

Forum: [Hack Forums](#)

Thread: [How can I decrypt that and Encrypt techniques ?](#)

vitaminic - September 25, 2014, 3:03 pm

Hey guys , I just tried to make an encryption , to be honest with random numbers . I just wrote some random things just to make it a big enough number and small enough to fit in a serializable file's name .

The problem is that I am so idiot that I did not think about decrypting , I just wrote numbers and numbers to make it impossible to decrypt that easily , but how the hell am I going to make a decrypt method if I made that impossible for myself ?

I wrote this :

```
Code public static long encryptNumber(String fullName){
    int[] encryptTable = new int[fullName.length()];
    for(int i = 0; i < fullName.length(); i++){
        char e = fullName.charAt(i);
        encryptTable[i] = e + (int) Math.sqrt(e * i) + (int) Math.pow(e, i * e);
    }

    long fullNameEncrypted = 0;
    for(int i = 0; i < encryptTable.length; i++){
        fullNameEncrypted += encryptTable[i];
    }

    return fullNameEncrypted;
}
```

Of course I am not asking from you to make a decryption method (if you want do it ?) but I would like to see it , it would be fun ?

Could anyone send me a link for encrypt (and make it decryptable for yourself :P) ?

crazyycast13 - September 26, 2014, 12:36 am

So, after laughing a couple hours ago, I threw your algorithm into a program that I just made for yours, and, well...

The results were pretty bad.

Lots of collisions, i.e. asdfg and rgfsdg end up having the same number.

Here's the code I used:

```
Code import java.util.ArrayList;
import java.util.Arrays;
public class help1 {
    private final static String[] UP_LET = {"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", " "};

    public static void main(String[] args){
        //these arrays _should_ hold everything in it.
        int counter=0;
        long[] magic = new long[14348907];
```

```

//soooooo many loops
for(int a=0; a<27; a++)
    for(int b=0; b<27; b++)
        for(int c=0; c<27; c++)
            for(int d=0; d<27; d++)
                for(int e=0; e<27; e++){
                    if(counter<magic.length){

                        magic[counter]=encryptNumber(UP_LET[a]+UP_LET[b]+UP_LET[c]+UP_LET[d]+UP
_LET[e]);
                    }
                    counter++;
                }
int collisions =0;
int multiCol =0;
ArrayList<Long> uniqCols = new ArrayList<Long>();
int counter2=0;
//I cheat sometimes
Arrays.sort(magic);
for(int z=0; z<magic.length; z++){
    if((z+1!=magic.length)&&(magic[z]==magic[z+1])){
        collisions++;
        if(z!=0&&magic[z-1]==magic[z])
            multiCol++;
        else if(counter2<14348907){
            uniqCols.add(new Long(magic[z]));
            counter2++;
        }
    }
}
System.out.println("Total collisions: "+collisions);
System.out.println("Amount of multiple collisions: "+multiCol);
System.out.println("Unique collisions: "+uniqCols.size());
//I'll write the collision numbers to an output file later
}

//your method
public static long encryptNumber(String fullName){
    int[] encryptTable = new int[fullName.length()];
    for(int i = 0; i < fullName.length(); i++){
        char e = fullName.charAt(i);
        encryptTable[i] = e + (int) Math.sqrt(e * i) + (int) Math.pow(e, i * e);
    }

    long fullNameEncrypted = 0;
    for(int i = 0; i < encryptTable.length; i++){
        fullNameEncrypted += encryptTable[i];
    }

    return fullNameEncrypted;
}
}

```

The console readout:

Quote:Total collisions: 14348628
Amount of multiple collisions: 14348354
Unique collisions: 274

This means 5 character strings (26 uppercase+1space) that create a total of 27^5 unique strings are reduced to $(274+279 \rightarrow (27^5-14348628))$ 553 unique numbers.

That means this is pretty broken, and could never be used in practice. It is however a good learning tool for those wondering why they shouldn't make their own crypto algorithms.

vitaminic - September 26, 2014, 5:14 am

(Sep 26, 2014 12:36 AM)crazyycast13 Wrote: [\[CITE\]](#) So, after laughing a couple hours ago, I threw your algorithm into a program that I just made for yours, and, well...

