Cryptris : Comprendre une des techniques les plus sophistiquées de cryptographie.

Mise en place du jeu : ce jeu est une activité encadrée, typiquement avec plusieurs joueurs et un animateur ; voici une démarche possible. Installer chaque joueur (ou par deux jouant à tour de rôle) devant le jeu et laisser jouer. Attendre que le joueur soit surpris de ce qui se passe, sinon susciter les interrogations en proposant les éléments de réponse dont on donne un exemple ici.

Utilisation en autonomie: il faut inviter le joueur à lire ce texte ou l'article explicatif mais il peut le faire après avoir joué. Il peut aussi aller plus loin et comprendre les dessous du jeu.

Après avoir suivi le scenario (« Nouvelle partie »), le joueur peut experimenter en mode arcade d'autre tailles et d'autres types de clefs (par exemple tenter de déchiffrer avec la clef publique, et voir que c'est en effet presque impossible).

Autre fonctionnement : Ce jeu se joue aussi à travers les réseaux sociaux usuels (facebook, twitter, google+ ou email) : un joueur peut envoyer un message chiffré à ses contacts, qui joue une simple partie pour le déchiffrer (sans scenario). Un avertissement cependant : Cryptris n'est qu'un jeu, la clef privée est incluse dans le lien et tous ceux qui ont accès au lien peuvent ainsi dechiffrer (pour etre serieux il faut utiliser PGP).

Partage de culture scientifique à travers ce jeu.
Les grands éléments de culture scientifique à partager sont :

1/ le mécanisme de clé publique / clé privée ;
2/ le fait que le joueur trouve par lui-même un algorithme pour gagner le jeu ;
3/ et que le bon fonctionnement d'un algorithme se démontre ;
4/ le fait que chaque geste du jeu correspond à un calcul (addition, produit) sur les colonnes ;
5/ la différence de fonctionnement entre la clé publique et la clé privée ;
6/ la notion de complexité qui est le fondement de la cryptographie ;

Pour s'y préparer il suffit de lire l'article d'introduction disponible. Ensuite, pour donner les éléments d'explication de manière attractive, découvrons ce dialogue lors d'une animation.

Exemple de séquence entre un animateur et un joueur.
Il s'agit d'un dialogue [presque[1]] imaginaire entre un joueur (disons Arthur) et un vulgarisateur (allez, appelons-le Léo), encadrant/animateur du jeu. Une constante ici est que l'animateur essaie de ne pas répondre, mais de donner juste les éléments nécessaires pour que le joueur construise sa propre réponse.

Léo : Alors, qu'en penses-tu ?

Arthur : Oh c'était chouette, je me suis pas ennuyé ; et puis j'ai gagné !

Léo : Oui, pas mal tu as été rapide. Mais au fait, en plus de t'être amusé est-ce que tu a bien compris ce que c'est la cryptographie asymétrique ?

Arthur : Mouais, non pas tout, c'est vrai.

1/ La métaphore du Cadenas

[1] Il est issu d'une expérimentation de l'activité à travers le Web.

L: OK, alors, peut-être commençons par ce que tu as compris.

A: Hum, il y a un ordinateur qui a été piraté et qui contrôle tout Inria bientôt tout Internet !
Pour l'arrêter on doit trouver les bons câbles à débrancher; et les numéros des câbles, et bien on les obtient en détruisant les briques mais j'ai pas trop compris pourquoi...

L: Je vois. Tu te souviens de ce qui s'est passé quand tu as essayé de débrancher le premier câble ?

A: Ah oui ! L'ordinateur nous avait écouté, et savait quel câble j'allais débrancher. Du coup il m'a électrocuté. Alors la chercheuse a dit qu'il fallait qu'on utilise de la cryptographie asymétrique.

L: Et donc ?

A: Il y a une histoire de clef et de cadenas. Tout le monde a le cadenas, mais je suis le seul à avoir la clef.

L: Oui ! On le cadenas joue le rôle de la clef publique, car tout le monde le connait. La clef du cademas joue le rôle de la clé privée, car seul toi la connais. Mais alors comment se sert-on de ce cadenas et de cette clef ?

A: Ah, euh... Oui, je me souviens ; j'envoie le cadenas ouvert à la chercheuse qui cache le message en fermant le cadenas, me l'envoie, et moi j'ouvre le cadenas avec la clef pour retrouver le message. L'ordinateur espion, lui il n'a pas la clef du cadenas et du coup il n'y arrive pas !

L: C'est ça ! La chercheuse utilisait la clef publique (le cadenas) pour *chiffrer* le message, et toi la clef privée (la clef du cadenas) pour le *déchiffrer*. Et ça n'est pas facile de forcer le cadenas sans la clef. Mais au fait, tu te souviens comment la clef et le cadenas sont fabriqués ?!

