PROJECT GENERATOR

Rapport de projet

Groupe MONDOT, GLENADEL, BARRAIRON, CASTANIE

Table des matières

I. PRESENTATION DU PROJET

A. PRESENTATION DU GROUPE DE PROJET

Jules MONDOT : Chef de projet, responsable communication
Romain CASTANIE : Responsable IHM et bases de données
Lucas GLENADEL : Couche métier
Vincent BARRAIRON : Couche métier

B. CONTEXTE

Un organisme militaire souhaite s'approprier des informations sensibles. Les militaires identifier et neutraliser un dangereux terroriste.

Des documents récemment dérobés contiennent le nom d'un informateur terroriste qui peut les renseigner sur l'identité du chef du réseau terroriste. Le problème est que ces informations sont chiffrées. Des sources fiables ont indiquées aux militaires, que le chiffrement n'est pas asymétrique. Il est opéré à l'aide de la technique du XOR. La taille de la clef est de 5 éléments (tous compris entre 0 et 9). Les militaires nous confient la mission 'generator'.

C. RAPPEL DU BESOIN

Nous devons :

- Rentrer en contact avec les militaires (gen.project.exia@gmail.com). Ils nous remettront les documents chiffrés qui contiennent le nom de l'informateur terroriste.
- Déchiffrer ces premiers documents.
- Rentrer en contact avec le terroriste afin de lui soutirer le nom du chef du réseau.
- Communiquer aux militaires l'identité du chef.

D. OBJECTIFS

1. SPECIFICATIONS FONCTIONNELLES

Nous devons concevoir et développer une plateforme distribuée permettant :

- D'authentifier l'utilisateur.
- De déchiffrer plusieurs documents de types « .txt » en simultané.
- De fournir un document chiffré de type « .txt » par document fichier source.
- De fournir un rapport de type « .pdf » présentant le taux de confiance d'un document déchiffré par document chiffré source.

II. PROJET GENERATOR

A. ANALYSE

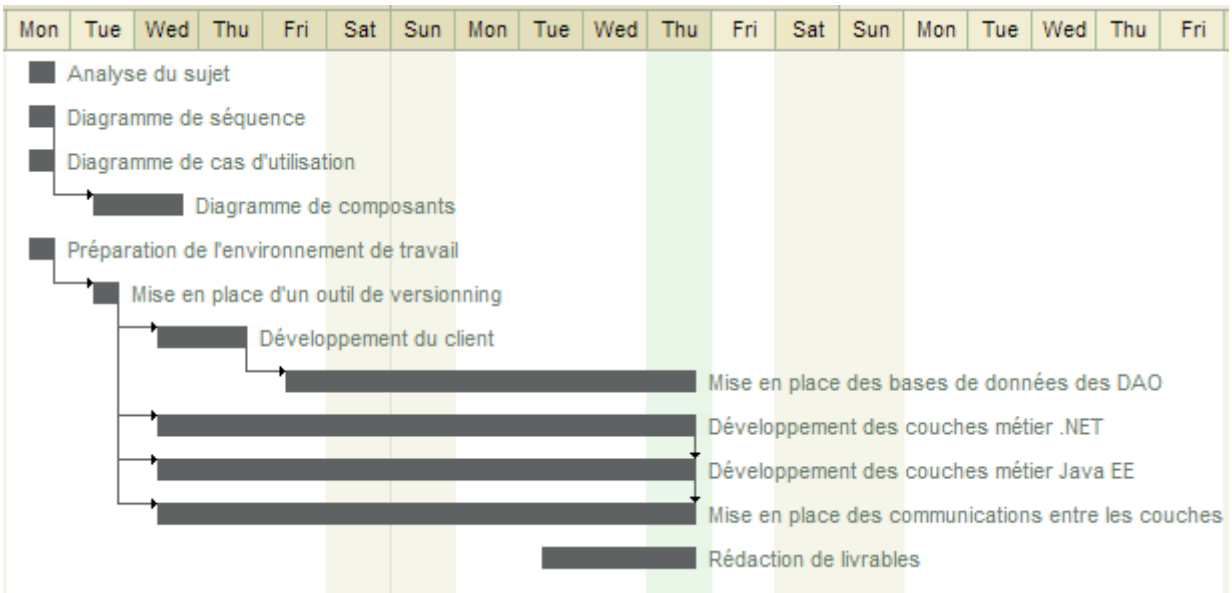
1. LES UTILISATEURS

Les utilisateurs du projet seront les militaires voulant décrypter un ou plusieurs fichiers.

