

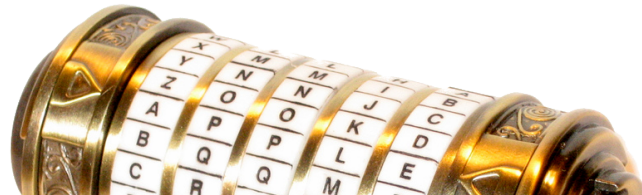


L'art d'encoder ses messages

Étudiants de deuxième année en bachelier en informatique

Depuis longtemps, les hommes ont voulu transmettre des informations secrètement, que ce soit pour lutter contre l'autorité ou pour des raisons militaires. À ces fins, deux solutions s'offrent aux protagonistes : soit cacher les messages, soit les rendre illisibles pour toute personne non autorisée. La première technique s'appelle la *stéganographie*, la deuxième la *cryptographie*.

Le stand de l'École Supérieure d'Informatique (ESI) présente les principes cryptographiques de base et permet au public de participer dans plusieurs ateliers interactifs. On y présente également la problématique de la *signature*, qui permet de s'assurer que l'expéditeur d'un message est bien celui qu'il prétend être.



Tout au long de l'exposé, diverses techniques de cryptographie seront exposées, ainsi que leur utilisation historique et leur conséquences potentiellement dramatiques. Plus particulièrement, les techniques de *scytales* et du *chiffrement de César* seront illustrées. Les participants seront également amenés à user d'astuce pour déchiffrer les codes qui seront proposés.

Pour les plus intéressés, une autre technique de chiffrement, le *chiffrement de Vigenère*, sera également exposé. Cette technique pallie les principaux défauts du chiffrement de César afin d'empêcher une lecture facile du texte chiffré. Encore une fois, les participants seront amenés à utiliser les techniques vues durant l'exposé afin de briser le code.

Finalement, les étudiants présentant le stand vous parleront de leur expérience au sein de l'école, des projets de programmation qu'ils sont amenés à implémenter, ainsi que des études qu'il est permis de suivre au sein de l'École Supérieure d'Informatique (ESI).