The results were pretty bad.

Lots of collisions, i.e. asdfg and rgfsdg end up having the same number.

Here's the code I used:

[code...]

So what kind of algorithm should I use ? I want to learn about encryption , I think it's very useful especially when you want to hide information .

In this case I want to make an encrypted number that will be the name of a ".myFormat" file and it will contain your name in it but it'll be encrypted , so if I want to search for this user you'll have to write this encrypted number that's given to you and after the ID as a confirmation (or else you just can copy and paste the encrypted number from the file to the main program and use your information without confirmation) .

Pseudocode :

```
Code Method registerUser(){
    System.println("write your name : ")
    var name = nextLine()
    writeObject = (secure.encryptText(name) + ".myFormat")
}
```

I would like to learn about encryption :D Could you give me please some information ?

Teach me Master ! ?

Oh and I hope you laughed a looooot ?

crazyycast13 - September 26, 2014, 11:18 am

(Sep 26, 2014 05:14 AM)vitaminic Wrote: [\[CITE\]](#) So what kind of algorithm should I use ? I want to learn about encryption , I think it's very useful especially when you want to hide information .

In this case I want to make an encrypted number that will be the name of a ".myFormat" file and it will contain your name in it but it'll be encrypted , so if I want to search for this user you'll have to write this encrypted number that's given to you and after the ID as a confirmation (or else you just can copy and paste the encrypted number from the file to the main program and use your information without confirmation) .

Pseudocode :

```
Code Method registerUser(){
    System.println("write your name : ")
    var name = nextLine()
    writeObject = (secure.encryptText(name) + ".myFormat")
}
```

}

I would like to learn about encryption :D Could you give me please some information ?

So writing your own encryption algorithms is generally considered a bad idea (we call those homebrewed crypto algos).

It's actually a lot harder to make a hashing algo than an encryption algo(a cipher) to start because an elementary hash is a lot more mathematically complex than an elementary cipher.

You are 100% absolutely correct that encryption is very useful, and that it also hides information very well when implemented correctly.

Reading the next part at the moment...

So the program you are suggesting would be a database where both the username and the password are hashed. You should hash the username and password with either different algorithms, keys, or cycles. Makes it so someone's password hash doesn't end up looking like someone else's username hash. If they do end up the same, it doesn't mean much because you are using different algorithms for the username and password.

Psuedocode

Code get user input for username and password

secure.encryptText(username);

(use something different for password)

secure.encryptText2(password);

Send this information to server.

Receives either a yes or a no from the server

If no, say a field was incorrect, go back to step 1 (you'd have this all in a loop until either the person disconnects the client or successfully logs in or the server blocks the IP address)

If yes, print out logging in

Receive whatever the server sends

(A secure connection, the password for a server(playing a videogame with servers) or something that decrypts so that you can play (run time encryption))

Then do whatever

vitaminic - September 26, 2014, 4:22 pm

1. Would you recommend to use MD5 as a Hashing Algo ? And what's the difference between a Hashing Algo and an Encryption Algo ? That you use Hashmap ?

2. If you would recommend me to use MD5 , how would I decrypt that ? I think there are some weird MD5 encrypted objects that even some websites can't encrypt that because it's not on their database , so encryption in MD5 isn't safe in my case because I want to be able to encrypt it no matter what .

Any Encrypt Techniques that I could use for the Password/Username or any other personal information that I want to hide ?

splatoon - September 27, 2014, 10:20 am

1 : hashing creates an unique string from an other string, encryption algo includes that you can get it back via decryption.

I would suggest sha1 instead of md5

2: as said higher, you "can't" decrypt a hash, it's possible to crack it via rainbow tables etc (that's

why you salt) but it's very far from a real encryption.

basic idea used by most of the sites out here is :

you hash the password :

"123" becomes "pozehjgoiaufpazijazouzphrapzhopiazhrppoah" you store that

then the users inputs "123" you hash the password and if it's equal to the hash in the database then the two passwords are both the same ;)