A: Ouh la, c'était au tout début ! J'avais déjà une clef privée ; et je l'ai "mélangée" pour fabriquer le cadenas, euh la clef publique. Après la chercheuse a mélangé le message "OK" avec cette clef publique et j'ai joué la première partie.

L: Je crois qu'on a fait le tour des principes de bases. Tu peux me résumer toutes les étapes pour recevoir des messages en secret !?

A: Je crois oui :

1/ Je crée une clef secrète.
2/ Je la mélange pour fabriquer une clef publique : c'est une sorte de cadenas, que ma clef seule ouvre.
3/ Je donne la clef publique à tout le monde ; et je garde la clef secrète pour moi seul.
4/ Celui qui veut m'envoyer un message utilise la clef publique : il la mélange au message.
C'est comme fermer le cadenas d'un coffre-fort.
5/ Je reçois le message mélangé à la clef publique ; et la clef privée me permet de dé-mélanger les deux.
C'est comme ouvrir le cadenas du coffre-fort.
6/ D'autre gens peuvent essayer de déchiffrer aussi ; mais ça leur prendra beaucoup, beaucoup de temps.
C'est comme essayer d'ouvrir le verrou avec une épingle à cheveux. C'est possible, mais vraiment pas facile ; et si le cadenas est assez gros c'est vraiment trop difficile.

2/ Déchiffrer avec la clef privée

L: Je suis impressionné, tu as une très bonne mémoire ! Tu as déjà tout compris au principe de la crypto asymétrique. Maintenant voyons voir ce que tu sais de plus ! Oui je suis sûr que sans t'en rendre compte tu à compris bien plus que ça !

A: Vous êtes sûr ?! Ça fait déjà beaucoup je trouve.

L: Voyons voir. Est-ce que tu peux m'expliquer comment tu déchiffrais dans le jeu ?

A: Ben, j'avais des briques en haut, des briques en bas. J'essayais de les éliminer en utilisant des couleurs opposées, pour qu'il en reste le moins possible ; à la fin il ne restait que le message.

L: Oui, ça c'était la règle du jeu en effet. Mais c'était quoi ta stratégie, ta recette pour faire tomber les brique.

A: Ahh ça ! Au début je savais pas trop mais j'ai vite pigé l'astuce ! Je mettais la grande barre du haut sur la plus grande barre du bas restante, j'inversais les couleurs et je faisais tomber. Et puis si ça suffisait pas, ben je recommençais...

L: Dis-moi, tu n'aurais pas fait des programmes informatiques toi ?

A: Moi ? Ouhla, non jamais de la vie; c'est trop casse-tête.

L: Et bien tu sais quoi ? Ce que tu viens de m'expliquer, c'est un *algorithme* ! Félicitation, tu viens de concevoir ton premier algorithme que tu pourrais écrire sous forme de programme :

1/ choisir en haut la plus grande barre et la positionner au-dessus de la plus grande barre du bas;
2/ inverser, si besoin, sa couleur pour qu'elle soit inverse de celle du bas
3/ faire tomber cette barre
4/ recommencer les étapes 1/, 2/ et 3/ tant qu'il reste des barres à réduire en bas

A: Nan, t'essaies de m'mettre en boite là ! J'ai vu des programmes, c'est plein de symboles bizarres partout, genre Matrix.

L: Ahah ! Non un programme c'est très simple ; c'est juste une recette pour arriver à un résultat comme tu viens de le faire. Le truc, c'est que les ordinateurs ne sont pas très malins ; ils ne comprennent que des langages très simples, dénués de pensée ; des langages d'ordinateurs. Mais ces langages ne sont pas si compliqués ; le plus dur c'est d'inventer des recettes comme la tienne ; le reste c'est juste de la traduction.

A: Du coup, si j'apprends une telle façon de penser *algorithmique*, j'peux donner des ordres à un ordinateur c'est ça ?

L: Oui et plein d'autres choses ! Tu pourras même créer des jeux vidéos... Mais reparlons de ton algorithme, de ta recette. Comment tu expliques que ça marche ?

A: Je sais pas, ça semble évident.

L: Certainement, mais si tu devais expliquer à quelqu'un qui trouve pas ça évident ?

A: Ouais, ben, à chaque fois que la grosse colonne du haut tombait sur la grosse colonne du bas, plein de briques disparaissaient dans cette colonne ; parce que je faisais attention à ce que les couleurs soit différentes.

L: Oui, mais du coup que se passait-il dans les autres colonnes ?

A: Euh... Y'avait pas beaucoup de briques dans les autres donc ça bougeait pas trop...

L: Donc au total que ce passait-il ?

A: J'en enlevais beaucoup dans une colonne, et ça changeait pas trop dans les autres ; donc au total j'en enlevais.

L: Ah, intéressant. Donc, en répétant cela plein de fois ?

