	Lycée de l'Hyrôme - Chemillé	2013 - 2014
	RC4	Langage C++
BTS IRIS		TP

Objectifs

- Savoir crypter et décrypter.
- Savoir utiliser la STL.
- Savoir manipuler les fichiers en utilisant la classe fstream.

Ressources disponibles

- Un PC.
- Un EDI.

1. Présentation

Nous allons réaliser un programme qui permet de crypter et de décrypter un fichier en utilisant l'algorithme RC4.

Le principe de l'algorithme RC4 est fourni en annexe.

Le programme comportera 3 classes : Random, RC4 et FichierCrypte.

2. La classe Random

2.1. Présentation

Cette classe permet de générer un tableau de valeur aléatoire.

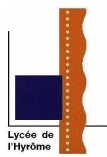
Fonctionnalités principales :

- . On peut spécifier la fourchette dans laquelle seront choisis les nombres aléatoires.
- . On peut spécifier la taille du tableau.

Pour les autres possibilités se référer au code source

2.2. Remarque

Le code source de cette classe vous est fourni.

	Lycée de l'Hyrôme - Chemillé	2013 - 2014
	RC4	Langage C++
BTS IRIS		TP

3. La classe RC4

3.1. Présentation

Cette classe permet de réaliser un cryptage en utilisant l'algorithme RC4.
Elle peut également générer une clé qui servira au cryptage.

3.2. Fichier « RC4.h »

Ce fichier vous est fourni en annexe.

Remarque :

tailleTableauEtat sera égal à 256.

3.3. Fichier « RC4.cpp »

RC4(unsigned int valTailleCle=0) fait appel à :

- . genereCle
- . initCodageDecodage

Si la valTailleCle est égal à 0, elle sera initialisée à une valeur aléatoire comprise entre 40 et 255.

RC4(unsigned char *valMaCle,int valTaille) fait appel à :

- . initCodageDecodage

RC4(vector <unsigned char> valMaCle) fait appel à :

- . initCodageDecodage

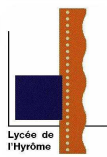
void initCodageDecodage() fait appel à :

- . melangeTableauEtat

Utilise l'algorithme « generate » de la STL (fait appel à Sequence()).

unsigned char chiffrage() fait appel à :

- . swap

	Lycée de l'Hyrôme - Chemillé	2013 - 2014
	RC4	Langage C++
BTS IRIS		TP

void genereCle()

Utilise un objet de type Random

vector <unsigned char> litCle()

unsigned int litTailleCle()

void melangeTableauEtat() fait appel à :
 .swap

void swap(unsigned char* val1,unsigned char* val2)

3.4. Travail demandé

Réaliser la classe et la tester.

4. La classe FichierCrypte

4.1. Présentation

Cette classe permet de crypter ou de décrypter un fichier en utilisant l'algorithme RC4.
La clé de cryptage (qui servira au décryptage) est insérée au milieu des données cryptées.

4.2. Fichier « FichierCrypte.h »

Ce fichier vous est fourni en annexe.

4.3. Fichier « FichierCrypte.cpp »

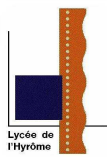
Le squelette de la classe FichierCrypte est fourni.

FichierCrypte(string valSource,bool valCryptage=true,string valExtension="") fait appel à :
 .nomFichierDestination

~FichierCrypte()

void decrypteFichier()

Utilise un objet de type RC4

	Lycée de l'Hyrôme - Chemillé	2013 - 2014
	RC4	Langage C++
BTS IRIS		TP

void crypteFichier()

Utilise un objet de type RC4

bool controleExtensionFichier(string valExtension)

void nomFichierDestination(string valExtension) fait appel à :
 . controleExtensionFichier

4.4. Travail demandé.

Réaliser la classe et la tester.

5. Programme principal

Ce programme nommé « princi.cpp » sera un programme de test qui permettra de crypter, puis de décrypter, un fichier nommé « essai.txt » qui sera créé sous un éditeur quelconque.

Tester le programme complet.