2. CHOIX DES TECHNOLOGIES

Nous avions l'obligation d'utiliser le .NET (C#/WCF) ainsi que le Java EE (EJB/JMS/Web services) afin de développer l'application.
Nous avons donc développé l'application .NET en C# et Java EE, langages avec lesquels nous sommes assez familiers.
Le Client a été fait en Windows Form, ce qui nous as permis une réalisation rapide.

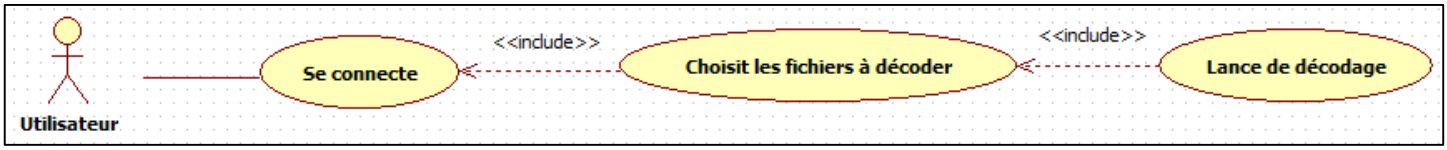
3. PLANNING



2. CONCEPTION

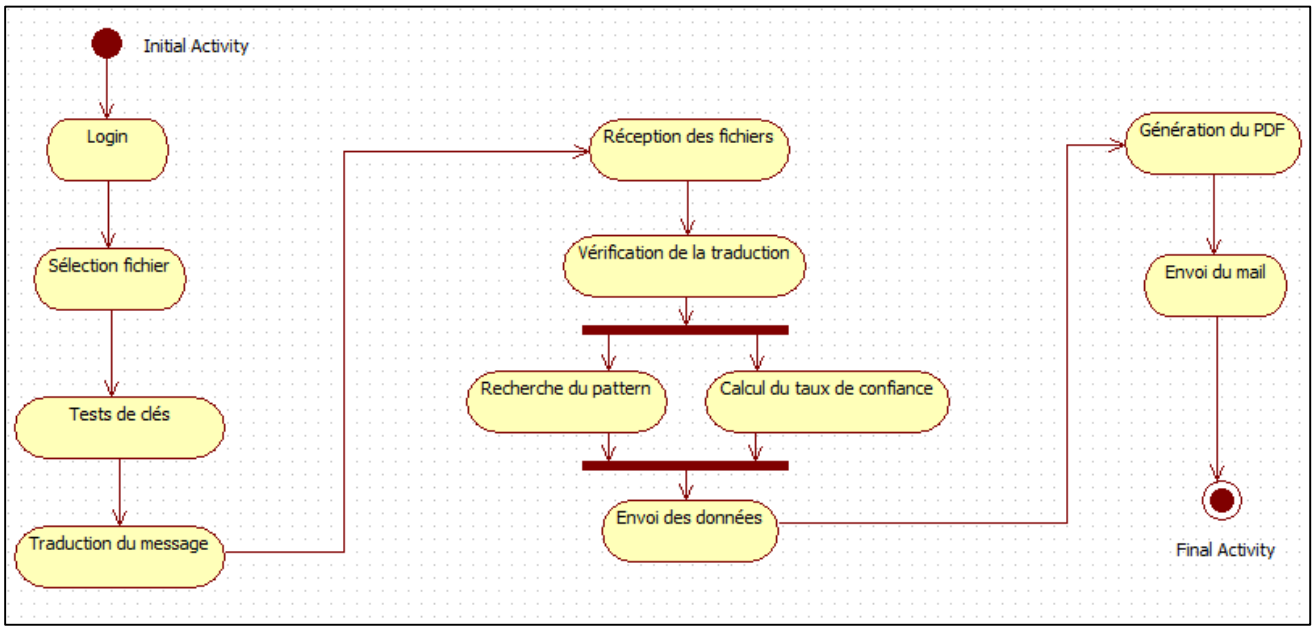
1. CAS D'UTILISATION

Le diagramme de cas d'utilisation est relativement simple :

