

1. Introduction

Dans ce chapitre, nous présentons une étude comparative entre les différents algorithmes de chiffrement appliqué sur les fichiers son de type WAV, nous avons établi une comparaison sur la qualité et la vitesse de l'opération de chiffrement. Nous avons utilisé un ordinateur Intel (R) core 2 duo cadencés à 2.00 MHz avec une RAM de 2.00 Go et un système d'exploitation vista.

2. Paramètres de comparaison

La comparaison va se faire sur plusieurs points et suivant certains critères :

- Qualité de chiffrement.
- Le temps de chiffrement et de déchiffrement.
- La variation de l'amplitude.

3. Présentation de l'application

❖ Langage utilisé

Le langage choisi pour réalisation de notre application est le **BORLAND C++ BUILDER6**. Ce choix repose sur le fait que Borland possède tout la puissance du langage C++ orienté objet comme il offre la possibilité de développer rapidement des applications sous Windows grâce à ses différentes bibliothèques. Il permet la création instantanée des interfaces utilisateurs car il offre une gestion de l'interface. [s27]

❖ L'interface de l'application

Description de l'application (interface et composants) : la fenêtre d'interface de notre logiciel est présentée ci-dessus par la figure :

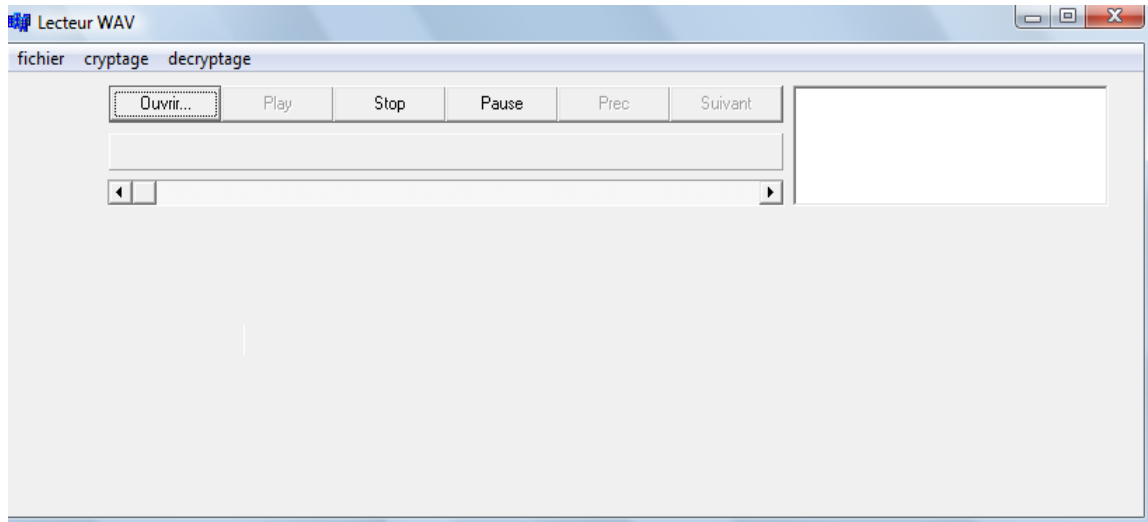
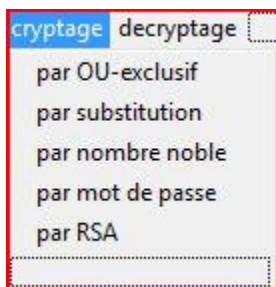
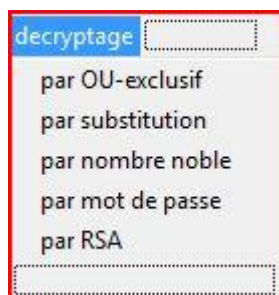


Figure 5.1 : interface de l'application

- Le menu de cryptage contient les algorithmes suivants



- Le menu de décryptage



- **Le bouton ouvrir** : permet d'ouvrir un fichier son
- **Le bouton play** : permet de jouer des fichiers audio
- **Le bouton stop** : permet d'arrêter la music
- **Le bouton pause** : pour faire une pause dans la lecture des fichiers audio

