A  Homework Report on

Password Cracking

In the partial fulfilment of the academic requirements for

M. S (Cyber Security) under Wright State University

By

Sudarshan Govindarajan               (U00793458)

**Implementation of the System**

The following is the report that illustrates the implementation of the password cracking obtained by expanding the existing system.

Most of the java class files are same as provided by the author.

**Dictionary attack**

**DictionaryAttack.java**

/\*

\* Basic code provided by the @author lingg

\* The following is the extended code to crack the password by Dictionary Attack

\*/

package Cracker;

import java.io.BufferedReader;

import java.io.File;

import java.io.FileNotFoundException;

import java.io.FileReader;

import java.io.IOException;

import java.io.Reader;

import java.util.zip.ZipException;

import de.idyl.winzipaes.AesZipFileDecrypter;

import de.idyl.winzipaes.AesZipFileEncrypter;

import de.idyl.winzipaes.impl.AESDecrypter;

import de.idyl.winzipaes.impl.AESDecrypterBC;

import de.idyl.winzipaes.impl.AESEncrypter;

import de.idyl.winzipaes.impl.AESEncrypterBC;

import de.idyl.winzipaes.impl.ExtZipEntry;

public class DictionaryAttack {

public static void encrypt(String inputFilename, String zipFilename, String password)

throws Exception {

AESEncrypter encrypter = new AESEncrypterBC();

AESEncrypter encrypter2 = new AESEncrypterBC();

AesZipFileEncrypter.zipAndEncrypt(

new File(inputFilename), new File(zipFilename), password, encrypter);

}

public static void decrypt(String zipFilename, String outputFilename, String password)

throws Exception {

AESDecrypter decrypter = new AESDecrypterBC();

AesZipFileDecrypter dec = new AesZipFileDecrypter(new File(zipFilename), decrypter);

ExtZipEntry entry = dec.getEntryList().get(0); // assumes only one item is in the zip file

dec.extractEntry(entry, new File(outputFilename), password);

//When appropriate password is used ZipException won't be raised hence execution will be in this function

dec.close();

//Printing the password which is used to decrypt the file

System.out.println("Password is :"+password);

//Exiting from the program once the password is printed.

System.exit(0);

}

/\*\*

\* @param args the command line arguments

\*/

public static void main(String[] args) throws Exception{

// TODO code application logic here

//encrypt("test.txt", "test.zip", "joyce");

//Creating the instance of the file blink.txt and object name is file

File file=new File("blink.txt");

BufferedReader reader; // To read text from input stream

try {

FileReader fr=new FileReader(file); // To read contents from file

reader=new BufferedReader(fr);

try {

//reads the line of the text and until the last line

while(reader.readLine()!=null)

{

try {

// Trying to decrypt the file using the password obtained from Dictionary

try

{

decrypt("test.zip", "test2.txt", reader.readLine());

}

//When wrong password is used ZipException is created and which is handled

catch(ZipException ze)

{

}

}

//Handling IO Exception

catch (IOException e) {

// TODO Auto-generated catch block

e.printStackTrace();

}

}

//Handling IO Exception

} catch (IOException e) {

// TODO Auto-generated catch block

e.printStackTrace();

}

//Handing FileNotFoundException

} catch (FileNotFoundException e) {

// TODO Auto-generated catch block

e.printStackTrace();

