Fiche récapitulative du projet d’ISN :

« Le codage RSA appliqué à un coffre »

Présentation du projet :

Le principe est assez simple : Guillaume souhaite être le seul à pouvoir ouvrir son coffre et ainsi récupérer le document confidentiel déposé à l’intérieur par un autre utilisateur Adrien. Pour cela, grâce à la brique Mindstorms n°1 (ou brique maitre), Guillaume va créer les clés publique et privée en rendant accessible uniquement la clé publique. Après que les deux clés aient été crées par Guillaume, son coffre étant près à l’utilisation, il s’en va. Adrien peut à tout venir et fermer le coffre à l’aide d’un code à trois chiffres en utilisant la brique Mindstorms n°1, après avoir déposé un document confidentiel à l’intérieur du coffre bien évidemment. Son code à trois chiffres est converti en sa correspondance ASCII par la machine, par exemple si le code choisi est 1 2 3 cela donne 49 50 51 puis il est chiffré grâce à la clé publique, rendu accessible par Guillaume. Le coffre fermé, Guillaume de retour veut récupérer le document confidentiel à l’intérieur. Pour cela il va utiliser sa brique Mindstorms n°2(ou brique esclave) où on été envoyé la clé privée et le code du coffre chiffré au préalable par Adrien grâce à sa clé publique. Il peut ainsi demander à la brique de déchiffrer à l’aide de sa clé privée le code transmis par Adrien au moyen de sa clé. Une fois le code déchiffré, il apparait à l’écran. Guillaume n’a plus qu’à le rentrer pour récupérer son document confidentiel !

Développement du projet:

Moyens : Pc avec Bricx Command Center (IDE permettant la programmation avec le langage NXC), pilote  [NXT Fantom](http://cache.lego.com/r/www/r/mindstorms/-/media/franchises/mindstorms%202014/downloads/firmware%20and%20software/nxt%20software/nxt%20fantom%20drivers.zip?l.r=717004469) assurant la connexion USB entre la brique programmable et le pc et Lego Mindstorms NXT.

Production : Un coffre en Lego Technic et deux programmes, un pour la brique maitre et un autre pour la brique esclave.

Description de la démarche collaborative dans le groupe :

Nous nous sommes répartis les tâches. La partie mathématique a surtout été vue par Guillaume. Adrien s’est chargé de la construction du robot. Une partie du programme a été vue en classe car certains points été assez délicats à traiter seul. Le reste a été fait chez nous en fonction du temps qu’on avait chacun.

Eléments de difficulté et perspectives de poursuite :

Nous avons rencontré certaines difficultés au cours de la réalisation de notre projet. Tout d’abord nous avons du nous familiariser avec le langage NXC. Ensuite, au niveau de la programmation, les difficultés ont surtout été du coté de l’envoi d’informations par connexion Bluetooth entre les deux briques. La construction du robot n’a pas trop posée de problème bien que le calibrage du degré de rotation du moteur lors de l’ouverture et la fermeture du coffre soit assez délicat à faire.

Enfin, bien que certaines choses puissent être améliorées, nous sommes satisfaits du résultat final. Pour perfectionner le projet, on pourrait rajouter certaines fonctions au robot comme par exemple un test de primalité ou bien même simplement optimiser le programme pour que le temps de calcul soit moins long.