4. Les résultats obtenus

4.1. Résultats de temps de chiffrement et de déchiffrement de son par les différents algorithmes de cryptage

			Temps de chiffrement par algorithme				
	Taille	Type	substitution	Nombre noble	XOR	Mot de passe	RSA
Fichier 1	652 ko	Parole	0.6090	0.3120	0.2340	0.2600	0.7710
Fichier 2	810 ko	Music	0.6710	0.3620	0.2990	0.3060	0.8430

Tableau 5.1 : temps de chiffrement du son par les différents algorithmes de cryptage



Figure 5.2 : le temps de chiffrement de son par les différents algorithmes de cryptage

Remarque

- Le temps de chiffrement est changé par le changement de la taille de fichier à chiffrer.
- Chaque fois en augmente dans la taille de fichier, la vitesse de l’opération de chiffrement sera automatiquement augmenté (le temps de chiffrement dépende de la taille de fichier audio)
- D’après les résultats obtenue, l’algorithme ou-exclusif c’est l’algorithme le plus rapide par contre l’algorithme RSA à clé publique c’est l’algorithme le plus lent.

◆ **Opération de déchiffrement**

	Temps de déchiffrement par algorithme				
	substitution	Nombre noble	XOR	Mot de passe	RSA
Fichier 1	0.4680	0.3060	0.2310	0.2514	0.7330
Fichier 2	0.5770	0.3231	0.2930	0.2880	0.8290

Tableau 5.2 : temps de déchiffrement du son par les différents algorithmes de cryptage

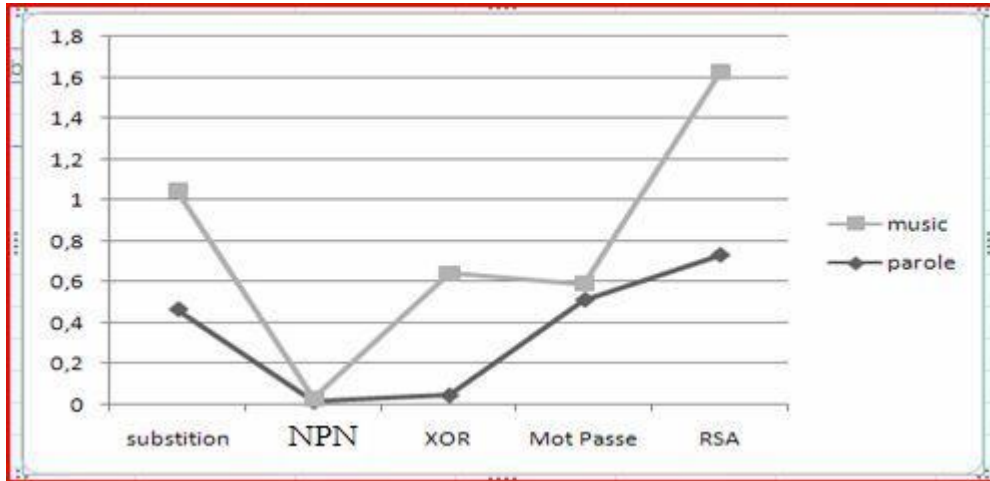


Figure 5.3 : Le temps de déchiffrement de son par les différents algorithmes de cryptage.

Remarque

- Nous observons que l’opération de déchiffrement par l’algorithme XOR donne un meilleur temps de déchiffrement cela revient à la simplicité de l’opération de XOR. Par contre l’algorithme RSA est considéré comme l’algorithme de déchiffrement le plus lourd.
- Nous remarquons aussi que le temps de déchiffrement est plus rapide que le temps de chiffrement.