}

}

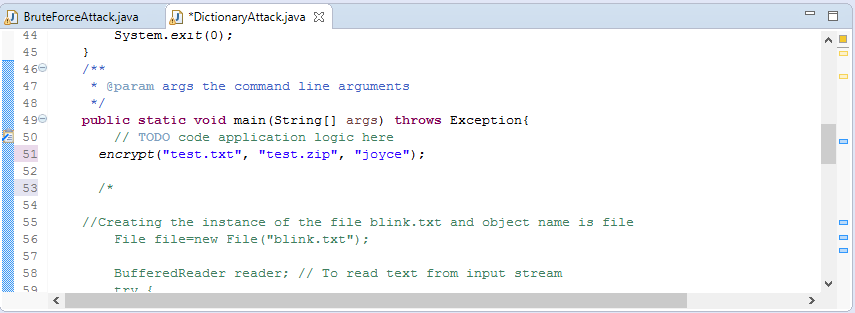
}

**Execution Steps:**

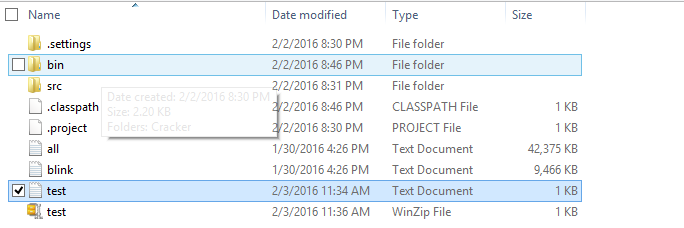
**Start Eclipse**

**File->Import->General->ExistingProjectsintoWorkSpace->PasswordCracker-Dictionary**

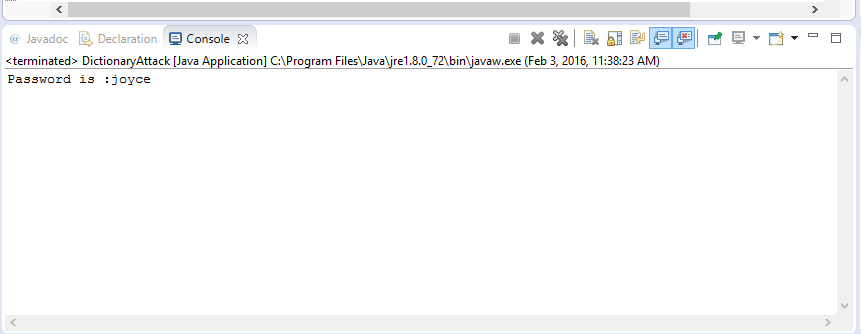
1. Create a notepad with name test.txt in the folder that which has bin ,src files of PasswodCracker-Dictionary Attack and having some content for example “Sun rises in the east”
2. Try to execute the program (Note: Only encrypt function needs to executed in main function)



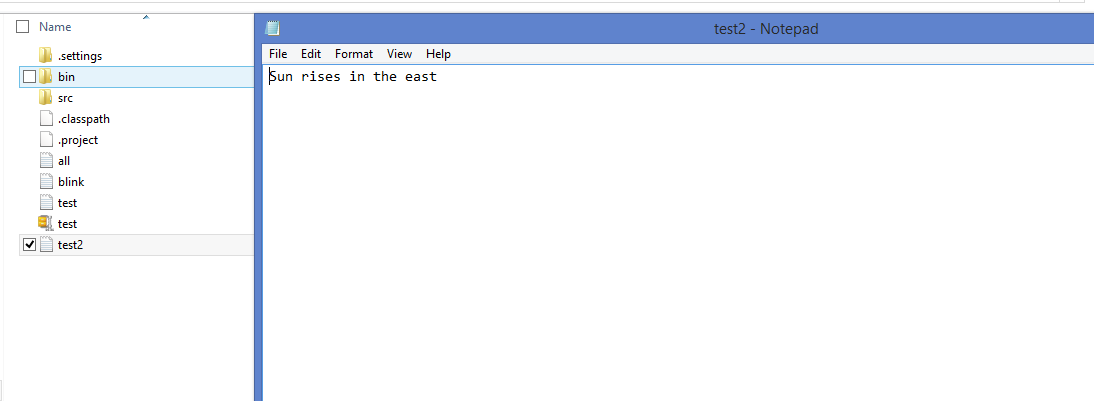
An encrypted file using the password “joyce” is created.



1. Try to Decrypt the program



1. A file test2 is created with the contents of test file.



**BruteForceAttack**

BruteForceAttack.java

/\*

\* Basic code provided by the @author lingg

\* The following is the extended code to crack the password by BruteForceAttack Method

\*/

import java.io.File;

import java.util.zip.ZipException;

import de.idyl.winzipaes.AesZipFileDecrypter;

import de.idyl.winzipaes.AesZipFileEncrypter;

import de.idyl.winzipaes.impl.AESDecrypter;

import de.idyl.winzipaes.impl.AESDecrypterBC;

import de.idyl.winzipaes.impl.AESEncrypter;

import de.idyl.winzipaes.impl.AESEncrypterBC;

import de.idyl.winzipaes.impl.ExtZipEntry;

public class BruteForceAttack {

public static void encrypt(String inputFilename, String zipFilename, String password)

throws Exception {

AESEncrypter encrypter = new AESEncrypterBC();