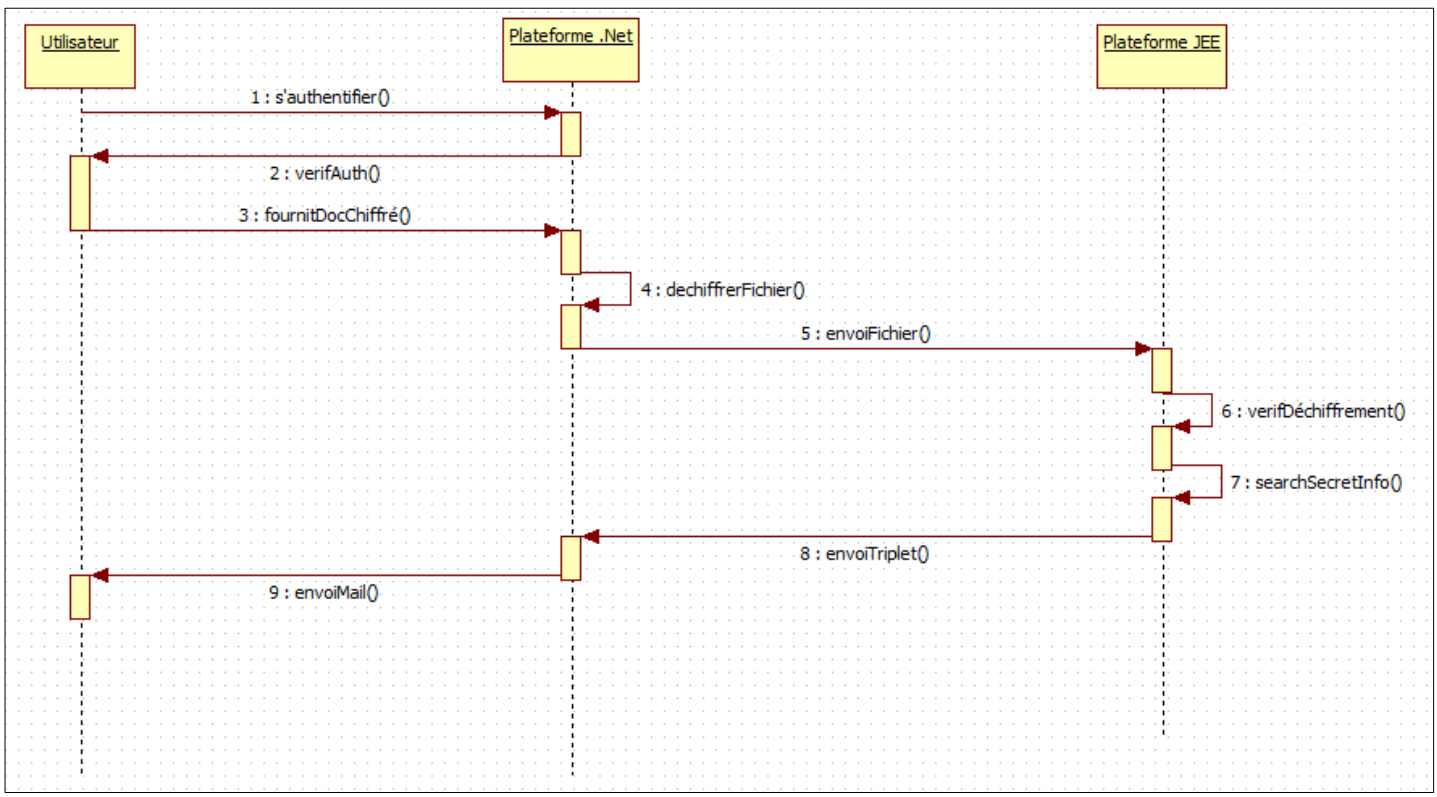


2. DIAGRAMME D'ACTIVITE

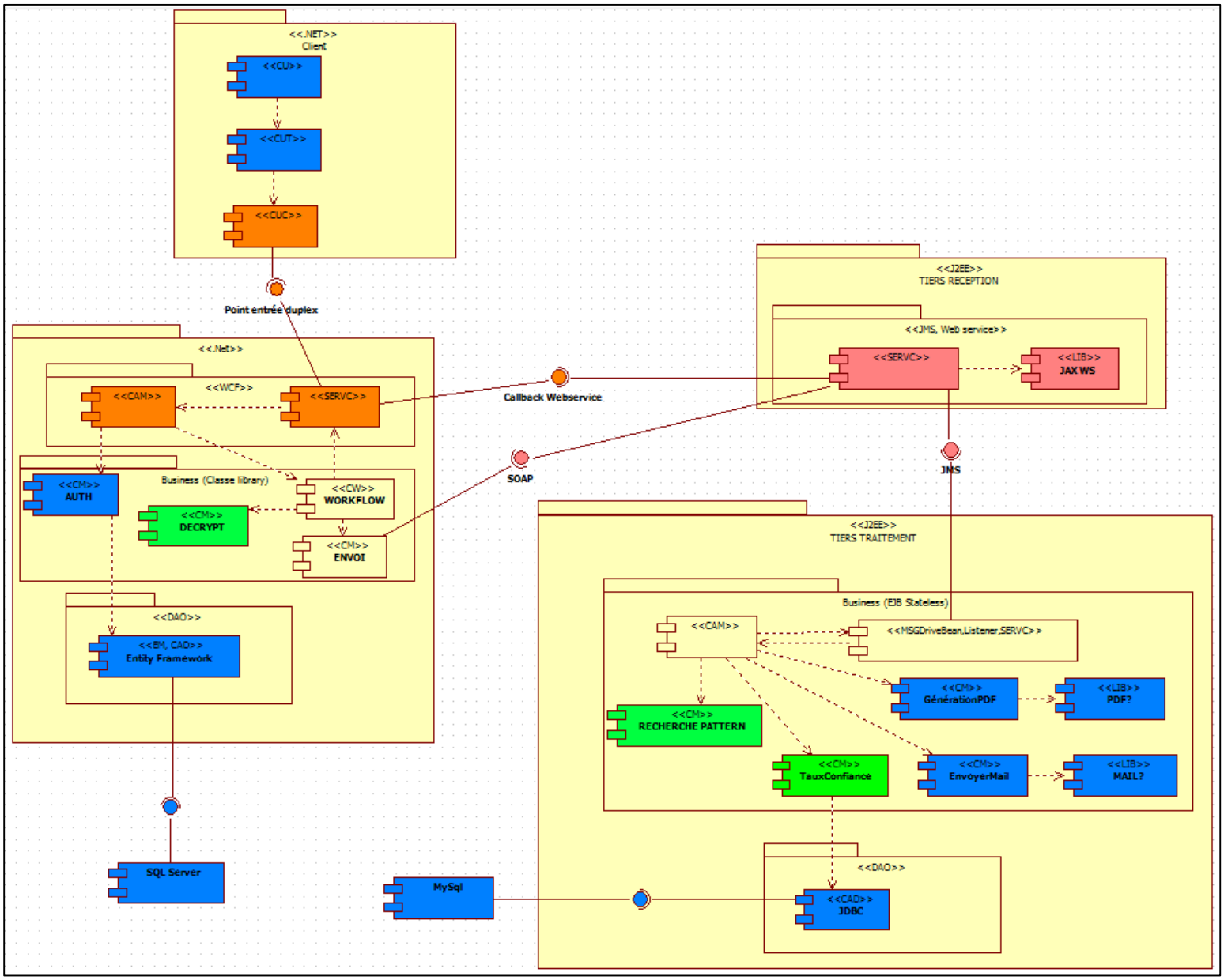
Le diagramme d'activité est une partie de l'analyse du logiciel qui est importante. Elle définit la façon dont le logiciel va fonctionner, et nous a permis ensuite de diviser le logiciel en tâches séparées.



3. DIAGRAMME DE SEQUENCE



4. ARCHITECTURE DE L'APPLICATION



3. REALISATION

1. ALGORITHMIQUE

La fonction de décryptage est le cœur du programme, c'est elle qui demande le plus de traitement il est donc important qu'elle soit la plus efficace et optimisé possible.

La conception de son algorithme commence par la méthode d'application du XOR. Pour cela, 3 méthodes ont dû être testées avec comme données :

- Clé : 9876
- Texte crypté : azerty

Méthode 1 : un caractère de la clé pour un caractère du message.

a	z	e	r	t	y
9	8	7	6	9	8

Méthode 2 : tous les caractères de la clé sont appliqué un par un pour un caractère du message.

