

# Énoncé du Travail Pratique 2

7 mars 2019

**Préparé par**  
Benjamin Lemelin

# 1 Résumé

Créez une application permettant de chiffrer et de déchiffrer un message en utilisant le [chiffrement de César](#). La clé de chiffrement devra être obtenue en appelant un serveur en ligne.

## 2 Conditions de réalisation

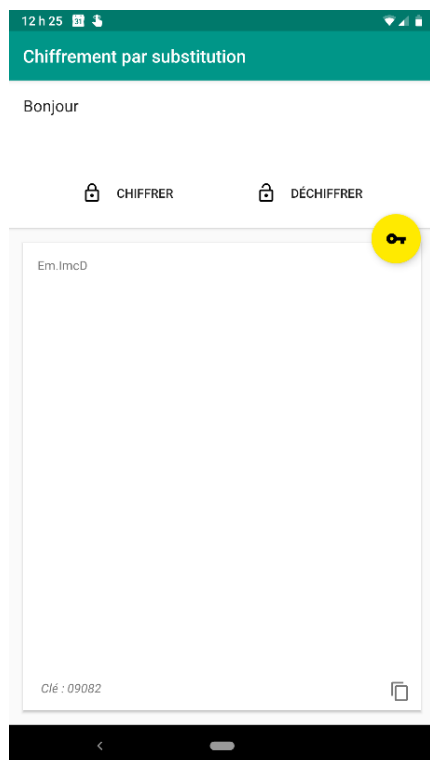
Valeur de la note finale	Type	Durée	Nombre de remises
15 %	En équipe	3 semaines	1

## 3 Spécifications

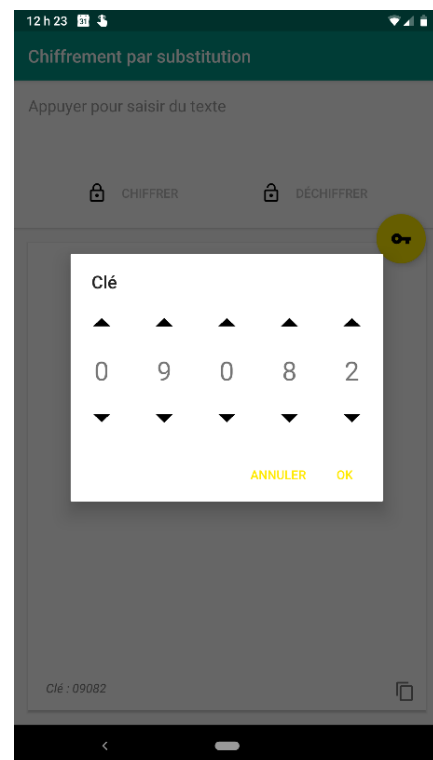
### 3.1 Projet Android Studio

Importez le projet fourni avec cet énoncé. Placez-le dans un dépôt privé Git ([GitHub](#), [GitLab](#) ou [BitBucket](#)). Donnez en accès à votre professeur. Tout le code doit être en Java.

