[illegible]

by KOSCI ConAA UDGUUSSKTO 7, 2014

There are three types of cryptography techniques :

1. Secret key Cryptography
2. Public key cryptography
3. Hash Functions

We discussed about the above techniques earlier in the Cryptography basics article.

One simple and basic method to encrypt a message is using Caesar's cipher. It is a very simple form of encryption, where we take letters one by one from the original message and translate it into an encrypted text.

In this article, you'll learn how to create a C program code that will encrypt and decrypt the text using Caesars cipher.

In this example, on a high-level, we will do the following:

- The source text that needs to be encrypted is given in lower case. But if you need to decrypt the text, it should be given in upper case.
- When it is encrypted, each letter will have its ANSII code increased for tree places. When it is decrypted, it will have its code moved toward left.
- The letter 'x' will be translated into 'A', the letter 'y' is transformed into the letter 'B', and the 'z' will change into 'C'.
- We are keeping this logic very simple so that we can understand the code. Once you get the hang of it, come-up with more complex logic to encrypt and decrypt.
- The program will handle only English letters and each input text will not be longer that one sentence. At the end of the input sentence it should have the marker for end '.'.
- If you don't have the sense marker, the longest sentence is 1024 letters long. This is some form of protection, which would prevent the user to input the sentence that would over populate size of the program.
- The numbers in the input will not be changed.
- The blank symbol or any non letter symbol will not be changed.

The following is an example of input text that needs to be encrypted:

```
this is a test message.
```

The following is the output decrypted text for the above input in Caesar's cipher.

COURSE

Linux Sysadmin CentOS 6 Course - Master the Tools, Configure it Right, and be Lazy

EBOOKS

Free Linux 101 Hacks 2nd Edition eBook - Practical Examples to Build a Strong Foundation in Linux

Bash 101 Hacks eBook - Take Control of Your Bash Command Line and Shell Scripting

Sed and Awk 101 Hacks eBook - Enhance Your UNIX / Linux Life with Sed and Awk

Vim 101 Hacks eBook - Practical Examples for Becoming Fast and Productive in Vim Editor

Nagios Core 3 eBook - Monitor Everything, Be Proactive, and Sleep Well

The Geek Stuff

Like

9,535 people like The Geek Stuff.

Facebook social plugin

POPULAR POS

12 Amazing and Essential Linux Books To Enrich Your Brain and Library

```
WLVLVD WHVW PHVVDJH.
```

The decryption is reverse. If you input the encrypted text, you should get decrypted text as the output.

C Source Code Example for Ceaser Cipher

```
#include <stdio.h>
#include <ctype.h>

#define MAXSIZE 1024

void encrypt(char*);
void decrypt(char*);

int menu();

int
main(void)
{

char c,
    choice[2],
    s[MAXSIZE];

 while(1)
 {
 menu();

 gets(choice);

 if((choice[0]=='e')||(choice[0]=='E'))
 {
  puts("Input text to encrypt->");
  gets(s);
  encrypt(s);
 }
 else if((choice[0]=='d')||(choice[0]=='D'))
 {
  puts("Input text to decrypt->");
  gets(s);
  decrypt(s);
 }
 else
    break;
 }

 return 0;
}

void encrypt(char*str)
{
 int n=0;
 char *p=str,
   q[MAXSIZE];

 while(*p)
 {
```