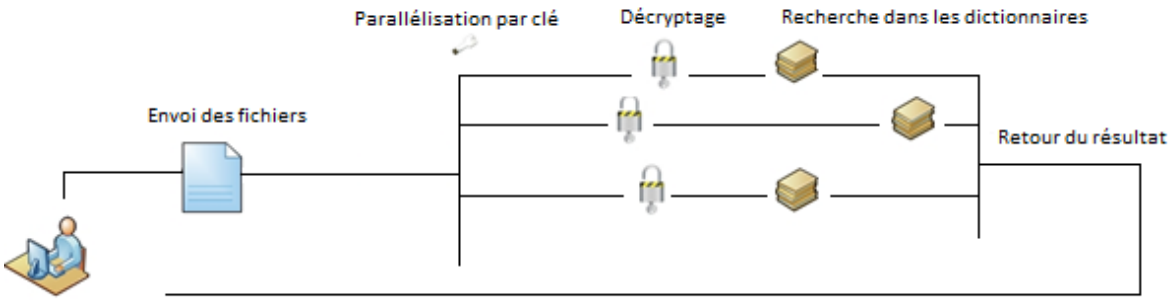
a	z	e	r	t	y
9	9	9	9	9	9
8	8	8	8	8	8
7	7	7	7	7	7
6	6	6	6	6	6

Méthode 3 : toute la clé pour un caractère du message.

a	z	e	r	t	y
9876	9876	9876	9876	9876	9876

Les fichiers étaient cryptés avec la 1ère méthode.

Pour trouver la clé il est nécessaire de tenter de décrypter le texte avec toutes les possibilités (soit 10longueur de la clé possibilités). Pour ce faire il devient impératif d'utiliser toutes la ressource disponible en travaillant en parallèle sur tous les processeurs.