### 3.2 Interface utilisateur



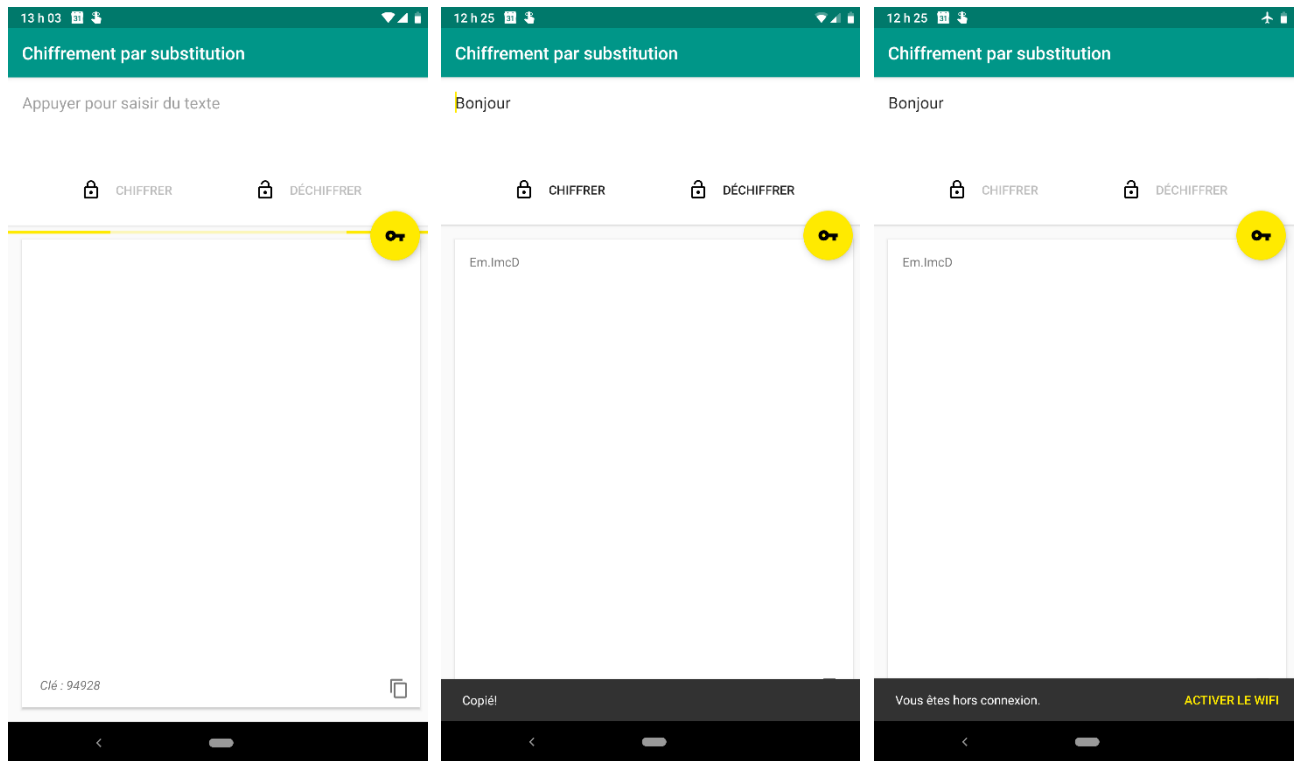
Interface de chiffrement/déchiffrement



Dialogue de sélection de clé

L'interface est fournie. Il ne doit y avoir qu'une seule activité. Le [thème](#) de l'application (couleurs, images) peut être modifié à votre guise. L'utilisateur saisit du texte en haut de l'écran et appuie sur « Chiffrer » ou « Déchiffrer ». Le résultat est affiché dans la [carte](#) en bas.

Le [bouton rond](#) et jaune affiche le dialogue de sélection de clé. La clé est immédiatement téléchargée lorsque l'utilisateur confirme son choix et elle est conservée pour les chiffrements et déchiffrements futurs. Notez qu'au lancement de l'application, il est impossible d'effectuer le chiffrement/déchiffrement tant qu'il n'y a [pas de clé](#). Dans ce cas, les deux boutons correspondants doivent être [désactivés](#).




Barre de progression

Copie

Message d'erreur

Lors du téléchargement, une [barre de progression](#) doit [apparaître](#). La barre de progression n'est qu'une animation et n'affiche pas la progression réelle. En cas d'erreur de réseau, un [message d'erreur](#) correspondant doit s'afficher. Dans le cas d'une [erreur de connectivité](#), le message doit [contenir un bouton](#) permettant [d'accéder](#) aux [options réseau](#). Dans le cas d'une [erreur serveur](#), faites patienter l'utilisateur.

L'interface doit [filtrer](#) les caractères en entrée en acceptant uniquement les lettres de l'alphabet, les espaces et les points. Une fois le texte chiffré ou déchiffré, le bouton «  » permet de copier le résultat dans le [presse-papier](#). Cela affiche aussi une confirmation.

Le numéro de la clé courante est affiché en tout temps au bas de l'écran. Les numéros ont toujours 5 caractères et débutent, au besoin, [par des « 0 »](#). Le format est important.

### 3.3 Chiffrement et déchiffrement

L'application utilise un [chiffrement par substitution](#) où chaque lettre est remplacée par une autre. Les classes créées pour ce besoin doivent être [testées](#) et [documentées](#). Les clés de chiffrement sont constituées de deux tableaux de caractères. La correspondance se fait via leur position.

