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

De part la réduction de l'anonymat et sur internet, je trouve la sécurité de nos données personnelles de plus en plus préoccupante. J'ai donc voulu mieux comprendre comment nos communications restent privées mais aussi à quel point ces protocoles de cryptage sont fiables.

Pour construire le problème de cryptographie d'ElGamal, nous avons besoin de construire un groupe cyclique car le calcul de logarithme sur ces groupes 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 ces chiffrement et déchiffrement se doivent d'être rapides et peu coûteuses à mettre en place.

Un de ces systèmes, introduit en 1984 par Taher Elgamal [1], le cryptosystème d'ElGamal est un protocole de cryptographie asymétrique largement utilisé et construit sur le problème du