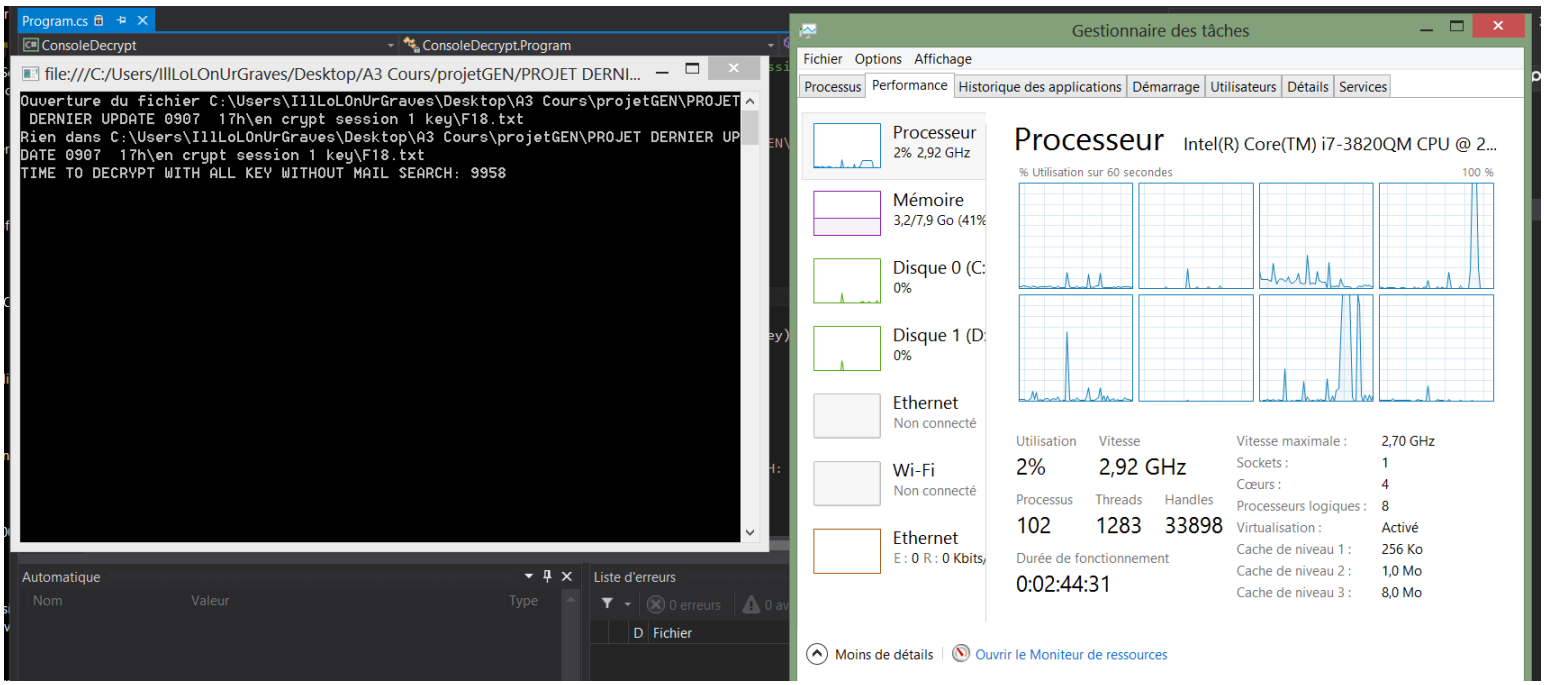
2. PROGRAMMATION

Lors de la phase de programmation, le travail ayant été bien réparti, nous avons chacun travaillé sur des projets en « local ». Puis, une fois notre travail (ou une partie) terminé, nous mettions la solution en commun à l'aide de GitHub. Nous avons cependant rencontrés quelques difficultés avec la mise en place de SQL Server (support de données de la plateforme .NET) ainsi qu'avec nos algorithmes (notamment la seconde partie) et la communication (au niveau des callback).

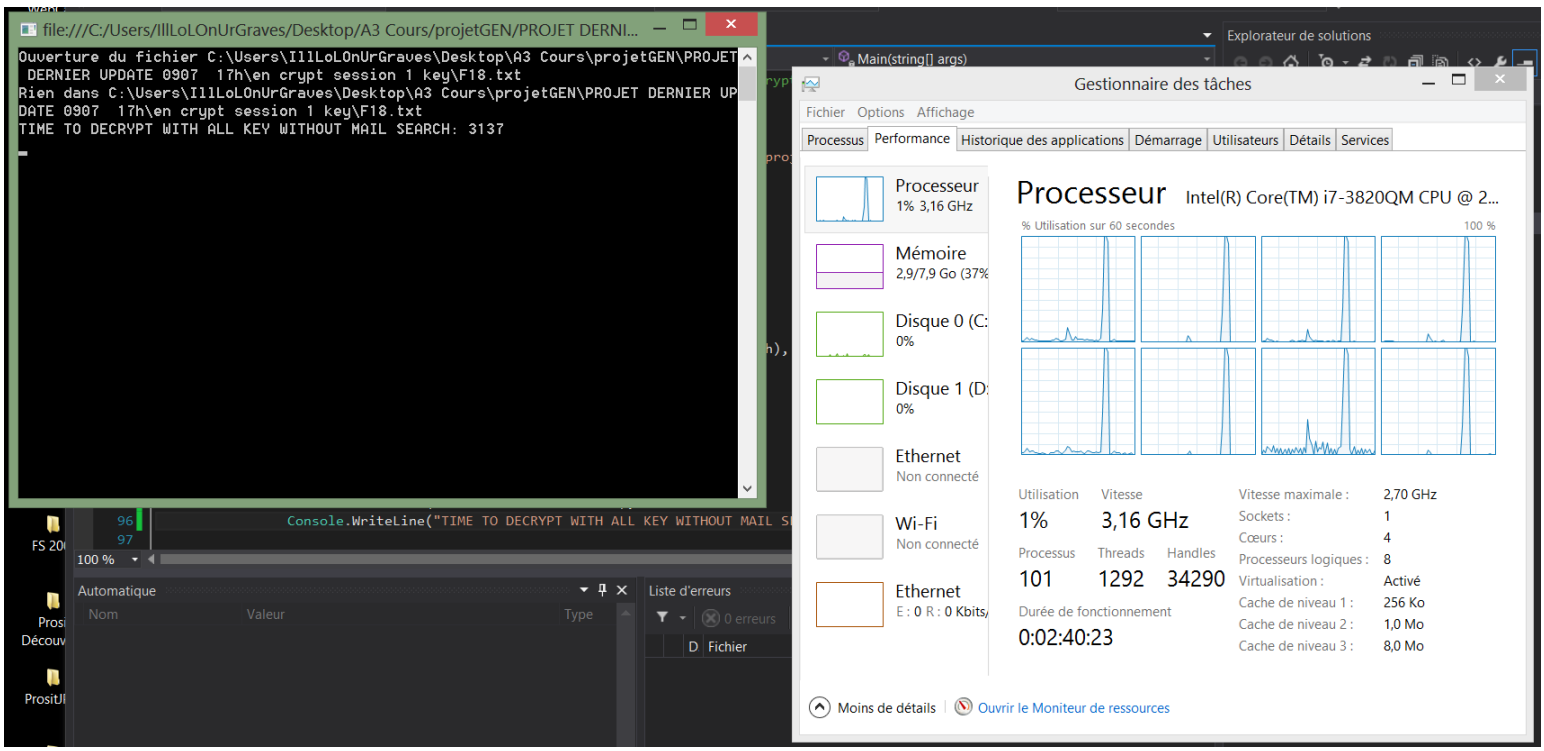
3. TESTS

La phase de test n'a pas vraiment eue lieu, à cause du manque de temps, nous avons dû procéder à des tests en même temps que nous développions, puis nous avons directement du décrypter les fichiers qui nous avaient étés donnés.