4.2. Résultats de la qualité de chiffrement de son par les différents algorithmes de cryptage

	substitution	Nombre noble	XOR	Mot de passe	RSA
parole	bonne	bonne	mauvaise	mauvaise	Très bonne
music	Très bonne	bonne	mauvaise	mauvaise	bonne

Tableau 5.3 : la qualité de chiffrement du son par les différents algorithmes de cryptage

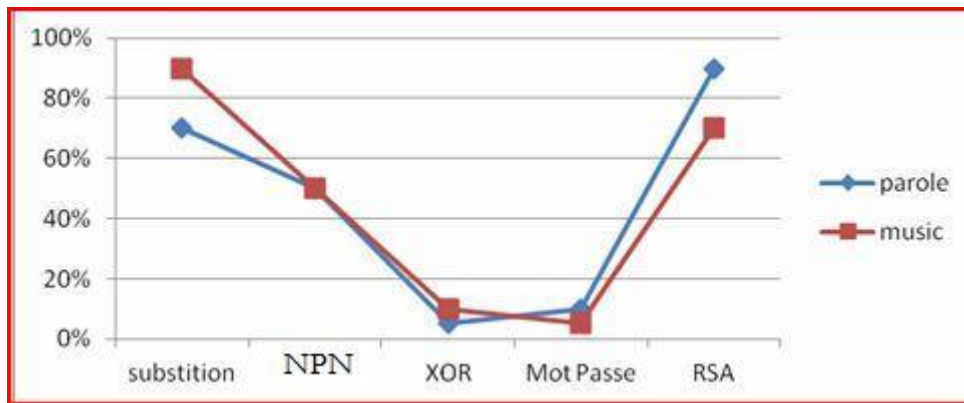


Figure 5.4 : la qualité de chiffrement du son par les différents algorithmes de cryptage

Remarque

- Dans le cryptage de la music ou de la parole, plus le son est bruité, la qualité de chiffrement est meilleure.
- D'après le tableau et les résultats obtenus, nous avons remarqué que la qualité de cryptage de la parole est très bonne dans l'algorithme RSA. Par contre l'algorithme de chiffrement par mot de passe et XOR donne une mauvaise qualité de chiffrement
- Même l'algorithme de substitution et l'algorithme des nombres nobles donnent une bonne qualité de chiffrement des fichiers music.

4.3. L'amplitude de chaque fichier crypté de chaque algorithme

➤ **Présentation de logiciel**

GoldWave est un outil d'édition de fichiers audio encodés dans différents formats.

➤ **Quelques fonctionnalités exceptionnelles de GoldWave :**

- Analysez le spectre complet de la voix humaine et des bruits d'animaux.
- Affiche la représentation des ondes acoustiques
- Convertit les fichiers dans différents formats dont WAV, WMA, MP3, OGG.
- Permet d'appliquer différents filtres sonores et effets.
- Utilisez l'outil de lecture de CD afin d'obtenir des copies numériques haute qualité de vos disques dans les formats WAV, WMA, MP3 et OGG.

GoldWave est un outil puissant pour le traitement audio proposant une interface dynamique complète. [s28]

