APP1: Ydana wheya

Florent Bouchez Tichadou, Guillaume Huard
florent.bouchez-tichadou@univ-grenoble-alpes.fr
guillaume.huard@univ-grenoble-alpes.fr

7 Septembre 2020

Source : http://www.geocaching.com

Objectifs d'apprentissage : raisonnements algorithmiques, manipulations d'ensembles et de séquences, de listes d'associations, et analyse de complexité algorithmique.

I. APP1 : Ydana wheya

I.1. Objectifs de la situation-problème

À l'issue de l'APP1, vous serez capable de :

- Effectuer diverses manipulation sur les *ensembles* et *séquences* représentés par tableau avec longueur explicite : insertion, suppression, parcours ;
- Utiliser les ensembles et séquences pour implanter des *listes d'associations* (ou *dictionnaires*) ;
- Choisir le type de données approprié pour traiter un problème ;
- Analyser la *complexité algorithmique* d'algorithmes utilisant ces structures de données.

I.2. Organisation des séances

Cet APP comportera six séances de groupe encadrées ainsi que plusieurs CM.

Entre chaque séance, du TRAvail Personnel (TRAP) est nécessaire et attendu !

- Séance Groupe d'ouverture (1h30) : découverte du problème et première analyse.
- Séance Pratique en binômes (3h) : découverte du code source de l'APP, premières implantations.
- Séance Groupe de mise en commun (1h30) : Comparaison des types utilisés et mise en commun des réflexions sur la manière d'aborder le problème.
- Séance Pratique en binômes (3h) : Implantation des algorithmes choisis.
- Séance Groupe de mise en commun (1h30) : Comparaison des algorithmes et de leur complexité algorithmique. Écriture de votre « tableau » qui servira pour l'évaluation de groupe.
- Séance Pratique en binômes (3h) : fin de l'implantation de votre programme. Rendu de votre code sur Caseine (évaluation en binômes).

Note : chaque semaine, il y a également un CM qui servira à éclaircir les points encore flous du contenu théorique, et à la pratique d'exercices « classiques ».

I.3. Ressources pour la recherche d'informations

- Polycopié du cours, Chapitre « Ensembles et séquences » *(sur Caseine)* ;
- Consultation de sites internet sur l'histoire de la cryptographie.

I.4. Évaluation

Cet APP (ainsi que les suivants) comporte une évaluation de *groupe*, une évaluation par *binômes*, ainsi qu'une évaluation *individuelle* qui compteront dans la note de contrôle continu.

L'évaluation individuelle sera faite lors des partiels de mi-semestre. Elle portera sur les objectifs mentionnés ci-dessus (plus de détails en fin de ce livret, Section XIII).

L'évaluation par binôme sur un rendu de code sur Caseine. La note prendra essentiellement en compte l'avancement dans l'APP ainsi que le respect des consignes de rendu.

L'évaluation de groupe se porte sur l'élaboration d'un tableau fin de dernière Séance Groupe . Elle est essentiellement formative pour vous aider à progresser et comptera comme un bonus dans la moyenne du contrôle continu.

I.5. Rôles

Pour cette séquence APP, inscrivez les personnes volontaires pour chacun des quatre rôles :

Modérateur _____

Gardien du temps _____

Scribe _____

Secrétaire _____

Situation — problème

Vous venez d'intercepter un message étrange dont voici un extrait :

> Hmjw Gtg,
> Stzx sj utzatsx uqzx stzx jhmfsljw ij rjxxfljx xnruqjrjsy ufw jrfnq. H'jxy ywtu wnxvzj. O'fn unwfyj qj xjwajzw i'jyzinfsyx utzw js kfnwj zs qnjz i'jhmfsljx uqzx inxhwjy. O'fn jkkfhj ytzyjx qjx ywfhjx (...)

Vous vous doutez immédiatement qu'il s'agit d'un message crypté de la plus haute importance et qu'il faut tout mettre en œuvre afin de déterminer son contenu. Étant probable qu'à l'avenir vous interceptiez d'autres messages similaires, il est primordial d'**automatiser** le décryptage par la rédaction d'un algorithme théorique et de son implantation sur ordinateur. Ce sera votre première tâche.

Par la suite, il y a fort à parier que, si vous réussissez à décrypter automatiquement leurs messages, Alice et Bob (ce sont toujours Alice et Bob) tentent d'améliorer leur protocole de communication.

Si vous trouvez de nouveaux messages cryptés au cours de votre investigation, il vous faudra tout mettre en œuvre pour parvenir à les décrypter.

