

Forum:[Hack Forums](#)

Thread: [Simple Message Cryper class \(using monoalphabetic cipher\)](#)

SIM-3364521 - January 17, 2017, 2:05 pm

Hey guys Im new to this Forums and im also kind of new to Java as well
But here is something i wrote real quick that might be useful for some...
(One can clearly tell that the code isn't optimized)

seams like the code is too long so i pasted it on pastebin:
pastebin.com/wAqVSy3v

How to use:

Code //first create a new Cryper Object:
Cryper cryp = new Cryper();

//Crypt() Method expects a String and return a long value:
long crypted = cryp.Crypt("Test");

//DeCrypt expects a long value and prints the decrypted Message to Console:
cryp.DeCrypt(crypted);
As You can see one is only able to crypt a String of the legth < 9.
So it might be helpful to use the String tokenizer / substring method on the Message first

SIM-3364521 - February 7, 2017, 3:17 pm

updated.

Now working differently and uses a password to crypt and decrypt
Instructions and the new source code can be found here:

pastebin.com/vrQHLCiA

clrlslwi - February 7, 2017, 3:47 pm

You've severely offended me with your code.

SIM-3364521 - February 7, 2017, 5:15 pm

(Feb 7, 2017 04:47 PM)Demmonic Wrote: [\[CITE\]](#) You've severely offended me with your code.Feel free to make it better :P

i know that is has some issues with mainly prformance and the 9 char limit and also collecting garbage (strings mainly) but it is working ... good enough for me :P

DarkShadowz - February 7, 2017, 8:31 pm

To deal with characters that are lower or higher case, have the character iterated intentionally lower-cased.

Use a Map to map from character to offset rather than having so many switch cases.

SIM-3364521 - February 8, 2017, 5:26 am

(Feb 7, 2017 09:31 PM)DarkShadowz Wrote: [\[CITE\]](#) To deal with characters that are lower or higher case, have the character iterated intentionally lower-cased.

Use a Map to map from character to offset rather than having so many switch cases.Thanks for the

tip (Y)

You are talking about the java.util.map right ? somehow i never liked using it but it seems like i should get used using it

P.s. btw. how can i like your comment in this forums ? am i blind/dumb or sth. ?

clrlslwi - February 8, 2017, 8:10 am

(Feb 7, 2017 09:31 PM)DarkShadowz Wrote: [\[CITE\]](#) To deal with characters that are lower or higher case, have the character iterated intentionally lower-cased.

Use a Map to map from character to offset rather than having so many switch cases.

A map would still require a lot of code. An alternative would be to generate the offsets randomly, using the password as the seed.

elmomcelroy - February 19, 2017, 12:14 pm

Why do you have message limit 9 chars? Also, substitution ciphers are VERY easy to break, so don't bother using them for any other reason than learning.

FriendOfRaven - February 20, 2017, 9:08 am

Try to make the program capable of deciphering without the password. If you generate all possible solutions, look at letter frequency in the english language. E is the most common letter, in this post up to this point I have used:

9 A
18 E
12 I
14 O
6 U

Try checking only the frequency of the Vowels first and potentially increase later so you can crack more poorly written pieces.

Another suggestion would be to use the ascii values to change the case of the letters, in ascii value a-z appear in the same order in both cases allowing you to change them all with minimal code.

SIM-3364521 - January 7, 2019, 6:35 pm

i dont this was purely for learning purposes.

I know this is a late reply but the string gets converted to a long value to apply the cipher using the password as offset (If i remembre that correctly)

and if the text would be longer than 9 chars it would cause an overflow of long so i capt it to 9 chars.

(although my code works i agree with @clrlslwi that its basicly shit.)

Also this method is only easy to crack with shorter passwords than the message and/or when you reuse the password. If you do that it is basicly as good as no encryption at all.

But if both sides start with the same password that is only used once and it is as long as the message it would effectively be a one time pad.

to exchange more than one message you would have to use and exchange a new password, wich could be done using the first 4 chars of the message or so, than have the same hashing algo on both sides and use the hash of those 4 chars than as new password.

This is ofc. all using pretty out dated methods of crypto and you would still be able to see the length of the original message.

Ofc. there are ways around this as well but just know that the methods i use for this exaple are pretty outdated and are not really used anymore at all.

Although i think the method i described in this comment could make up for a solid base of a practical

cypher i would suggest to have a look at these two principles, which are used in modern cryptography (non symmetric):

1) RSA

basic theory behind it:

part1: [YouTube/4zahvcJ9glg](https://www.youtube.com/watch?v=4zahvcJ9glg)

part2: [YouTube/oOcTVTpUsPQ](https://www.youtube.com/watch?v=oOcTVTpUsPQ)

2) diffie hellman key exchange:

basic theory: [YouTube/NmM9HA2MQGI](https://www.youtube.com/watch?v=NmM9HA2MQGI)

this should give you a starting point on how you could go about creating a modern and secure cypher yourself.

Just note that some people have tried to create a their own cypher or tried to implement a common cypher on their own instead of using code that was already mathematically proven to be secure and most of them where basicly broken in a very short time.

I know this was probably a long comment on a already dead topic but i thought you should know this in case you where searching for a way to create your own cypher like i did in this topic. For learning purposes this is great but if you want more than that you have to be very careful and think about if any step you do might be not secure enough. Before you put your cypher into the field you must have it tested and proven its secure (you can find how to do that on youtube as well)

Again sorry for the long comment and waking up a dead post.

Ensky - January 13, 2019, 2:58 am

Any encryption with a decrypter is not worth using!

SIM-3364521 - January 13, 2019, 7:09 am

you must be thinking of a hash then?

It literally doesnt make any sence to use a crypter you cant decrypt.

If you want something like that use a hash instead.

there are different approaches to create a hash function but a good one is really hard to create. So hard in fact i would almost never code it myself and use current standards like sha-3 instead.