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	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	.
x	T	H	I	a	q	Z	O	X	V	z	v	S	M	R	L	h	m	B	l	d	e	s	K	N	n	Q	r	p	D	o	I	g	W	b	.	G	U	E	w	C	f	P	k	A	J	t	F	c	y	u	j	Y

### 3.4 Obtention des clés

Les clés de chiffrement doivent être obtenues en effectuant un appel à [ce service web](#). Chaque clé est unique et identifiée par un numéro.

```
https://m1t2.blemelin.tk/api/v1/key/{id}
```

Il est possible de l'essayer dans un navigateur. Par exemple, pour le « id » « [01977](#) » :

```
{
  "id": 1977,
  "outputCharacters": "xTHIaqZOXVzvSMRLhmB ldesKNnQrpDoigWb.GUEwCfPkAJtFcyujY",
  "inputCharacters": "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ ."
}
```

Pour plus d'informations sur le fonctionnement du service et la structure des données, consultez [sa documentation](#).

Utilisez une tâche asynchrone pour [appeler](#) ce service web. Ce dernier retourne du « [JSON](#) », et donc, vous devrez effectuer de la désérialisation avec [Jackson](#) pour obtenir une clé utilisable.

!!!! ATTENTION !!!!

Le serveur est ouvert de **8h à 20h** seulement, et ce, pour toute la durée du travail. En dehors de ces heures, veuillez déployer par vous-même le serveur, fourni sur LÉA. Vous devrez alors modifier l'url du serveur pour pointer vers le vôtre en utilisant votre adresse IP et le port 8080.

Par exemple :

```
https://192.168.1.20:8080/api/v1/key/{id}
```

### 3.5 Objets « [ObjectMapper](#) » et « [OkHttpClient](#) »

Ces objets sont déjà créés pour vous dans la méthode « `createDependencies` » de « `MainActivity` ». Pour que les tests fonctionnent, assurez-vous d'utiliser ces objets et de **ne pas les recréer par vous-même**.

### 3.6 Interaction avec les autres applications

L'application doit pouvoir chiffrer ou déchiffrer du texte [en provenance](#) de [n'importe quelle application](#). Le dialogue de sélection de clé doit alors s'ouvrir au lancement. Si l'utilisateur annule, [l'application doit se fermer](#). Sinon, l'application doit télécharger la clé et procéder normalement.

Il n'y a aucune option de partage vers d'autres applications.

Partager



Mon disque  
benjamin.le



Mon disque  
blemelin@ce



Chiffrement  
par



Post on  
Reddit



Keep



Ajouter à  
Firefox



Google+



Gmail





Traduction



Discord

### 3.7 Liste des fonctionnalités

Description
Une clé aléatoire doit être choisie au lancement de l'application.
Le bouton « Chiffrer » doit utiliser la clé actuelle pour chiffrer le texte.
Le bouton « Déchiffrer » doit utiliser la clé actuelle pour déchiffrer le texte.
Seuls les lettres de l'alphabet, les espaces et les points sont acceptés en entrée.
Le bouton «  » doit permettre de choisir une nouvelle clé.
Confirmer le choix d'une nouvelle clé doit la télécharger et la conserver pour usage futur.
Le numéro de la clé doit être affiché en bas de l'écran, avec le bon formatage.
Les boutons « Chiffrer » et « Déchiffrer » doivent être désactivés en l'absence de clé.
Le bouton «  » doit copier le résultat dans le presse-papier.
Il est possible de partager du texte à l'application en vue d'être chiffré ou déchiffré.
Tout texte partagé à l'application doit être affiché en entrée, comme si l'utilisateur l'avait saisi.
Le dialogue de choix de clé doit être affiché lorsque du texte est partagé à l'application.
Si l'utilisateur annule le choix d'une clé après un partage, l'application doit se fermer.
En cas d'erreur de connectivité, un message d'erreur comportant un bouton pour accéder aux options de l'appareil doit être affiché.
En cas d'erreur de serveur, un message d'erreur doit être affiché pour faire patienter l'utilisateur.