➤ L'interface de logiciel

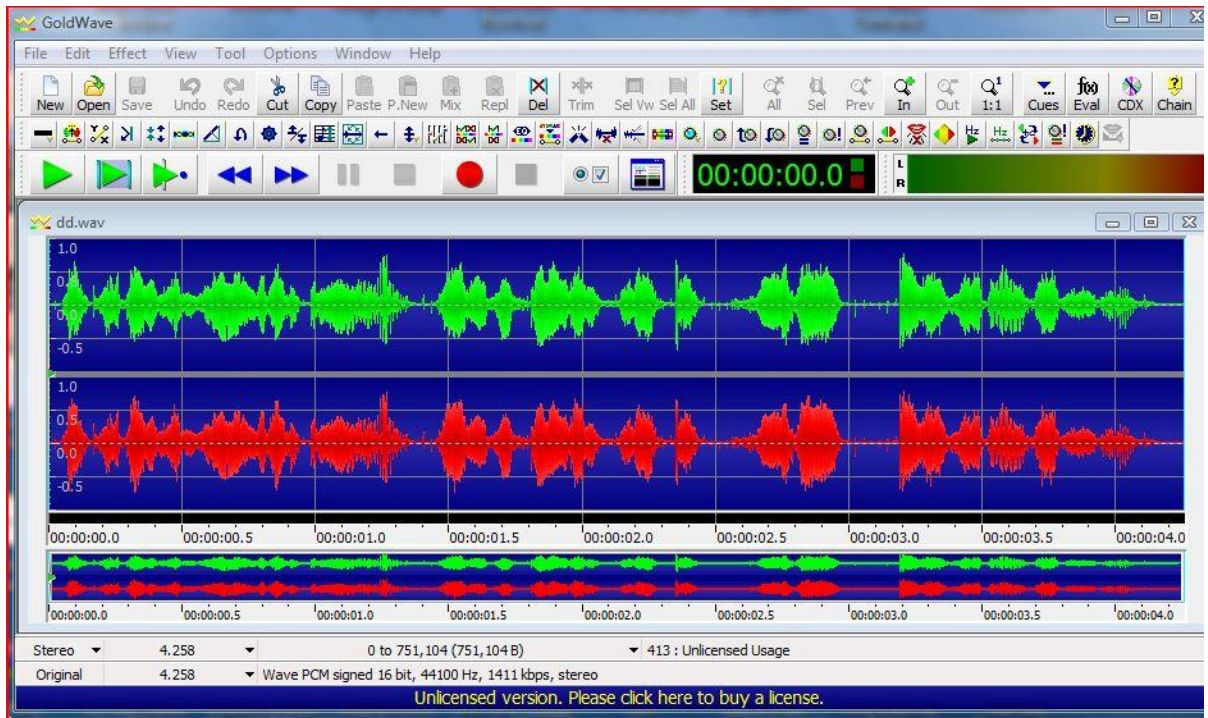
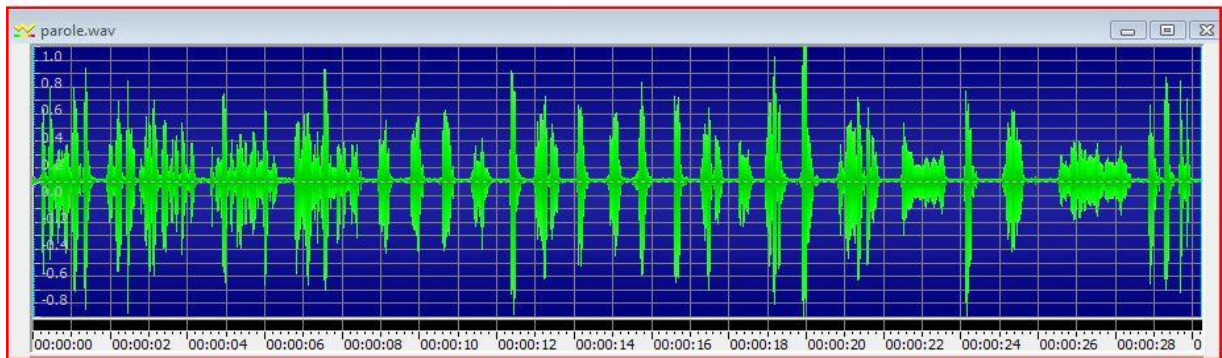
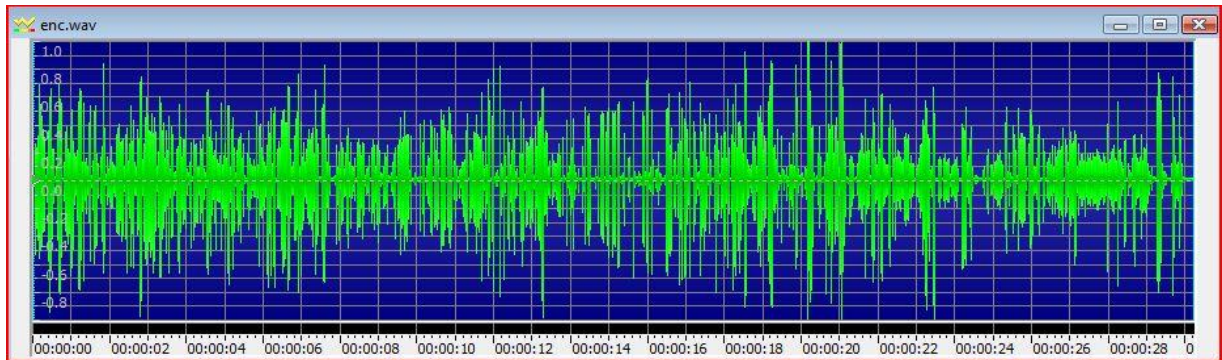