A: À chaque fois j'en enlève un peu ; donc au bout d'un moment y'a presque plus rien.

L: CQFD !

A: Quoi ?

L: CQFD ! Ce Qu'il Fallait Démontrer ! Non seulement tu as conçu un algorithme sans t'en rendre compte, mais en plus, ce que tu viens de me raconter, c'est une démonstration informatique qui explique le fait que cet algorithme terminait.

A: Tu rigoles ? C'est pas des maths ! J'ai pas parlé de chiffres ou de quoi que ce soit.

L: Bien sûr que si tu parlais de chiffres ; enfin de nombres de briques. Nombres de briques dans une colonne, nombres de briques au total. T'es un vrai crack des maths ouais ! C'est même un raisonnement par récurrence que tu viens de faire.

A: Un raisonnement par quoi ?

L: Par récurrence... Tu viens de m'expliquer que
1/ Si il y a disons N briques, à l'étape suivante le nombre total de briques diminue.
2/ Donc que d'étape en étape le nombre de briques ne peut que décroitre, car nous utilisons la bonne clé privée.
3/ Donc il atteindra forcément zéro au bout d'un nombre fini d'étapes.

A : Certes.

L : Tu vas épater ton prof de maths ;)

A : Pas tout à fait convaincu ! On ne fait pas de vrai calcul ici, des additions ou des soustractions, quoi…

L : Vraiment ? Mais quand une colonne du haut tombe sur une colonne du bas que se passe-t'il ?

A : Ah oui ! Le nombre de briques s'ajoutent en fait, mais alors… changer la couleur c'est comme changer le signe de +1 à -1 et donc en changeant le signe, ça fait des soustractions.

L : Le bleu disons azur correspond donc aux nombres négatifs

A : Et le bleu clair aux nombres positifs !

L : Parfait ! Et quand tu fais tourner les colonnes, ça te fait penser à quelle opération ?

A : C'est moins clair,

L : Bon, prenons exemple avec les entiers; si tu multiplie 123 par 10, ca fait combien ?

A : 1230; trop facile de multiplier par 10 !

L : Daccord, mais qu'est ce que tu remarques ? Qu'est il arrive au chiffres 1 2 et 3 ?

A : Ils ont été décalés d'un cran vers la gauche ! Ah ouais. Mais ici c'est pas tout à fait pareil car les chiffres de gauche reviennent par la droite.

L : Bingo ! Tu as deux fois raison, c'est une opération qui a des points communs avec la multiplication mais pas tout à fait, tu viens de bien identifier une opération mathématique nouvelle !

A: Attends, mais tu m'as bien eu la ! C'est toi le chercheur, mais c'est toi qui me poses des questions, et moi qui t'explique. Parce que j'ai bien deux trois colles pour toi aussi, alors.

L: Je t’écoute...

3/ Déchiffrer avec la clef publique, pourquoi c'est difficile.

A: Tu m'as bien eu avec ton histoire de cadenas et de clef. Au final le cadenas c'est une clef aussi ; et même si elle est publique ; pourquoi ça marcherait pas ?

L: Ah c'est une bonne colle, effectivement. Mais au fait, c'est quoi une clef, dans ce jeu ?

A: Bah, un tas de briques qu'on peut faire tomber sur un autre tas de brique. Esquive pas !

L: Pardon pardon. Bon, on est d'accord que la clef publique et la clef privée était les deux des tas de briques. Mais elles étaient différentes.

A: Oui, la clef publique était "plus grosse".

L: C'est ça. Le truc important c'est qu'elle avait plusieurs grosses colonnes ; du coup, si on essaie ta recette avec cette clef...

A: Ben ça va pas marcher ! Comment on choisit une colonne en particulier pour mon algorithme dans ce cas ?

L: Disons qu'on choisit la plus grande ; et au hasard s'il y a égalité.

A: Hum je vois. Oui mais non, ça va toujours pas marcher. Comme il y a d'autres grandes colonnes, même quand j'en fais baisser une, plein d'autres vont beaucoup monter.

L: Et oui ! Et donc le raisonnement de tout à l'heure ne fonctionne pas ; ta recette ne marche qu'avec la clef privée, pas avec la clef publique. C'est exactement ce qu'on voulait pour construire un vrai système de cryptographie asymétrique ! Bravo, tu as tout compris !

A: Ça sent l'arnaque ton histoire. OK ma recette ne marche pas ; mais pourquoi il n'y aurait pas d'autres recettes, d'autres algorithmes qui eux marcheraient avec la clef publique ?

L: Hum, tu poses une vraie colle là. Pour être tout à fait honnête avec toi, la meilleure réponse que nous avons est "On ne sait pas si de tels algorithmes existent, mais on a de bonnes raisons de penser qu'ils n'existent pas".

A: C'est pas très mathématique comme réponse...