- [50 UNIX / Linux Sysadmin Tutorials]
- [50 Most Frequently Used UNIX / Linux Commands (With Examples)]
- [How To Be Productive and Get Things Done Using GTD]
- [30 Things To Do When you are Bored and have a Computer]
- [Linux Directory Structure (File System Structure) Explained with Examples]
- [Linux Crontab: 15 Awesome Cron Job Examples]
- [Get a Grip on the Grep! – 15 Practical Grep Command Examples]
- [Unix LS Command: 15 Practical Examples]
- [15 Examples To Master Linux Command Line History]
- [Top 10 Open Source Bug Tracking System]
- [Vi and Vim Macro Tutorial: How To Record and Play]
- [Mommy, I found it! – 15 Practical Linux Find Command Examples]
- [15 Awesome Gmail Tips and Tricks]
- [15 Awesome Google Search Tips and Tricks]
- [RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams]
- [Can You Top This? 15 Practical Linux Top Command Examples]
- [Top 5 Best System Monitoring Tools]
- [Top 5 Best Linux OS Distributions]
- [How To Monitor Remote Linux Host using Nagios 3.0]
- [Awk Introduction Tutorial – 7 Awk Print Examples]
- [How to Backup Linux? 15 rsync Command Examples]
- [The Ultimate Wget Download Guide With 15 Awesome Examples]
- [Top 5 Best Linux Text Editors]
- [Packet Analyzer: 15 TCPDUMP Command Examples]
- [The Ultimate Bash Array Tutorial with 15 Examples]
- [3 Steps to Perform SSH Login Without Password Using ssh-keygen & ssh-copy-id]
- [Unix Sed Tutorial: Advanced Sed Substitution Examples]
- [UNIX / Linux: 10 Netstat Command Examples]
- [The Ultimate Guide for Creating Strong Passwords]
- [6 Steps to Secure Your Home Wireless Network]
- [Turbocharge PuTTY with 12 Powerful Add-Ons]

CATEGORIES

- Linux Tutorials
- Vim Editor
- Sed Scripting
- Awk Scripting
- Bash Shell Scripting
- Nagios Monitoring
- OpenSSH
- IPTables Firewall
- Apache Web Server
- MySQL Database
- Perl Programming

```
   if(islower(*p))
   {
    if((*p>='a')&&(*p<'x'))
     q[n]=toupper(*p + (char)3);
    else if(*p=='x')
     q[n]='A';
    else if(*p=='y')
     q[n]='B';
    else
     q[n]='C';
   }
   else
   {
    q[n]=*p;
   }
   n++; p++;
  }
  q[n++]='\0';
  puts(q);
 }

 void decrypt(char*str)
 {
  int  n=0;
  char *p=str,
    q[MAXSIZE];

  while(*p)
  {
   if(isupper(*p))
   {
    if((*p>='D')&&(*p<='Z'))
     q[n]=tolower(*p - (char)3);
    else if(*p=='A')
     q[n]='x';
    else if(*p=='B')
     q[n]='y';
    else
     q[n]='z';
   }
   else
   {
    q[n]=*p;
   }
   n++; p++;
  }
  q[n++]='\0';
  puts(q);
 }

 int menu()
 {
  puts("To encrypt, input e or E\n");
  puts("To decrypt, input d or D\n");
  puts("To exit, input any other letter\n");
  puts("Your choice:->\n");
  return 0;
 }
```

Code Analysis

The main function does the following:

- First we include the stdio.h and ctype.h
- Then we create a macro for maximum sentence size. In this example, it is 1024.
- There are a few declarations to reserve place for things that we use in our code.
- While loop will repeat until user inputs proper letter to stop the program.
- In the while loop, we call the function menu(), which will display the menu to the user.

Next, it does the following:

- When you input the letter, function gets() reads your choice. According to the user input

Google Tutorials

Ubuntu Tutorials

PostgreSQL DB

Hello World Examples

C Programming

C++ Programming

DELL Server Tutorials

Oracle Database

VMware Tutorials

Ramesh Natarajan

Follow

appropriate function would be called.

- One function encrypts the text, and the other function decrypts it.
- First function gets one string into it, and modifies it. After that, we are changing each letter according to the rule we need to apply.
- The pointer q is a helper to read the original string, and the q is used to store the output.
- tolower() will transform the letter into lower case. toupper() will transform the letter into upper case.
- Function gets() is used to read the input string from user.

Now, to the function encrypt:

- To encrypt, this code will move letters to a different offset by 3 spaces in ASCII table. Also, at the end of alphabet you wrap around and replace: x, y and z, with: a, b and c.
- Instead of char type, use wcahr_t symbols that could be good for languages other than English. There are usually similar functions that will work with two byte letters. Sometimes it is enough to use one additional w.

As an additional exercise, modify the above C sample code to include different offsets in one sentence itself.

When we talk about breaking Caesars cipher, first algorithm that could be applied is statistical decryption. For each language, there are usual frequencies of each letter and they could be used to figure out the encrypted text without getting the key. On a related subject, you should also explore how Vigener’s cipher works.

Again, it is very easy to break the encrypted text generated by this example. The above code is given only for learning purpose to understand how this works.

g+1 15 Tweet Like 13 > Add your comment

If you enjoyed this article, you might also like..

