Encryption and Cracking the Code

•••

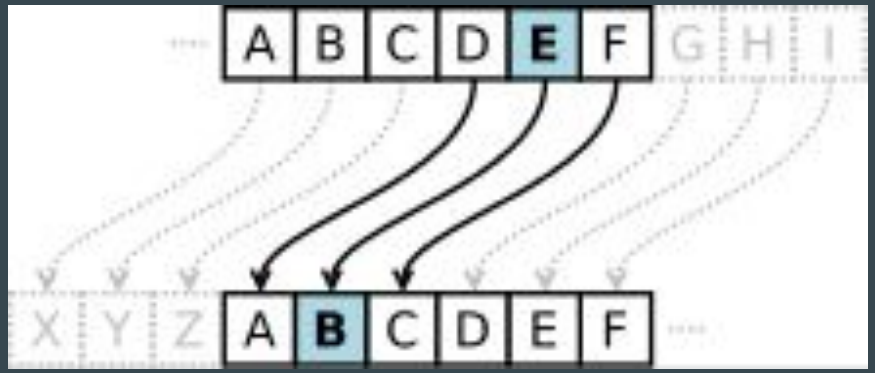
Jonathan Benishay and Sam Rasmussen

What is Encryption?

- Process of encoding information into a secret code
- Used often for messaging
- Original information known as plaintext
- New information known as ciphertext
- Should a third party obtain information, they will be unable to understand it

Caesar Cipher

- One of most widely known encryption techniques
- Easy encryption method to learn
- Shifts placement of alphabet by a specified number
- Named after Julius Caesar
- Used by Romans with shift of three to send military messages



Encoding with the Caesar Cipher

Phrase	Ciphertext
A	Z
C	B
O	N
W	V
J	I
U	T
M	L
P	O
E	D
D	C
O	N
V	U
E	D
R	Q
T	S
H	G
E	D
M	L
O	N
O	N
N	M

Letter	Code
A	Z
B	A
C	B
D	C
E	D
F	E
G	F
H	G
I	H
J	I
K	J
L	K
M	L
N	M
O	N
P	O
Q	P
R	Q
S	R
T	S
U	T
V	U
W	V

Shift
25

Brute Force Attack on Caesar Cipher

	A	C
1	Cipher Text (enter in lowercase and as one word if it is a phrase):	Deciphered Text:
2	trvjritzgyvijrivhlzkvvrjpkftirtb	squiqhsyfxuhiqhugkyjuuqiojeshqsa
3		rpthpgrxewtghpgtfjxittphnidrgprz
4		qosgofqwdvsfgofseiwhssogmhcqfoqy
5		pnrfnepvcurefnerdhvgrrnflgbpenpx
6		omqemdoubtqdemdqcgufqqmekfaodmow
7		nlpdlcntaspcdlcpbfteppldjeznclnv
8		mkockbmszrobckboaesdookcidymbkmu
9		ljnbjalryqnabjanzdrcnnjbhcxlajlt
10		kimaizkqxpmzaizmycqbmmiagbwkziks
11		jhlzhyjpwolyzhylxbpallhzfavjyhjr
12		igkygxiovnkxygxkwaozkkgyezuixgiq
13		hfjxfwhnumjwxfwjvznyjjfxdythwfhp
14		geiwevgmtlivweviuymxiiewcxsgvego
15		fdhvduflskhuvduhtxlwhhdvbwrfudfn
16		ecguctekrjgtuctgswkvggcuavqetcem
17		dbftbsdjqifstbsfrvjuffbtzupdsbdl
18		caesarciphersarequiteeasytocrack
19		bzdrzqbhogdqrzqdpthsddzrxsnbqzbj
20		aycqypagnfcpqypcosgrccyqwrmapyai
21		zxbpxozfmebopxobnrfqbbxpvqlzoxzh
22		ywaownyeldanownamqepaawoupkynwyg
23		xvznvmxdkczmnvmzlpdozzvntojxmvxf
24		wuymulwcjbylmulykocnyyumsniwluwe
25		vtxltkvbiaxkltkxjnbmxxtlrmhvktvd
26		uswksjuahzwjksjwimalwwskqlgujsuc
27		trvjritzgyvijrivhlzkvvrjpkftirtb
28		