Complément d'informations

Concentrez-vous initialement sur la méthode de chiffrement utilisée. Sachant qu'Alice et Bob sont toujours très polis, déterminez comment vous pourriez exploiter cette faille afin d'obtenir des informations sur le texte original, et d'avoir un algorithme complètement automatique (sans intervention manuelle). Favorisez le **raisonnement** logique avant de déterminer les **détails algorithmiques**. Il sera important dans la suite de **valider** empiriquement vos algorithmes. Pour cela, vous devrez tester vos programmes sur Caseine, et sur une autre plateforme pédagogique qui est pour l'instant secrète...

Pour faciliter le raisonnement, ne vous préoccupez pas des détails techniques de lecture et écriture des fichiers. Considérez par exemple que vous avez une fonction `lire_ligne`, qui vous renvoie à chaque fois la prochaine ligne du texte à décrypter (un tableau de caractères).

Pour les Séance Pratique (TPs), dans un premier temps, vous devrez faire l'exercice préparatoire sur Caseine. Comme son nom l'indique, cet exercice est à faire **avant** la prochaine séance de TP. **Il est primordial de faire cet exercice par vous même.**

Pour la suite, vous trouverez des fichiers utiles, soit **sur Caseine au format** `zip`, soit sur la plateforme pédagogique secrète, soit directement **sur Turing** dans le répertoire de l'APP correspondant à votre parcours :

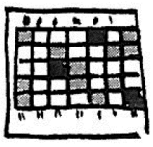
— pour les groupes INF et MIN : `/Public/301_INF_Public/APP_C/APP1`
— pour les groupes MAT : `/Public/301_INF_Public/APP_Python/APP1`

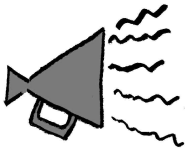
II. Session 1 : Découverte et analyse du problème

Timing	*Tâches à réaliser durant la séance*
1 5 min.	Organisez votre groupe : attribuez les rôles (modérateur, gardien du temps, scribe, secrétaire) pour le projet. Les personnes doivent être volontaires... Inscrivez les personnes choisies page 3.
2 20 min.	**Attention:** Phase individuelle (pas de discussion !) Prenez connaissance du problème : lisez attentivement l'énoncé. Essayez de trouver par vous-même des éléments de réponse au problème posé.
3 55 min.	Mise en commun de votre compréhension du problème et de vos premières idées. Notez au tableau toutes vos réflexions en réservant bien une zone pour noter les éléments à éclaircir avec le tuteur.
4 10 min.	Présentez au tuteur une synthèse rapide de vos discussions et prenez connaissance des consignes pour la séance 2.

Total: 90 min.


Comprendre

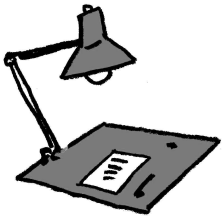

Organiser le groupe


Favoriser l'expression de chacun

III. Consignes pour la prochaine séance

La prochaine séance sera une Séance Pratique . Il est primordial de bien préparer cette séance afin qu'elle soit efficace. Vous devez absolument avoir un programme fonctionnel qui décrypte les messages avant la fin de cette séance.

1. Connectez-vous à votre compte Caseine (caseine.org), inscrivez-vous au cours INF301 (http://caseine.org/course/view.php?id=72), et faites obligatoirement le premier exercice de l'APP **individuellement**. (Pour avoir accès à l'exercice, renseignez votre groupe (INF, MIN ou MAT) et haut de la page). Cet exercice préparatoire vous permettra de commencer efficacement la Séance Pratique. Si vous n'arrivez pas à valider cet exercice, vous pourrez demander de l'aide à la prochaine séance, mais il faut impérativement avoir essayé de le faire seul au préalable.
2. À partir des pistes de réflexion élaborées durant la séance 1, tirez au clair la méthode générale de résolution du problème que vous allez suivre.
3. Déduisez-en la structure de l'algorithme : identifiez les fonctions dont vous aurez besoin, et pour chacune précisez en quelques lignes sa signature (types des paramètres et de la valeur de retour) et ce qu'elle fait.
4. Écrivez en détail l'algorithme que vous allez utiliser. Le but est d'avoir un algorithme le plus clair possible afin de pouvoir l'implanter rapidement durant la prochaine séance.



Important

Il est crucial que chaque membre du groupe fasse sa part de de travail, pour que vous puissiez travailler lors de la prochaine séance. Vous êtes responsables de **votre propre apprentissage**, mais l'apprentissage des autres membres du groupe **dépend aussi de vous** !

