teaser "1, 2, 3... codez !" au cycle 4 : projet "cryptographie"

Soumis par david Wilgenbus le ven, 02/06/2017 - 14:34

Voici un second petit teaser du tome 2 de "1, 2, 3... codez !", qui concerne le collège (cycle 4).

Aujourd'hui, je vous présente un projet sur la **cryptographie**, qui mèle à part égale informatique débranchée (algorithmique, information) et informatique branchée (programmation Scratch). Ce projet s'adresse aux professeurs de mathématiques.

La première séquence, entièrement débranchée, permet aux élèves de découvrir à la fois les méthodes de la cryptographie (depuis le chiffrement de César jusqu'au chiffrement par substitution mono-alphabétique), mais aussi les méthodes de cryptanalyse (en particulier l'analyse fréquentielle), c'est-à-dire l'art de casser un chiffrement quand on ignore sa clé. Le travail porte ensuite sur la question de l'échange des clés, crutiale quelle que soit la méthode de chiffrement : les élèves découvrent l'intérêt du couple clé publique / clé privée. Enfin, la classe débat sur les enjeux actuels de la cryptographie.

La seconde séquence, entièrement branchée, et optionnelle, propose de programmer le chiffrement de César, puis l'analyse fréquentielle sous Scratch (avec tracé d'un graphique normalisé). On y voit que Scratch permet bien d'autres choses que la programmation de jeux vidéos ! Pour le réaliser, les élèves se familiarisent avec les variables simples et les listes ainsi qu'avec la notion de fonction, à travers les blocs personnalisés qu'ils vont créer.

Le plan de ces 2 séquence est (cliquer pour agrandir l'image) :

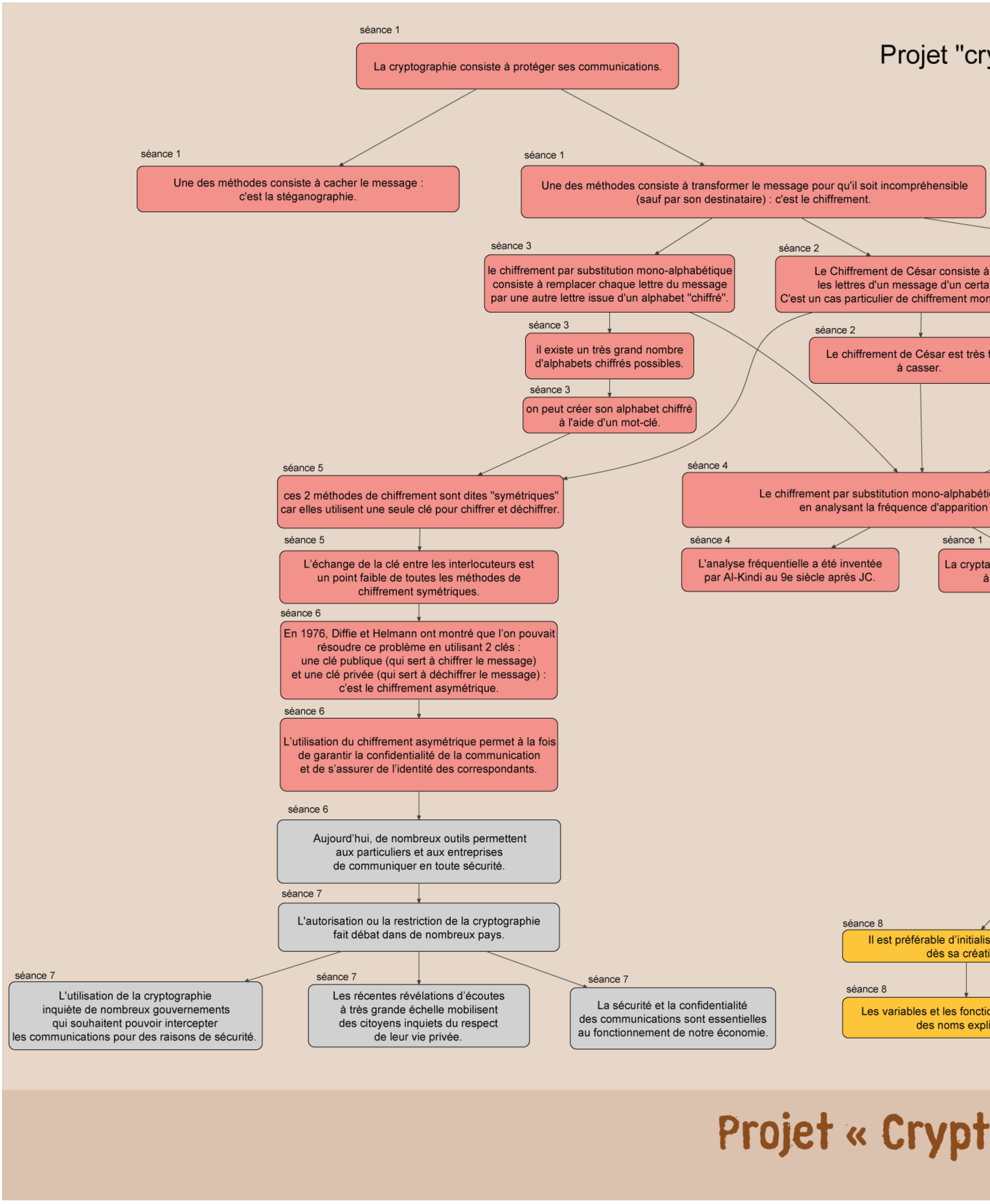
Projet « Cryptographie »