Figure 5.5 : l'interface de logiciel GOLDEWARE

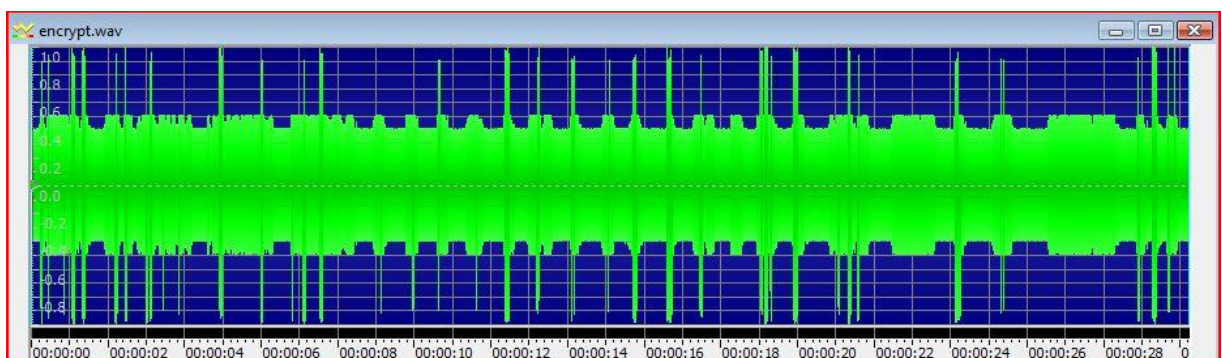
- L'amplitude de fichier origine (parole.wav)



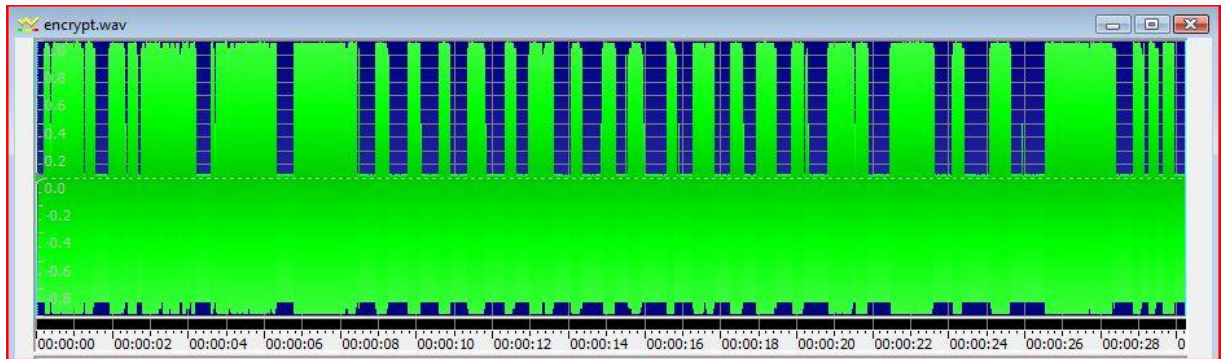
- L'amplitude de fichier crypté par nombre noble