Cependant afin de vérifier l'efficacité du travail en parallèle et du premier algorithme, nous avons réalisé quelques essais, avec le même fichier.



Test 1 : Simple boucle for, trouve la clé en 10 secondes pour 100000 possibilités !



Test 2 : Parallèle for, trouve la clé en 3 secondes pour 100000 possibilités !

III. BILAN

A. BILAN DU PROJET

La façon dont ce projet a été amené était différente de ce dont nous avions l'habitude, ce qui nous a plu. Cependant, nous avons été surpris par l'ajout de travail au milieu du projet, ce qui nous a causé quelques soucis par la suite comme nous l'avons expliqué précèdement. Nous avons toutefois tenter de gérer au mieux les changements à effectuer.

Le nombre de ressources attribuées au projet était à notre goût le bon nombre. En effet, cela a permis une bonne division des tâches et ainsi une bonne synergie au sein du groupe.

B. BILANS PERSONNELS

1. JULES MONDOT

Ce projet m'a permis de comprendre les avantages d'une application distribuée quelques soit le langage utilisé. J'ai pu approfondir mes connaissances concernant les communications SOAP et j'ai aussi pu découvrir comment mettre en place une architecture impliquant des langages différents et nécessitant une programmation parallèle. Certaines fonctionnalités nous ont obligé à faire de nombreuses recherches, notamment sur la mise en place d'un duplex et la communication entre deux langages différents. C'est en grande partie pour cette raison que nous pouvons constater des écarts à la fin de notre période de projet. Cependant ces écarts ne sont pas très grands et je suis satisfait du travail fournis par notre groupe. J'ai apprécié travailler avec notre groupe de projet, l'ambiance était bonne et nous avons su tirer profit des différents points de vue et des phases de discussion sur les problèmes rencontrés. Le travail fournis par chacun nous permet de fournir une solution suffisamment complète pour que l'on ne soit pas déçu de notre travail.

2. LUCAS GLENADEL

Ce projet m'a permis de développer mes compétences en .Net et en architecture SOA et de remettre en œuvre mes connaissances en développement JavaEE pour le serveur. Le projet était très long et très complexe mais nous sommes arrivé à un résultat satisfaisant. En effet nous avons pas pu mettre en place l'architecture souhaitée. Nous restons conscients des écarts restants. Nous avons réfléchi à ce qu'il faut faire et si nous avions eu plus de temps je pense que nous aurions pu rendre un projet définitivement complet. Le travail en groupe a été très efficace, nous avons rapidement pris nos places. Nous nous sommes mutuellement apporté des connaissances et des méthodologies qui permettent de mieux appréhender les projets.

3. VINCENT BARRAIRON

Malgré des écarts au niveau des attendus, ce projet m'aura permis d'améliorer mes compétences en architecture logicielle, en .NET et de confirmer mes acquis en JEE (EJB /JMS/web services). Notre plus gros souci a été de connecter les plateformes entre elles et au moment où j'écris ces lignes nous sommes en train de faire tout notre possible afin de corriger le problème. J'ai apprécié travailler avec Jules, Lucas et Romain.

4. ROMAIN CASTANIE

J'ai beaucoup aimé la manière dont a été amené le projet, c'est une manière originale mais assez sympathique. Ce projet m'a permis de mieux comprendre tout ce qui est architecture d'une application distribuée et m'a également permis de revoir certains diagrammes UML (partie dans laquelle j'ai quelques lacunes). Concernant les différentes parties dont j'ai eu la charge, elles n'ont pas été trop problématique (mis à part un souci avec la mise en place de la BDD SQL Server). Enfin, concernant la synergie et la dynamique du groupe de travail, elles ont été très forte. En effet, une importante communication ainsi qu'une entre-aide mutuelle nous a permis de souvent nous sortir de situations délicates.