AESEncrypter encrypter2 = new AESEncrypterBC();

AesZipFileEncrypter.zipAndEncrypt(

new File(inputFilename), new File(zipFilename), password, encrypter);

}

public static void decrypt(String zipFilename, String outputFilename, String password)

throws Exception {

AESDecrypter decrypter = new AESDecrypterBC();

AesZipFileDecrypter dec = new AesZipFileDecrypter(new File(zipFilename), decrypter);

ExtZipEntry entry = dec.getEntryList().get(0); // assumes only one item is in the zip file

dec.extractEntry(entry, new File(outputFilename), password);

dec.close();

System.out.println("password is:"+password);

System.exit(0);

}

/\*\*

\* @param args the command line arguments

\*/

public static void main(String[] args) throws Exception{

// TODO code application logic here

// encrypt("test.txt", "test.zip", "abcd");

String alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";

char[] value=alphabet.toCharArray();

int len; //Length of the password

System.out.println("Brute force method is carried out for password length between 4 and 15");

int minlen=4; //Minimum length of the password

int maxlen=15; // Maximum length of the password

String pass="";

int i,j,k;

for(len=minlen;len<=maxlen;len++)

{

int[] flag=new int[len]; //Declaring the array which indicates the length of the password

// Carrying out the Brute force attack

// Checking the condition to carry out the BruteForce till the last value(flag[0]<61) since password contains lowercase letters ,uppercase letters and numericals and total count of letters is 62

while(flag[0]<value.length)

{

pass="";

// To obtain a password of certain length i.e if length 5 password will be abcde or aaaaa

for(k=0;k<len;k++)

{

pass=pass+value[flag[k]];

}

//Obtaining the next value for password, by moving to next character in value array , initially increment only the last letter of the password.

flag[len-1]++;

try

{

decrypt("test.zip", "test2.txt", pass);

}

catch(ZipException ze)

{

}

// Increment to next position once end value at a certain position(e.g if aa9 is reached then moving to ab0) in password has been reached

for(i=len-1;i>0;i--)

{

if(flag[i]>value.length-1)

{

flag[i-1]++; //By shifting 1 position to the left of the password and incrementing to next value.

flag[i]=0; // Once last value of a certain position further no changes are made to that position

}

}

}

}

}

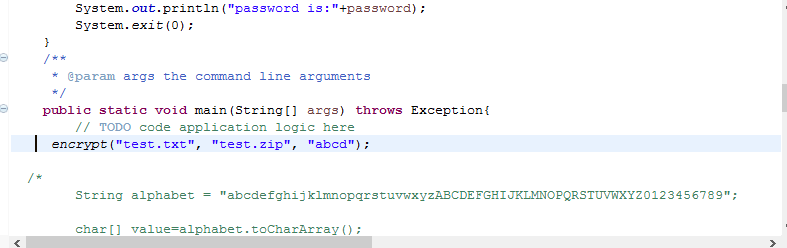
}

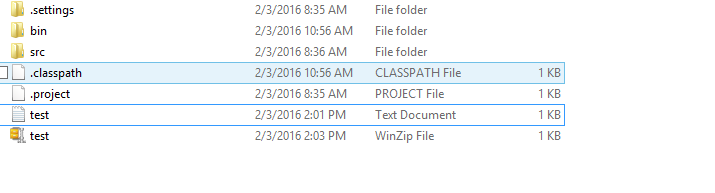
**Execution Steps:**

**Start Eclipse**

**File->Import->General->ExistingProjectsintoWorkSpace->PasswordCracker-Dictionary**

1. Create a notepad with name test.txt in the folder that which has bin ,src files of PasswodCracker-BruteForce and having some content for example “Sun sets at the east”.
2. Try to execute the program (Note: Only encrypt function needs to executed in main function)





A encrypted file with the password “abcd” is created.

1. Try to decrypt the file, the file once decrypted will output the file

