Sonny Klotz, **Idir Hamad**,
Younes BenYamna et **Malek Zemni**
Université de Versailles Saint-Quentin-En-Yvelines

Alex Gélin

Versailles, le 8 janvier 2018

Objet : candidature pour le projet de cryptographie «Logarithme Discret»

Monsieur,

Notre groupe, formé par les étudiants dont les noms sont cités ci-dessus, est motivé pour traiter le sujet du Logarithme Discret.

Tout d'abord pour nous présenter, nous pouvons dire que nous sommes étudiants à l'UVSQ depuis la licence, nous avons donc suivi le module cryptographie en L3 en addition du module de cryptopgraphie pour M1. Idir et Younes ont travaillé sur des sujets de cryptographie pour le projet de fin de licence (Cryptographie RSA et chiffrements par substitution respectivement) , et, trois des quatres membres du groupe (Idir, Malek et Younes) ont pour vocation de poursuivre avec un M2 Secrets. Voilà ce qui explique notre volonté de choisir un sujet portant sur la cryptographie.

Par ailleurs, en ce qui concerne notre aptitude à traiter le sujet, nous sommes familiers avec LaTeX et GMP. En effet, LaTeX est l'outil avec lequel nous avons écrit cette lettre, mais aussi, le module Cryptographie de licence nous a permis de découvrir la librairie GMP avec le développement des tests de primalité de Fermat et de Miller-Rabin en langage C.

Nous espérons avec ce sujet nous perfectionner et étendre notre culture sur des concepts clés (clé secrète lol) de la cryptographie.

Avec l'espoir de vous convaincre de notre enthousiasme, nous vous prions d'agréer, Monsieur, nos respectueuses salutations.

Cordialement.