IV. Session 2 : implantation (3h)

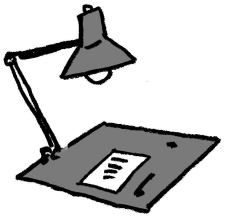
Timing	*Tâches à réaliser durant la séance*
1 15 min.	Si vous n'avez pas validé le premier exercice sur Caseine (César), discutez-en avec votre binôme et assurez-vous d'avoir chacun validé 100% des tests : `http://caseine.org/course/view.php?id=72`, section APP1.
2 165 min.	Une fois l'exercice terminé, vous avez accès à un message secret... Prenez connaissance de ce message et... débrouillez-vous :-) N'hésitez pas à demander de l'aide si tout n'est pas clair ou s'il y a des étapes qui ne fonctionnent pas. Pour les groupes INF et MIN, vous allez maintenant travailler sur Turing, récupérez le squelette à l'adresse suivante en utilisant la commande ci-dessous (ne pas oublier le « . » à la fin, et placez vous bien dans votre répertoire de travail) : `cp -r /Public/301_INF_Public/APP_C/APP1 .` Pour les groupes MAT, vous pouvez également travailler sur Turing (voir ci-dessus), ou utiliser l'éditeur `Idle` sous windows. Dans ce cas, récupérez le squelette sur Caseine au format `zip` ou sur la plateforme pédagogique secrète.

Total: 180 min.

V. Consignes pour la prochaine séance

En fonction de votre avancement, réalisez les tâches ci-dessous :

1. Si vous avez un programme fonctionnel qui décrypte automatiquement les messages cryptés, vous êtes dans les temps.
   Vous devriez maintenant avoir des pistes sur le travail qu'il reste à faire... Préparez alors la prochaine Séance Groupe en réfléchissant au(x) nouveau(x) problème(s) qui se pose(nt) à vous...
2. Si vous n'avez pas de programme fonctionnel, vous êtes en retard sur l'APP. Identifiez les problèmes qui se posent à vous et corrigez l'algorithme. **Il vous faut absolument avoir un algorithme de décryption fonctionnel** avant la prochaine séance pour avancer dans l'APP !



Travailler individuellement !

VI. Session 3 : mise en commun (1h30)

Timing	*Tâches à réaliser durant la séance*
1 30 min.	Mise en commun des problèmes recontrés et des solutions algorithmiques que vous envisageaz. Discutez des similitudes ainsi que des différences entre vos algorithmes. Gardez en tête que pour le rendu de groupe (“tableau”), vous aurez à présenter une étape intéressante d’un algorithme choisi (état de la mémoire, explication de ce qui aura lieu après, analyse de complexité. . .).
2 60 min.	Après discussion avec votre tuteur, réflexion individuelle puis collective selon votre avancement dans l’APP. C’est à vous de gérer les tâches à effectuer à présent.

Total: 90 min.

VII. Consignes pour la prochaine séance

1. Le chapitre sur les ensembles et séquences est à maîtriser en totalité d’ici la fin de l’APP. Relisez le attentivement et notez les points qui sont encore obscurs.
2. Choisissez au moins un exercice proposé du chapitre. Servez-vous de cet exercice pour identifier les points qui restent difficiles du cours. Posez des questions à l’enseignant sur ces points au prochain CM.

Travailler individuellement !

VIII. Session 4 : implantation (3h)

Timing	*Tâches à réaliser durant la séance*
1 180 min.	Continuez l’implantation ou l’amélioration de vos algorithmes de décryptage. Une fois que vous avez réussi à coder un algorithme de cryptage ou décryptage, prennez le temps d’avoir un regard critique sur votre travail : avez-vous été efficaces ? Votre code est-il compréhensible par quelqu’un d’autre ? Qu’allez-vous améliorer pour la prochaine étape ?

Total: 180 min.

IX. Session 5 : mise en commun (1h30)

Timing	*Tâches à réaliser durant la séance*
1 90 min.	Éclaircissez les derniers points de détails et mettez à profit cette dernière séance de groupe pour être certains de ne pas être passé à côté d'un point important. Sollicitez pour cela votre tuteur ! Réalisez votre « tableau » qui sera évalué pour une note "bonus" sur votre contrôle continu. Soignez la présentation et soyez le plus précis possible. La note (informative) tiendra compte de la difficulté de l'algorithme présenté (en fonction de l'avancement dans l'APP), de la clarté de vos explications, du choix des exemples d'exécution, de l'analyse de complexité. N'hésitez pas à demander de l'aide à votre tuteur·trice. Points importants : commencez toujours par **expliquer** le fonctionnement de vos algorithmes avant d'en donner le pseudo-code. Essayez de rester aussi haut-niveau que possible dans vos algorithmes, et décrivez les opérations bas-niveau opérant sur les structures de données de manière séparée.

Total: 90 min.

X. Session 6 : implantation (3h)

Timing	*Tâches à réaliser durant la séance*
1 180 min.	Terminez vos implantations d'algorithmes. Soignez votre code : indentation, commentaires pour les points-clés fonction, noms de variables appropriés. Vous devez rendre un code commun pour votre groupe d'APP sur Caseine.

