électronique, les communications sensibles, réseaux mobiles.

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique), INFORMATIQUE (Informatique Théorique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Cryptographie	*Cryptography*
Logarithme discret	*Discrete Logarithm*
Codage	*Encoding*
Courbe elliptique	*Elliptic curve*
Chiffrement de bout en bout	*End-to-end encryption*

Bibliographie commentée

Autrefois utilisée que par l'armée et les services secrets, **la cryptographie** protège désormais les documents des industriels voire des particuliers. L'un de ses buts, comme son nom l'indique (crypto- signifie cacher et -graphie est un suffixe référant à l'écriture), est de stocker ou d'échanger des informations avec un groupe restreint de personnes tout en empêchant à d'autres d'y avoir accès. [1]

Le chiffrement de bout en bout consiste à chiffrer les messages sur un dispositif pour que seul le destinataire puisse le déchiffrer. Le message effectue tout le voyage entre l'expéditeur et le destinataire sous forme chiffrée. Assurant ainsi la confidentialité des échanges.

Tous les codes et chiffrements reposaient sur l'hypothèse que les personnes essayant de communiquer, ont préalablement partagé une clé secrète , sans laquelle le cryptage / décryptage est impossible' que leur adversaire ne possédait pas. cependant , on a abouti à des méthodes dites à clé publique permettant d'échapper à cette exigence, ce concept généralement attribué à Whitfield Diffie et à Martin Hellman qui l'ont présenté au public à la
National Computer Conférence en 1976 [5] qui ont même présenté un procédé d'échange de clés basé sur le problème du logarithme discret .

Le Problème du logarithme discret est un problème mathématique qui apparaît dans plusieurs formes , tel que le modulo arithmétique sur lequel le cyptosystème de **RSA** proposé par le trio Rivest ,Shamir et Adleman s'est basé pour résoudre le problème de Diffie-Hellman qui est

vastement utilisé aujourd'hui dans les télécommunications ,ainsi que le procédé d'échange de clés fondé sur la théorie des les courbes elliptiques sur un corps fini (**ECC**) qui a été suggéré, de manière indépendante, par Neal Koblitz et Victor S. Miller en 1985.[4]
Cependant ces méthodes ne s'avèrent utiles que si les données à transmettre sont formalisées , pour être manipulables par la machine (des entiers ou des points sur une courbe elliptiques) un codage préalable est donc nécessaire , et ceci est possible grâce à **ASCII** *(The American Standard Code for Information Interchange)*, qui permet de coder chaque caractère alphanumérique sur un nombre de 0 à 2^8 et à la la méthode de codage de Koblitz qui permet de coder un message sur une courbe elliptique.[3]

Problématique retenue

Comment utiliser la cryptographie à courbes elliptiques pour assurer une sécurité bout à bout des messages textuels à travers un canal de communication ?

Objectifs du TIPE

Je me propose d'utiliser une suite d'algorithmes se basant sur la théorie des courbes elliptiques pour modéliser un chiffrement bout à bout d'un texte .(dès la sa rédaction par l'émetteur à la lecture par le récepteur) et ceci en suivant les étapes :

1- Codage du texte rédigé par l'émetteur sur une courbe par **la méthode de Koblitz**
2- Echange de clés (Authentification) l'aide de **l'échange de Massey-Omura.**
3- Envoi du message.
4- Décodage des données reçues.
et proposer une implémentation à l'aide du langage de programmation PYTHON.

Références bibliographiques (ETAPE 1)

[1] Jeffrey Hoffstein : An introduction to mathematical cryptograph : *Elliptic Curves and Discrete Logarithm chapters*

[2] Padma Bh, D.Chandravathi , P.Prapoorna Roja : Message Security on Chat App based on Massey Omura Algorithm : *International Journal Of Information System & Technology Vol. 1, No. 2, (2018), pp. 16-23*

[3] Padma Bh, D.Chandravathi , P.Prapoorna Roja : Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method : *International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1904-1907*

[4] Neal Koblitz : Elliptic curve cryptosystems : *Mathematics of computation 48 (1987), 203-209*

[5] W. Diffie et M. Hellman : New directions in cryptography : *IEEE Transactions on Information Theory (Volume: 22, Issue: 6, Nov 1976)*

[6] WhatsApp : Sécurité sur WhatsApp : *https://www.whatsapp.com/security/*

[7] Menezes, A.; VanOorschot, P.; Vanstone, S. . : (1996). Handbook of Applied Cryptography : *pp. 500, 642.*

DOT

[1] *Novembre 2020 :Choix du sujet suite à la lecture d'un article proposée par le service de messagerie Whatsapp expliquant le niveau de confidentialité qu'il offre à ses utilisateurs*

[2] *Décembre 2020 et Janvier 2021: recherches bibliographiques permettant la mise en oeuvre théorique et pratique d'une chaine d'algorithmes permettant de chiffrement de bout en bout en s'inspirant des travaux de Padma Bh*

[3] *Fevrier 2021: Lecture de cours d'algèbre présentant les courbes elliptiques et mise en place de la classe de fonctions permettant la manipulation des points sur courbes elliptiques*

[4] *Mars 2021: Rédaction des algorithmes d'encodage numérique et elliptique et premiers tests*

[5] *Avril 2021: Approfondissement sur les méthodes d'authentification en particulier celle de Massey Omura , et rédaction de code informatique associé , J'ai retrouvé initialement des problèmes lors des tests*

[6] *Mai 2021: Décision d'utiliser SageMath , pour simuler l'opération de transmission de messages puis Rédaction de la présentation et de l'Mcot*