RÉSUMÉ DU PROJET « SUR LES TRACES D'ENIGMA »

Ce projet a été mené dans le cadre d'un atelier MATh.en.JEANS au lycée Maurice Genevoix d'Ingré, encadré par M. Grillot, enseignant-chercheur à l'Université d'Orléans, et Mme Rougerie, professeure de mathématiques.

Toutes les semaines, les séances ont réuni dix élèves de 1ère S et terminales (S et STI2D) du lycée :
Maxime Bausmayer, Marie Bernier, Thomas Cazajous, Julien Gleyze, Lucas Judeaux, Julien Lebeau, élèves de 1ère S
Imane El Kerrach (TS), Mathys Grandet (TS), Quentin Riffault (TSTI2D) et Benjamin Rojo (TS).

Le sujet général du cryptage a été imposé aux élèves de l'atelier en début d'année.

Étape 1 :
- Entrée dans le thème du cryptage et de la cryptanalyse par quelques jeux
- Découverte de quelques systèmes de codage, leurs forces et leurs faiblesses

Nous leur avons ensuite proposé de s'attaquer à la machine Enigma et ils ont choisi de s'engager dans ce projet.

Contexte historique :
Années 1930. Le nazisme s'impose peu à peu en Allemagne. Hitler est de plus en plus menaçant et revendique des territoires. L'armée allemande a un avantage de taille : elle dispose d'un système de cryptage réputé inviolable (il l'était encore à ce moment-là !) : *la* machine ENIGMA. Comprendre son fonctionnement, en déterminer les réglages et en fabriquer des répliques est dès lors devenu vital pour ces voisins européens…

À leur tour, en s'appuyant sur des documents techniques authentiques et avec les outils numériques d'aujourd'hui, les élèves de l'atelier ont étudié ces machines. Ils se sont employés à créer un programme informatique et à faire fonctionner une réplique électronique reproduisant le fonctionnement des vraies machines authentiques.

Étape 2 : Comprendre le fonctionnement d'une machine Enigma
- Réalisation d'une maquette papier simulant une version de base à partir de documents fournis (en anglais)
- Identification des éléments constituant la machine et des transformations successives opérées sur chaque lettre à partir de documents techniques et historiques fournis et complétés par leurs propres recherches.
- Modélisation de ces opérations sous forme algorithmique

Étape 3 : Constitution de 2 groupes
- Élaboration, par un premier groupe, d'un programme simulant le codage effectué par Enigma en langage Python et en langage C++ prenant en charge :
  - La rotation du rotor de « rapide »
  - Les connexions du tableau de fiches (en cours de finalisation)
  - Le choix de l'orientation initiale des rotors (en cours de finalisation)
  - La rotation des deux autres rotors (modélisation en cours)

- Adaptation en cours de ce programme au système électronique préparé par M. Séguret, professeur au lycée.

- Un groupe étudie la puissance de la machine par une analyse combinatoire des clés quotidiennes.

Réalisations et productions :
- Vidéo et diaporamas pour le concours CGénial ainsi que pour présentations lors d'un « évènement MATHS » au lycée et lors de nos portes ouvertes, participation au congrès MATh.en.JEANS de Poitiers (mars 2018).

- Programmes et machine électronique, articles pour publication sur le site de l'association MATh.en.JEANS.