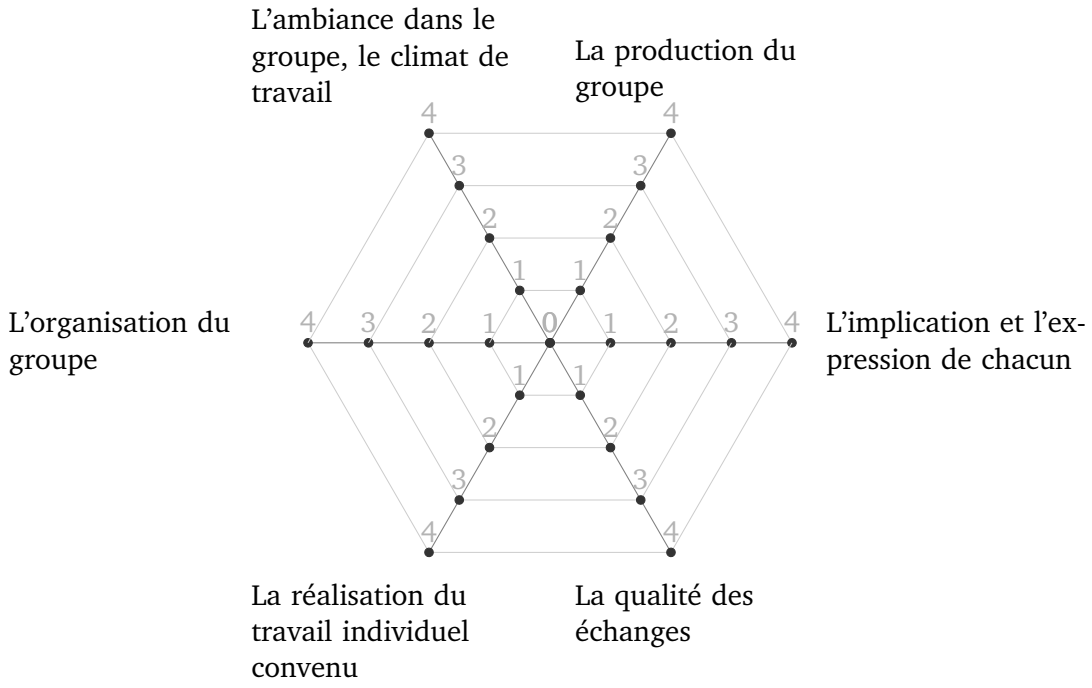
Total: 180 min.

XI. Auto-évaluation du travail de groupe — Circept

A faire au début de la première séance de l'APP suivant.

XI.1. Faire un bilan du travail de groupe

— **Individuellement :** remplissez le circept (cf. informations complémentaires page suivante) et répondez aux questions sur le travail de groupe (10 min.) ;
— Comparez vos réponses et tirer un bilan du travail de groupe ;
— Faites part de votre analyse au tuteur.



XI.2. Donner deux points positifs de votre travail de groupe :

—
—

XI.3. Donner deux points négatifs de votre travail de groupe :

—
—

XI.4. Quels engagements prendriez-vous pour améliorer votre travail de groupe ?

—

XII. Exercices d'entraînement

Entraînez vous sur le chapitre du cours correspondant (exercices proposés). Nous vous recommandons de faire au moins quelques exercices autour de chaque notion importante (voir section suivante) pour vous entraîner.

XIII. Vos apprentissages

Pour chaque objectif de cet APP, estimez vous-même le niveau de vos apprentissages après cette séquence.

Au terme de l'APP, vous êtes capable de :	*Oui*	*Non, mais voici ce que je vais faire pour y remédier*
1. Tracer un algorithme simple pour en vérifier la justesse sur quelques exemples ;	▫	_____
2. Corriger un algorithme simple faux (qui ne vérifie pas la spécification demandée ou l'explication algorithmique) ;	▫	_____
3. Expliquer la différence entre un ensemble, une séquence, et un tableau ;	▫	_____
4. Lister les opérations de haut niveau sur les ensembles et séquences et leurs effets ;	▫	_____
5. Expliquer comment implanter un ensemble ou une séquence avec un tableau ;	▫	_____
6. Donner les schémas bas-niveau de recherche, d'ajout, de suppression dans un ensemble (à base de tableau) ;	▫	_____
7. Donner les schémas bas-niveau de recherche, d'ajout, de suppression dans une séquence (à base de tableau) ;	▫	_____
8. Donner les complexités algorithmiques de ces schémas ;	▫	_____
9. Implanter une liste d'association en utilisant un ensemble ou une séquence (haut niveau) ;	▫	_____
10. Donner les complexités des opérations travaillant sur une liste d'association.	▫	_____