L: Et non ! Mathématiquement parlant on ne connait pas la réponse. En plus tu entres dans une autre science que les mathématiques, la science informatique.

A: Tu esquives ! Comment on peut prétendre que ça existe pas si on en sait rien ?

L: C'est que, vois-tu, un certain nombre d'informaticiennes et d'informaticiens (de chercheurs en science informatique) très intelligents se sont posés la question. Ils bataillent entre eux pour trouver les algorithmes les plus rapides. Ils ont cherché pendant longtemps, et n'ont rien trouvé. C'est une bonne raison de croire qu'il n'y a pas de solution, ou au moins que jamais personne ne la trouvera...

A: Mouais... Peut-être que quelqu'un de plus malin y arrivera un jour. Et puis quelle perte de temps alors !

L: Pas complètement. On a tout de même découvert quelque chose de très important. Il se trouve que si on savait résoudre ce problème de Cryptris, alors on pourrait se servir de la solution pour résoudre beaucoup d'autres problèmes. Car on a réussi à montrer que beaucoup de problèmes pour lequels il n'y a pas d'algorithme efficace sont équivalents, c'est à dire qu'avec la solution de l'un il serait facile de résoudre les autres. On dit que ces problèmes sont NP-complets[2].

A: Des problèmes NP-complets ? De quel genre de problème parle t'on ?

L: Plein de problèmes d'optimisation. Par exemple, un livreur doit visiter plein de maisons. Dans quel ordre doit-il faire sa visite pour faire le moins de route possible ? C'est le problème du « voyageur de commerce ».

---

[2] Ici, on fait le choix d'assumer une inexactitude. Tous les problemes utilises en cryptographie sont dans NP interesection co-NP; donc on soupconne qu'elle ne sont pas NP complet, mais approximativement NP-complet; certes on ne pourrait pas résoudre exactement le sac a dos ou le voyageur de commerce, mais on pourrait trouver de bonnes approximations de la meilleure solution sachant casser Cryptris/ou les vrais cryptosystemes à base de réseaux.

A : C'est le seul exemple ?

L : Non il y a aussi le problème de remplir un «sac à dos» avec des objets précieux de valeurs et de poids divers. Ce sac à dos ne peut supporter qu'un certain poids et on cherche à le remplir pour emporter la plus grande valeur en objets précieux. Il y aussi plein d'autres problèmes…

A : Alors résolvons un de ces problèmes et le tour est joué !

L : Justement, depuis plus d'un demi-siècle toutes les chercheuses et les chercheurs du monde n'ont pu en résoudre efficacement aucun ! On pense donc que, sauf miracle, il n'y a pas de solution efficace. La seul issue est d'énumérer toutes les possibilités pour trouver la bonne.

A : Je comprends bien. Comme quelqu'un qui énumèrerait toutes les clés privées possibles dans l'espoir de trouver la bonne.

L : En définitive, oui.

A: Ok, donc si j'ai bien compris :
1/ Personne ne sait résoudre le problème du voyageur de commerce
2/ Si on savait casser Cryptris, alors résoudre le problème du voyageur de commerce deviendrait facile.
Conclusion : Personne ne sait casser Cryptris car il est NP-complet. CQFD ?

L: Ahah, oui c'est ça ! Ce coup-ci c'est du raisonnement par l'absurde. Un autre raisonnement logique.

A: Et si j'arrive à casser Cryptris avec un algorithme facile ? Ou à résoudre le problème du voyageur de commerce ?

L: Tu impressionneras pas mal de monde … et tu deviendras riche et célèbre !

A: Ah bon ?

L: Oui, tu auras répondu à un des problèmes ouverts les plus célèbres qu'on nomme 'P=NP'. Un prix de un million de dollar est offert à la personne qui le résoudra. Et son nom sera à jamais dans tous les livres de mathématiques et d'informatiques.

A : Oui mais du coup, toutes les cartes bancaires du monde et tous les mots de passe du monde se feront immédiatement piratés !!

L : Tout à fait ! Tu comprends l'immense enjeu ici. Après pour tout te dire, on sait qu'il existe des petites failles dans ce jeu Cryptris (qui a été aménagé pour aider à comprendre), mais la vraie cryptographie a des parades contre ces failles … même si Cryptris casse pas des briques.

A: Très drôle ! Bon mais alors, Cryptris, c'est pas que des briques, il y a des mathématiques et de l'informatique derrière tout ça ?

L: Hum, quelle belle curiosité. Mais, toute ta classe est déjà repartie ! Tu ne t'en es même pas rendu compte.

A: Ah ! Oui. Merci m'sieur, faut qu'je file là, ils m'attendent.

L: Merci à toi ! C'est un vrai plaisir que de partager ça avec toi.

Voix : Adèle Viéville, et Jean-Émile Meyer.