1. 50 Linux Sysadmin Tutorials
2. 50 Most Frequently Used Linux Commands (With Examples)
3. Top 25 Best Linux Performance Monitoring and Debugging Tools
4. Mommy, I found it! – 15 Practical Linux Find Command Examples
5. Linux 101 Hacks 2nd Edition eBook Free

- Awk Introduction – 7 Awk Print Examples
- Advanced Sed Substitution Examples
- 8 Essential Vim Editor Navigation Fundamentals
- 25 Most Frequently Used Linux IPTables Rules Examples
- Turbocharge PuTTY with 12 Powerful Add-Ons

Tags: Caesar Cipher C Language

{ 6 comments… read them below or add one }

mandrew December 8, 2014 at 6:47 pm 1

This is a really nice post and really helpful.
I have a question though. From the example above you had a fixed shift of 3, but what if this number was much bigger? How would you write the code if you wanted to shift by 20 for example?

duskoKoscica December 19, 2014 at 5:35 am 2

In order to work on programmers tenacity, I would like to add few infos.
1. All permutations of the set would not outperform the Caeser cypher you would be able to consider this.
If you are trying to think of permutation as f, then your task would be to look for f^-1, which would be equivalent of decription. Instead of that, you could perform f^2, f^3, f^4,… f^n, which would lead you to identical transformation.

2. Oh yes, you could be naive and think that f*g would lead you to more secure encription, but it is just matter of finding f*g=h, and now You could apply first step, and not worry about it, if you are Eva.

3. So, what is beyond asimetric and quantum encription!

duskoKoscica January 17, 2015 at 4:50 am 3

@mandrev

Nice, but you have missed the point, there is place for some other things.

In professional application, which should be obvious from comment, I would not even care for that…
There is statistical and some other attacks … that would penetrate this simple encryption…

Well, if yo rally like to hear answer, I am without idea for something like that….

hihhiiihiihihhhihihih!!!!!

I hope you have some nice ideas to help me with this problem….

duskoKoscica January 17, 2015 at 5:49 am 4

Before I start, about my ideas I would like to listen to Lura.

It is cool,

perhaps this one> Fitiço di funana

I am kind a stressed now!

duskoKoscica January 19, 2015 at 5:59 am 5

Ok!

Fine, today I fell like to relaxed I need, for example>
apocaliptica

or some music like that.

Why do you need that addition any way?!?

duskoKoscica January 20, 2015 at 2:03 am 6

Ok, even I have not used all excuses, and the subject of this article is a ceaser cypher, I will provide few answers.
This problem is very serious, and it could be done in many ways, one of them would be to create some form of a table that could be implemented in form of matrix but that is not all of it, oh no, not at all.
The second idea is to create one function that would produce shift for one place to left and if you go over the ‘z’ you return back to ‘a’.
For some of us, it would be an introduction into topic of round buffer.
But there is one more general way, that would serve as example how to generate more general algorithm that could be applied in more situations.
Lets have cShift taken into our function, then you would use something like this cShift%=26; that will be used to shift our situation and loose some of periods that are not important in this disc.
So, one of the important lines would be>

```
if(islower(ch))
if(ch + iShift &lt=’z’)
ch+=iShift;
else
ch=(‘z’- 26 + iShift) + ‘a’;
```

THX for participating in our disc.

Leave a Comment

Name

E-mail

Website

□ Notify me of followup comments via e-mail

Submit

PREVIOUS POST 10 insserv Command Examples for Linux System Init Scripts

NEXT POST Intro to Android MonkeyRunner MonkeyDevice and MonkeyImage Functions

About The Geek Stuff

My name is **Ramesh Natarajan**. I will be posting instruction guides, how-to, troubleshooting tips and tricks on Linux, database, hardware, security and web. My focus is to write articles that will either teach you or help you resolve a problem. Read more about Ramesh Natarajan and the blog.

Contact Us

Email Me : Use this Contact Form to get in touch me with your comments, questions or suggestions about this site. You can also simply drop me a line to say hello!.

Follow us on Google+

Follow us on Twitter

Become a fan on Facebook

Support Us

Support this blog by purchasing one of my ebooks.

Bash 101 Hacks eBook

Sed and Awk 101 Hacks eBook

Vim 101 Hacks eBook

Nagios Core 3 eBook