Code

Click to run the Brute-Force Attack

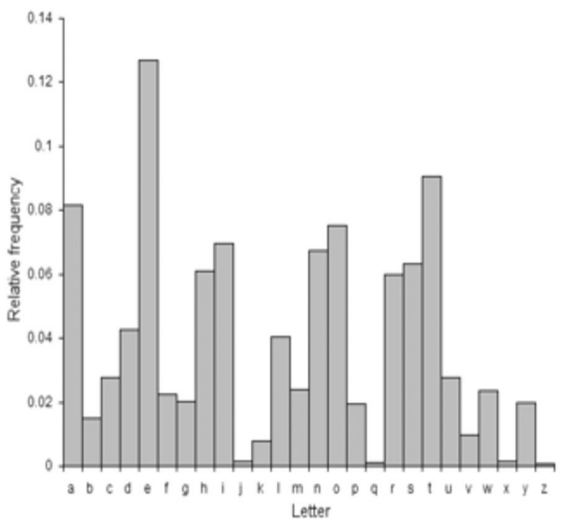
CeaserCipherBruteForceAttack.xls - Module1 (Code)

(General) | Run

```
Dim Counter As Integer
Sub Run()
'dim=declaring variables(giving them a name)
'As ___ = type of variable (string is letters, integers are represented by numbers)
'shift variable= every shift from 1-26
'alphabet variable= defining every letter which will correlate with the amount of times each letter shifts
Dim shift As Integer
Dim alphabet As String
Dim alphabetposition As Integer
Dim count As Integer
shift = 1 'where the program locates the enciphered code
alphabet = "abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz"
cipher = Cells(2, 1).Value 'the cipher text that was entered in that we want to decrypt
Do While shift <= 26 'repeats until the amount of shifts is less than or equal to 26
For count = 1 To Len(cipher) '1 to Len means the amountof characters in the cipher text
alphabetposition = InStr(alphabet, Mid(cipher, count, 1)) 'Mid=(string, where it starts, the length of string) in this case we want to go
decipherednum = alphabetposition + 26 - shift Mod 26 'mathematical decryption algorithm...m=c+26-k (mod 26)
DeCiphered = Mid(alphabet, decipherednum, 1) 'this is what each letter will be decrypted and shown
DeCipheredText = DeCipheredText & DeCiphered "brings both string expressions together(like addition for strings)
Next 'indicates that it will be repeated a.k.a For...Next loop
Cells(shift + 1, 3).Value = DeCipheredText 'where the brute-force attack attempts will be located on excel
shift = shift + 1 'this will shift all the characters and eventually show the correct deciphered text
DeCipheredText = ""
Loop
End Sub
```

Letter Frequency Analysis

Enter English Cipher Text:	Letter:	How many occurences of each letter:
Aol Jhlzhy jpwoly pz vul vm aol Ihysplza ruvdu huk zptwslza jpwolyz.	a	3
	b	0
	c	0
	d	1
	e	0
	f	0
	g	0
	h	4
	i	0
	j	2
	k	1
	l	9
	m	1
	n	0
	o	4
	p	5
	q	0
	r	1
	s	2
	t	1
	u	4
	v	3
	w	3
	x	0
	y	4
	z	6




```
=LEN(A2)-LEN(SUBSTITUTE(A2,"l",""))
```

Frequency Analysis in Different Languages

29	Enter Spanish Cipher Text:	Letter:	How many occurences of each letter:
30	aescsobkbocobfkbexkwockzkbkmsxmy	a	1
31		b	6
32		c	5
33		d	0
34		e	2
35		f	1
36		g	0
37		h	0
38		l	0
39		m	2
40		n	0
41		ñ	0
42		o	5
43		p	0
44		q	0
45		r	0
46		s	3
47		t	0
48		u	0
49		v	0
50		w	1
51		x	3
52		y	2
53		z	2

UK English Language Letter Frequency:

e t a o i n s r h l d c u m f p g w y b v k x j q z

Spanish Language Letter Frequency:

e a o s r n i d l c t u m p b g y í v q ó h f z j é á ñ x ú ü w k

German Language Letter Frequency:

e n i s r a t d h u l c g m o b w f k z v ü p ä ß j ö y q x

French Language Letter Frequency:

e s a i t n r u l o d c m p é v q f b g h j à x è y ê z ç ô ù â û î œ w k ï ë ü æ ñ

Italian Language Letter Frequency:

e a i o n l r t s c d u p m v g h f b q z ò à ù ì é è ó y k w x j ô

Dutch Language Letter Frequency:

e n a t i r o d s l g h v k m u b p w j c z f x y (ë é ó) q

Greek Language Letter Frequency:

α ο ι ε τ σ ν η υ ρ π κ μ λ ω δ γ χ θ φ β ξ ζ ψ

Russian Language Letter Frequency:

о е а и н т с в л р к д м п у ё я г б з ч й х ж ш ю ц щ е ф (ъ ы ь)

Encryption Today

- Gives us the ability to communicate through secure channels
- Protects and secures our data and personal information
  - E.g Public-Key Cryptography and Diffie-Hellman Key
- Investment in encryption for businesses can prevent attacks and unwanted costs
- Innovations in the computing world creates new security risks

Q & A