EPSI l'École d'ingénierie informatique

BACHELOR 3
2013/2014

PROJET DEVELOPPEMENT JAVA

CODE	Semestre	Nombre min. d'heures	Nombre de crédits	Langue
-*	2	20	2*	Français

* en complément au projet engagé précédemment

Objectifs et compétences

OBJECTIFS

Maîtriser la conception orientée objet
Savoir monter de toute pièce une classe, faire appel à l'héritage lorsque cela est nécessaire, faire appel à la création d'interface lorsque cela est nécessaire
Mettre en pratique les concepts avancés (fichiers, gestion d'exceptions, gestion de threads, …)
Construire des algorithmes et choisir les structures de données de la bibliothèque standard
Acquérir une certaine fluidité dans la programmation en langage JAVA

RESUME DU PROJET

Aborder la programmation d'algorithmes de cryptologie
Aborder les concepts de cryptanalyse
Automatiser les programmes de cryptanalyse

Formule pédagogique

PREREQUIS

Algorithmique

DEROULEMENT

8 séances de 4 heures et deux séances de soutenances

LIVRABLES

Code source du projet

Plan détaillé

ETAPE 1 – ALGORITHME A DECALAGE : CODAGE

- Codage de César : le principe, simple, est de décaler de n lettres l'alphabet retenu.
- Problèmes sous-jacents : quel domaine ? (alphabet, avec ou sans accents, minuscule ou majuscule, …)
- Réaliser la classe qui permet de coder sur le principe de César
- Apports complémentaires en langage JAVA : gestion de fichiers, déplacement dans les répertoires, gestion des exceptions

ETAPE 2 – ALGORITHME A DECALAGE : DECODAGE

- Comment décoder un texte codé avec le principe de César … ?

- Construire les classes qui permettent d'effectuer une analyse sur du texte codé en César afin de le décoder.

Etape 3 – Algorithme d'analyse statistique

- Ecrire un algorithme capable d'analyser la fréquence d'apparition des lettres de l'alphabet dans un texte.
- Réaliser les classes correspondantes
- Peut-on détecter la langue d'un texte en clair automatiquement ?
- Peut-on détecter la langue d'un texte codé automatiquement ?

Etape 4 – Algorithme a permutation : Codage

- Codage : le principe, simple, est d'affecter une autre lettre de l'alphabet dans le désordre sans employer de mot clé.
- Réaliser la classe qui permet de coder sur ce principe
- Apports complémentaires en langage JAVA : emploi d'objets de type liste ou autre de la bibliothèque

Etape 5 – Algorithme a permutation : Decodage

- Comment décoder un texte codé avec ce principe ?
- Construire les classes qui permettent d'effectuer une analyse sur du texte codé avec ce principe afin de le décoder.

Etape 6 – Algorithme du carre de Polybe : Codage

- Codage : le principe de base est de construire un tableau de 5 par 5, soit 25 cases. A chaque case est affectée une lettre de l'alphabet, excepté le W qui sera remplacé par un V dans le texte en clair. Chaque ligne ou colonne est numérotée de 1 à 5. Le texte chiffré devient un couple de chiffre, construit à l'aide des abscisse et ordonnée du tableau pour une seule lettre.
- Réaliser la classe qui permet de coder sur ce principe

Etape 7 – Algorithme du carre de Polybe : Decodage

- Comment décoder un texte codé avec ce principe ?
- Construire les classes qui permettent d'effectuer une analyse sur du texte codé avec ce principe afin de le décoder.

Etape 8 – Algorithme de transposition triangulaire : Codage

- Codage : le principe de base est de construire un triangle dans lequel le texte clair est écrit. En première ligne, il n'y a qu'une seule lettre, en seconde, deux lettres, en troisième trois, … En dernière ligne (souvent incomplète), on place un mot clé répété plusieurs fois en correspondance avec les deux dernières lignes. (voir l'exemple ci-après en annexe)
- Apports complémentaires en langage JAVA : traitements algorithmiques complexes

Etape 9 – Algorithme de transposition triangulaire : Decodage

- Comment décoder un texte codé avec ce principe ?
- Construire les classes qui permettent d'effectuer une analyse sur du texte codé avec ce principe afin de le décoder.

Soutenance – groupes de 2 ou 3 personnes

Remise des codes sources via email
20 minutes de test de décryptage automatique et questions/réponses
Note individuelle (suivi du projet et questions/réponses)

Annexes

Annexe A – Codage de cesar

En première ligne se trouvent les caractères de l'alphabet, en version non codé. La seconde ligne correspond, pour chaque colonne, à la version codée de la lettre ci-dessus. Ici le décalage possède la valeur 3.

Tableau de correspondance pour un alphabet de 26 caractères.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Texte en clair : « LECODAGEPARLECODEDECESAR »

Texte codé : « OHFRGDJHSDUOHFRGHGHFHVDU »

Annexe B – Codage par permutation

Tableau de correspondance pour un alphabet de 26 caractères.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	S	M	U	K	A	Z	V	B	X	Q	N	C	G	H	T	W	I	D	R	E	J	F	L	P	Y

Texte en clair : « LECODAGEPARPERMUTATION »

Texte codé : « NKMHUOZKTOITKICERORBHG »

Annexe C – Codage par le carre de Polybe

Tableau de correspondance pour un alphabet de 25 caractères.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Texte en clair : « LECODAGEPARLECARREDEPOLYBE »

Texte codé : « 32151335141122154111433215131143431514154135325412 15 »

ANNEXE D – CODAGE PAR TRANSPOSITION TRIANGULAIRE

Tableau de mise en œuvre pour un exemple donné.

							L							
						E		C						
					O		D		A					
				G		E		P		A				
			R		T		R		A		N			
		S		P		O		S		I		T		
	I		O		N		T		R		I		A	
N		G		U		L		A		I		R		E
C	O	D	A	G	E	C	O	D	A	G	E	C	O	D
3	13	6	1	11	9	4	14	7	2	12	10	5	15	8

Texte en clair : « LECODAGEPARTRANSPOSITIONTRIANGULAIRE »

Clé du message codé : « CODAGE »

Texte codé : « ROAARNEEOLTRSGCPSAEOTNNIGPUAIIILDRTA »