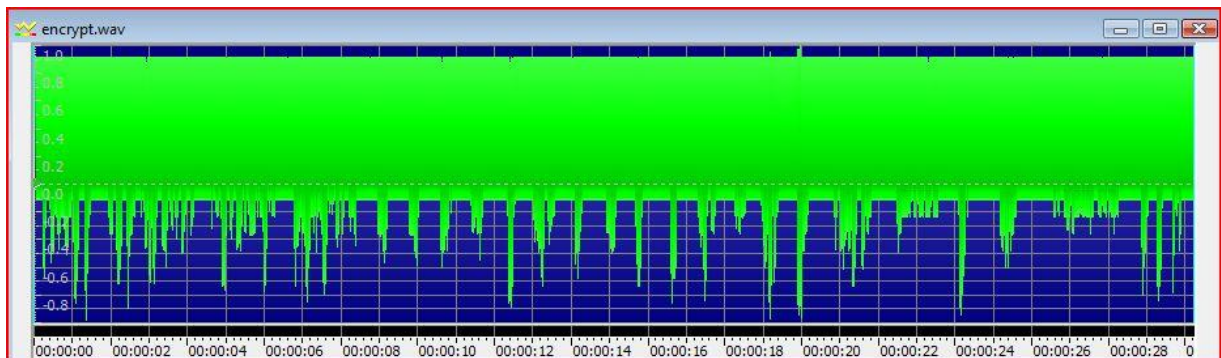
- L'amplitude de fichier crypté par l'algorithme XOR



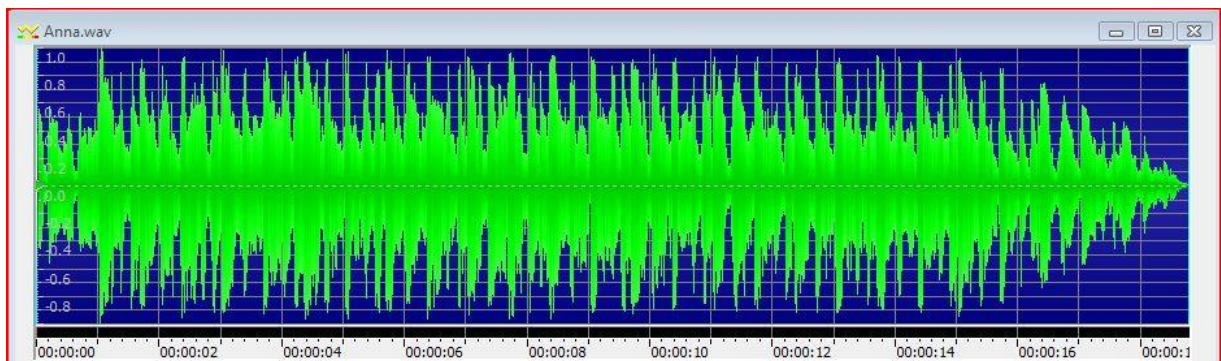
- L'amplitude de fichier crypté par l'algorithme RSA



- L'amplitude de fichier crypté par mot de passe



- L'amplitude de fichier crypté par substitution



Remarque

La variation de l'amplitude entre le fichier originale audio et le fichier crypté donne le niveau de la qualité de l'opération de chiffrement.

5. Conclusion

Dans ce chapitre, nous avons présenté les différents résultats obtenus par l'opération de cryptage des fichiers audio de format wav par quelques algorithmes de chiffrement comme XOR, RSA et nombre noble.

Notre objectif de cette implémentation se base sur la performance et l'efficacité de chaque type d'algorithme de cryptage appliqué dans le chiffrement des fichiers son (fichier wav).

Les critères de performance sont basés sur deux facteurs : le temps et la qualité de son crypté.

L'algorithme RSA (qui est un algorithme standard) et l'algorithme nombre noble donnent une meilleur qualité dans le chiffrement des fichiers son. Par contre l'algorithme XOR est considéré comme l'algorithme le plus rapide dans le temps de chiffrement/déchiffrement.