

Forum:[Hack Forums](#)

Thread: [Classical Encryption Tutorial](#)

baymandernam - December 2, 2012, 12:25 pm

Hey all! Welcome to my Classical Encryption Tutorial!

There are many different types of classical encryptions, some of which include:

Beale cipher

Transposition ciphers

ceasar cipher

atbash cipher

playfair cipher

polyalphabetic substitution

Columnar transposition

In this tutorial we will be focusing on the Columnar transposition, and the polyalphabetic substitution cipher. Lets get started

The Polyalphabetic cipher

This cipher is a simple substitution cipher which an alphabet that changes.

For example:

Original text: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher Alphabet 1:BCDEFGHIJKLMNOPQRSTUVWXYZA

Cipher Alphabet 2:DEFGHIJKLMNOPQRSTUVWXYZABC

as you can see, this cipher just increments the letters by a certain amount. Cipher 1 is incremented by 1 and cipher 2 is incremented by 3. Thus, "Hello World" In cipher 1 would be: IFMMP XPSME

To decode one of these ciphers one must know the amount each letter is incremented by, For example if I just gave you: HNUMJW decrypting it would take a long time. However, if i told you that each letter was Incremented by +5 (goes forward A-Z 5 for each letter) then you would be able to tell me that HNUMJW translated to CIPHER.

In addition, Text can be encrypted more than once. For example, If I used +5,-3,+4 on the word "DEATH" It would translate to: JKGYM

This is so because:

DEATH + 5 = IJFYM

IJFYM - 3 = FGCVJ

FGCVJ + 4 = JKGYM

Challenge(answers at bottom of thread):

Translate This: URYYB JBEYQ the cipher is 14.

Translate This: SVCM

Columnar transposition cipher

The Columnar transposition cipher is a cipher that consists of writing the original text as a column and then separating each column:

For Example:

Original text: HELLO FRIEND

HELL
OFRI
END

HOE EFN LRD LI = HELLO FRIEND

This cipher is very strong when used with others such as the polyalphabetic cipher.

To decrypt one of these ciphers you need to put each line of text into a column:

HOE

H
O
E

EFN

E
F
N

LRD

L
R
D

LI

L
I

Final:

HELL
OFRI
END

HELLOFRIEND = HELLO FRIEND

Challenge(answers at bottom of thread):

Translate This: GNT OI OG DH

Translate This: IE LY OO VU

CONCLUSIONS

When used together ciphers can be a very powerful way of protecting data. For Example:

If I write "KILL THEM ALL" with the cipher of +4,columnar, + 2 I will get: QZG ONR RKR RS

In addition, If I encoded any word and didnt tell you what the cipher was, you would have a really tough time decoding it.

Challenges(answers at bottom of thread):

Translate This: SHW ZOC WW PZ encoded with: +14, columnar, -2, columnar

Translate This: KGJ JO CC VV encoded with +2,columnar

I hope you liked this tutorial, keep an eye out for new program releases and tutorials by me!
Thanks!

CHALLENGE ANSWERS:

POLYALPHABETIC CIPHER:

CHALLENGE 1: HELLO WORLD

CHALLENGE 2: LOVE

COLUMNAL CIPHER:

CHALLENGE 1: GOOD NIGHT

CHALLENGE 2: I LOVE YOU

CUMULATIVE CHALLENGE:

CHALLENGE 1: HELLO WORLD

CHALLENGE 2: I HATE MATH