### 3.8 Liste des spécifications techniques

Description
L'usage du langage « Java » est obligatoire.
L'état de l'application doit être conservé au travers des changements d'orientation.
Le dialogue de sélection de clé doit rester ouvert après un changement d'orientation.
Les éléments publics de la couche « Modèle » doivent être documentés.
La couche « Modèle » doit être complètement testée unitairement.
Les couches « Vue » et « Contrôleur » doivent être testées avec Espresso. Ces tests sont fournis.
La clé de chiffrement doit être obtenue via le service en ligne.
L'usage de « OkHttp » pour les appels réseau est obligatoire.
L'usage de « Jackson » pour la désérialisation des données est obligatoire.
Tout traitement lourd doit être effectué via une tâche asynchrone.
Une rétroaction visuelle doit être affichée lors de traitements lourds.

### 3.9 Liste d'autres demandes

Description
L'interface de l'application doit supporter l'orientation portrait et paysage.
L'application doit être traduite en français et en anglais.

## 4 Modalités de remise

Remettre sur LÉA un fichier texte incluant :

1. L'adresse vers le dépôt Git
2. Les matricules de chaque membre de l'équipe

Une seule équivalent à une pénalité de 15 %. Au-delà de ce délai, le travail la note « 0 » est attribuée.

## 5 Évaluation

Éléments
<b>Fonctionnalités</b> (incluant, mais sans s'y limiter) : <ul style="list-style-type: none"><li>• Clé aléatoire choisie au lancement de l'application.</li><li>• Chiffrement et déchiffrement fonctionnels.</li><li>• Seuls les lettres de l'alphabet, les espaces et les points sont acceptés en entrée.</li><li>• Il est possible de choisir une nouvelle clé.</li><li>• Le numéro de la clé est affiché en bas de l'écran, avec le bon formatage.</li><li>• Boutons « Chiffrer » et « Déchiffrer » désactivés en l'absence de clé.</li><li>• Il est possible de copier le résultat dans le presse-papier.</li><li>• Il est possible de partager du texte à l'application pour le chiffrer ou le déchiffrer.</li></ul>
<b>Interface utilisateur</b> (incluant, mais sans s'y limiter) : <ul style="list-style-type: none"><li>• L'interface doit respecter les maquettes.</li><li>• L'interface doit être disponible en anglais et en français.</li></ul>
<b>Service Web</b> (incluant, mais sans s'y limiter) : <ul style="list-style-type: none"><li>• Les clés sont obtenues à partir du service en ligne.</li><li>• Toutes les erreurs possibles sont gérées correctement, rétroaction incluse.</li></ul>
<b>Tests unitaires et d'interface</b> (incluant, mais sans s'y limiter) : <ul style="list-style-type: none"><li>• La couche modèle testée intégralement.</li><li>• Les tests unitaires s'exécutant avec succès.</li><li>• Les tests d'interface s'exécutant avec succès.</li><li>• Tous les tests sont robustes, fiables, complets et lisibles.</li></ul>
<b>Qualité générale de l'application mobile</b> (incluant, mais sans s'y limiter) : <ul style="list-style-type: none"><li>• Changement d'orientation et d'application supporté, sans perte de données.</li><li>• Traitements lourds toujours effectués sur une tâche asynchrone.</li><li>• Présence de rétroaction visuelle lors de traitements lourds.</li></ul>
<b>Documentation du code</b> (incluant, mais sans s'y limiter) : <ul style="list-style-type: none"><li>• Les éléments de la couche « Modèle » doivent être documentés intégralement.</li></ul>

**Qualité générale du code** (incluant, mais sans s'y limiter) :

- Logique bien pensée, juste, et « non patché ».
- Découpage adéquat du code en classes, méthodes et packages.
- Architecture adéquate au type d'application développée.
- Séparation raisonnable des responsabilités entre les classes.
- Respects des standards du langage de programmation.
- Nommage clair et sans ambiguïté des éléments.
- Utilisation de constantes, lorsque nécessaires.
- Commentaires compensant uniquement le manque d'expressivité du code.
- Respect des bonnes pratiques de programmation générales.
- Code propre, sans résidus et facilement lisible.
- Aucune erreur ni avertissement à la compilation.

**Qualité générale du travail** (incluant, mais sans s'y limiter) :

- Configuration Gradle fonctionnelle.
- Respect des consignes de remise.
- Aucun fichier inutile remis avec le projet.
- Travail remis via l'outil gestion de code source Git.

La qualité de la langue française fait partie de l'évaluation. Chaque faute de français retire 0,5 % à la note finale jusqu'à concurrence de 20 %.