Mise en place d'un cryptosystème d'ELgamal sur les courbes elliptiques et étude de sa sécurité.

De nos jours, nos informations personnelles sont plus sujettes à être hébergées par des sociétés privées, c'est pourquoi je trouve l'insécurité de celles-ci de plus en plus préoccupante. J'ai donc voulu mieux comprendre comment nos communications restent privées mais aussi à quel point les protocoles de cryptage sont fiables.

Pour mettre en œuvre le procédé de cryptographie d'Elgamal, nous avons besoin de construire un groupe cyclique dans lequel le calcul de logarithme est difficile. De plus pour attaquer notre chiffrement, nous utilisons l'algorithme rho de Pollard qui cherche un cycle dans les valeurs d'une suite récurrente.

Le candidat atteste avoir travaillé en monôme.

Positionnement thématique (ÉTAPE 1) :

- INFORMATIQUE (Informatique pratique)
- MATHEMATIQUES (Mathématiques Appliquées)
- MATHEMATIQUES (Algèbre)

Mots-clés (ÉTAPE 1) :

Mots-clés (en français)	**Mots-clés (en anglais)**
Cryptographie	*Cryptography*
Courbes elliptiques	*Elliptic curves*
Logarithme discret	*Discrete logarithm*
Cryptanalyse	*Cryptanalysis*
Calcul numérique	*Numerical computation*

Bibliographie commentée

De par l'essor des échanges d'information sensible qu'a apporté l'ère numérique, la cryptographie s'est révélée être un domaine essentiel à la sécurité des communications. De plus, chiffrement et déchiffrement se doivent d'être rapides et peu coûteux à mettre en place.

Le cryptosystème d'Elgamal, introduit en 1984 par Taher Elgamal [1], est un protocole de cryptographie asymétrique largement utilisé et construit dont la sécurité repose sur la difficulté du logarithme discret [2]. Cet algorithme permet à deux parties d'échanger un message de manière sécurisée en utilisant une paire de clés : une clé publique et une clé privée qui servent respectivement à chiffrer le message et à le déchiffrer.

Les meilleurs algorithmes connus pour résoudre le problème du logarithme discret sur les corps de nombres tels que le crible généralisé ont une complexité sous-exponentielle par rapport à la longueur des clés en bits [3], tandis que les meilleurs algorithmes connus pour les groupes construits sur les courbes elliptiques [4] , comme l'algorithme de rho de Pollard [5] , ont une complexité exponentielle.

C'est pourquoi en 2005 la National Security Agency (NSA) des États-Unis a recommandé l'utilisation de courbes elliptiques pour les systèmes de cryptographie à clé publique, soulignant leur efficacité et leur sécurité accrues par rapport aux méthodes traditionnelles [6].

Le principe du chiffrement par la méthode d'ElGamal repose sur la difficulté du problème du logarithme discret : calculer g^x mod p où g est un générateur et p un nombre premier et rapide mais retrouver x à partir de g^x mod p en connaissant g et p est très difficile. Dans le cadre des courbes elliptiques, le groupe cyclique (fini et monogène) sur lequel on applique ce problème est construit à partir de points d'une courbe elliptique sur un corps fini. Cette courbe est une partie du plan projectif dans lequel les calculs sont aisés.

Une première approche pour casser ce codage serait d'essayer toutes les valeurs possibles de la clé privée jusqu'à trouver la bonne, d'opérer en force brute. Cependant, la taille des clés utilisées dans les systèmes modernes rend cette approche impraticable car le nombre de possibilités serait astronomique. Pour des clés de 256 bits, il y aurait 2^256 possibilités, ce qui est bien au-delà de la capacité de calcul de n'importe quel ordinateur.

Pour réduire les temps de calcul au maximum, nous allons nous intéresser à l'algorithme dit du "rho de Pollard" [7] qui est un algorithme probabiliste qui repose sur le paradoxe des anniversaires [8] et de la détection de cycles dans une suite récurrente. Il est nettement plus efficace que la force brute pour résoudre le problème du logarithme discret, il permet de trouver la clé privée en un temps proportionnel à 2^(k/2) où k est le nombre de bits de la clé, il offre donc une complexité exponentielle. Nous allons donc étudier la sécurité de ce cryptosystème en jouant le rôle d'un attaquant qui cherche à retrouver le message chiffré, en comparant le temps que nous mettons à résoudre ce problème mathématique avec plusieurs algorithmes.

Cependant, il est important de noter que la sécurité de ce cryptosystème sera compromise quand des ordinateurs quantiques suffisamment puissants seront développés, car ils pourraient résoudre le problème du logarithme discret en temps polynomial grâce à l'algorithme de Shor.

Pour conclure, les courbes elliptiques offrent une sécurité supplémentaire comparée aux groupes cycliques usuels utilisés dans le cryptosystème originel d'Elgamal. Leur structure mathématique

complexe et leur mise en place relativement aisées offrent une solution de cryptographie robuste et efficace, adaptée à l'échange de clés de sécurité dans des contextes de confidentialité très variés.

Problématique retenue

En quoi les courbes elliptiques sont des objets mathématiques indispensables à la cryptographie moderne ?

Objectifs du TIPE du candidat

- Construction de groupes cycliques sur les courbes elliptiques.

- Etude et mise en place du cryptosystème d'El Gamal sur les courbes elliptiques.

- Comparaison de différents algorithmes de résolution du problème du logarithme discret.

Références bibliographiques (ÉTAPE 1)

[1] TAHER ELGAMAL : A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *: Advances in Cryptology – CRYPTO 1984,p10-18. https://doi.org/10.1007/3-540-39568-7_2*

[2] LE GLUHER (A) : Problème du logarithme discret appliqué à la cryptanalyse sur courbes elliptiques : algorithme MOV. *: 22 août 2015. p3-4*

[3] BOUDOT (F), GAUDRY (P), GUILLEVIC (A), HENINGER (N), THOMÉ (E) : Nouveaux records de factorisation et de calcul de logarithme discret. *: Techniques de l' Ingénieur, 2021.*

[4] BLAKE (I.F), SEROUSSI (G), SMART (N) : Elliptic Curves in Cryptography. *: London Mathematical Society Lecture Notes Series 265, Cambridge University Press, 1999. p30-38*

[5] MENEZES (A), VAN OORSCHOT (P), VANTSONE (S) : Handbook of Applied Cryptography. *: 1996. chapitre 3, p91-92*

[6] NATIONAL SECURITY AGENCY (NSA) : Suite B Cryptography *: 2005. https://web.archive.org/web/20150815072948/https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml - janvier 2026*

[7] J. M. POLLARD : MATHEMATICS OF COMPUTATION, Monte Carlo Methods for Index Computation (mod p) *: volume 32, juillet 1978, p918-924*

[8] BIBMATH : Le paradoxe des anniversaires *: https://www.bibmath.net/dico/index.php?action=affiche&quoi=./a/anniversaire.html -janvier 2026*