	Séance	Titre	Page	Résumé
	Séance 1	Comment communiquer secrètement ?	119	Les élèves cherchent plusieurs méthodes permettant de crypter un message, et discutent de la fiabilité de ces méthodes.
	Séance 2	Le chiffrement de César	125	Les élèves s'initient à la cryptanalyse : ils doivent décrypter un message sans savoir, a priori, comment ce message a été crypté. Ils découvrent le chiffrement de César, forme très simple de cryptage par substitution mono-alphabétique.
	Séance 3	Chiffrement mono-alphabétique : explosion du nombre de clés possibles	131	Les élèves généralisent le chiffrement de César à n'importe quel chiffrement par substitution mono-alphabétique. Ils apprennent comment chiffrer un message à l'aide d'un mot-clé ou d'une phrase-clé, et calculent le nombre (énorme) d'alphabets chiffrés possibles.
	Séance 4	Casser le chiffrement mono-alphabétique : l'analyse de fréquence d'Al-Kindi	136	Les élèves découvrent et appliquent la méthode d'analyse fréquentielle inventée par Al-Kindi, nécessitant des allers-retours entre la statistique et la linguistique.
	Séance 5	Comment communiquer sans échanger la clé ?	147	Les élèves modélisent les échanges entre 2 personnes à l'aide de cadenas et de clés. Ils prennent conscience du point faible de la plupart des méthodes de chiffrement : l'échange de la clé ; et comprennent que l'usage de plusieurs clés permet de résoudre ce problème. C'est le principe du chiffrement asymétrique.
	Séance 6	Clé publique, clé privée	150	Les élèves perfectionnent leur algorithme de chiffrement asymétrique, en utilisant des clés publiques (qui servent à chiffrer) et des clés privées (qui servent à déchiffrer).
	Séance 7	La cryptographie, amie ou ennemie ?	154	Les élèves participent à un « atelier philo » portant sur les enjeux actuels de la cryptographie. Faut-il l'autoriser, au risque d'empêcher les agences de sécurité de faire leur travail ? Faut-il l'interdire, au risque de voir disparaître notre vie privée ?

	Séance	Titre	Page	Résumé
	Séance 8	Programmer le chiffrement de César (1/4)	159	Les élèves explicitent l'algorithme et listent les étapes qui vont structurer leur projet de programmation du chiffrement de César. Ils programment, dans l'environnement *Scratch*, une première fonction permettant de trouver la lettre correspondant à un rang dans l'alphabet.
	Séance 9	Programmer le chiffrement de César (2/4)	165	Les élèves modifient leur programme précédent pour introduire une « fonction » (bloc personnalisé).
	Séance 10	Programmer le chiffrement de César (3/4)	169	Les élèves avancent leur programme du chiffrement de César : ils sont capables de trouver le rang d'une lettre, puis de chiffrer cette lettre en décalant le rang d'un certain nombre (la clé).
	Séance 11	Programmer le chiffrement de César (4/4)	172	Les élèves terminent leur programme du chiffrement de César, qui permet désormais de chiffrer un message entier, en tenant compte des espaces, de la ponctuation et des accents. Ils apprennent également à commenter un programme de façon à le rendre lisible et compréhensible. Une activité de prolongement est proposée afin de les aider à manipuler les opérateurs logiques.
	Séance 12	Programmer l'analyse fréquentielle	180	Les élèves élaborent un nouveau programme qui permet de calculer les fréquences de chaque lettre d'un message, de façon à faciliter sa cryptanalyse. Ils apprennent à manipuler des variables de type « liste ».
	Séance 13	(optionnelle) Programmer l'affichage de l'histogramme des fréquences (1/2)	186	Les élèves perfectionnent leur programme précédent pour qu'il affiche l'histogramme des fréquences du texte analysé. Ils tracent les axes du graphique et utilisent des costumes (notions propres à *Scratch*) afin de légender l'axe des abscisses.
	Séance 14	(optionnelle) Programmer l'affichage de l'histogramme des fréquences (2/2)	190	Les élèves terminent leur programme en lui faisant tracer le graphique correspondant à l'histogramme des fréquences.

Et voici le scénario conceptuel (cliquer pour agrandir) :

Addons



L'intégralité du projet sera en ligne d'ici au 12 juin. A bientôt !

Commentaires
Aucun commentaire