Puzzles

PreComputer

Shift (Caesar's) Cipher Puzzle

Shift Cipher used in TV era; search for Video

"Captain Midnight Decoder Ring" on YouTube

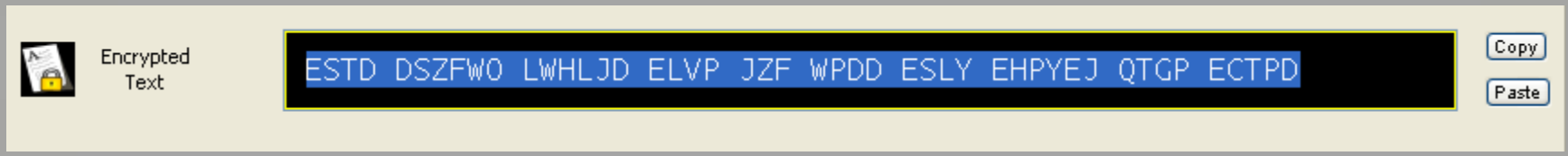
Shift Cipher Puzzle

DeCrypt This

ESTD DSZFWO LWHLJD ELVP JZF WPDD ESLY EHPYEJ QTGP ECTPD

How

1. Copy “ESTD DSZFWO LWH…” from above into ‘Encrypted Text’



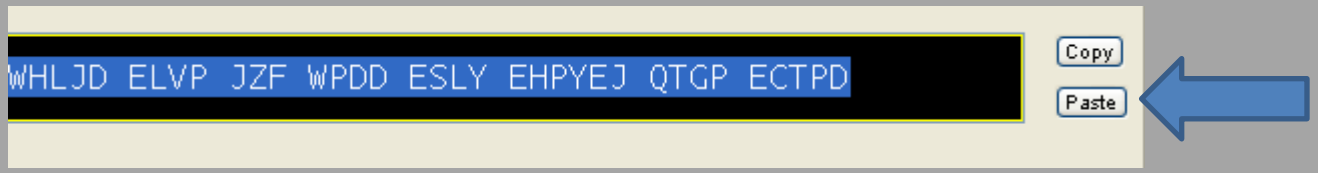
2. Hit ‘Decrypt’. If decrypted message makes words➔ done;
3. else hit ‘Shift Encrypted Letter’ & try ‘Decrypt’ again, etc.

Shift Cipher Puzzle

Short Cut

1. Copy text to clipboard
   (highlight and hit ‘Control+C’)

2. Hit ‘Paste’ button in program



ESTD DSZFWO LWHLJD ELVP JZF WPDD ESLY EHPYEJ QTGP ECTPD

Shuffle Cipher Puzzle

DeCrypt This

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

Shuffle Cipher Puzzle

DeCrypt This

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

How

Programs (like those below) help count letter frequencies.

Letter frequency counters:

characterfrequencyanalyzer.com/english/

csgnetwork.com/documentanalystcalc.html

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

Frequencies of encrypted letters

Shuffle Puzzle

Frequency Analysis

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

E ?

T ?

English letters used most* (decreasing order)

E used most; then T, A, O, I, N, S, H, R

So assuming this particular encryption matches letter frequencies . . .

Assume

L is encrypted E

R is encrypted T

And do the following →

* Analysis may vary

Shuffle Puzzle

Substitute ‘E’ for ‘L’

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

-EE- -E --E-E ---E- E-E-E- -E- -- -- ---- ---------

Shuffle Puzzle

Substitute ‘T’ for ‘R’

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

E , T, A, O, I, N, S, H, R

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

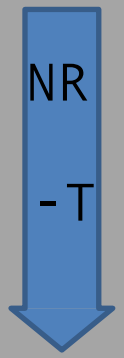
-EET -E T-E-E --TE- E-E-E- TE- -- -T ---- -----T--T

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

-EET -E T-E-E --TE- E-E-E- TE- -- -T ---- -----T--T



What could ‘N’ be ?

‘N’ - Must be a vowel: ‘A’, ‘E’, ‘I’, ‘O’ or ‘U’
because –T must be a word

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

-EET -E T-E-E A-TE- E-E-E- TE- -- AT ---- -----TA-T

What could ‘N’ be ?

‘N’ - Must be a vowel: ‘A’, ‘E’, ‘I’, ‘O’ or ‘U’
because –T must be a word

➔ Try ‘A’ (more frequent than ‘I’)

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

-EET -E T-E-E A-TE- E-E-E- TE- -- AT ---- -----TA-T

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

Most used:
~~(E , T, A~~, O, I, N, S, H, R)

What could ‘M’ be ?

D, **N**, O, X, Y, Z

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

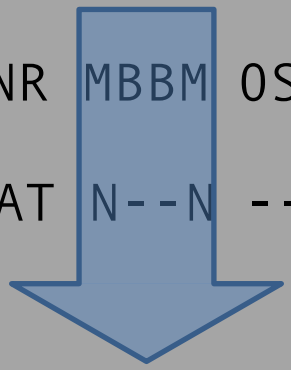
-EET -E T-E-E A-TE- E-E-EN TEN -- AT N--N -----TANT

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

-EET -E T-E-E A-TE- E-E-EN TEN -- AT N--N -----TANT



What could ‘BB’ be ?

Most used:
~~(E , T, A~~, O, I, ~~N,~~ S, H, R)

Must be a vowel: ~~‘A’, ‘E’,~~ ‘I’, ‘O’ or ‘U’

➔ ‘O’ by elimination

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

-EET -E T-E-E A-TE- E-E-EN TEN O- AT NOON ---O-TANT

Candidates ? : B, H, M

Shuffle Puzzle

Other Clues . . .

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

MEET ME T-E-E A-TE- E-E-EN TEN O- AT NOON -M-O-TANT

M seems likely

Shuffle Puzzle

What's Left ?

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

MEET ME T-E-E A-TE- E-E-EN TEN O- AT NOON -M-O-TANT

Used: A E M N O T

Most used:
~~(E , T, A, O~~, I, ~~N~~, S, H, R)

Left: B C D F G H I J K L P Q R S U V W X Y Z

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

Shuffle Puzzle

What's Left ?

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

MEET ME T-E-E A-TE- E-E-EN TEN O- AT NOON -M-O-TANT

Most used:
~~(E , T, A, O~~, I, ~~N~~, S, H, R)

Try: G = I S H or R

Must be: R

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

Shuffle Puzzle

What's Left ?

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

MEET ME T-ERE A-TER E-E-EN TEN OR AT NOON -M-ORTANT

Used: A E M N O T R

Most used:
~~(E , T, A, O~~, I, ~~N~~, S, H, ~~R~~)

Left: B C D F G H I J K L P Q S U V W X Y Z

Try: I S H

A	1
B	4
D	1
G	4
L	10
M	5
N	3
O	1
R	7
S	3
T	1
X	1
Y	1

Shuffle Puzzle

What's Left ?

SLLR SL RALGL NYRLG LXLTLM RLM BG NR MBBM OSDBGRNMR

MEET ME THERE A-TER E-E-EN TEN OR AT NOON IM-ORTANT

Shuffle Cipher Puzzle - 2

Here's an encrypted quote from the famous cryptologist, Bruce Schneier.*

MHOJO AJO MVC MYFOK CR OGSJYFMUCG CGO MHAM VUEE FJOTOGM YCQJ KUKMOJ RJCN JOAWUGD YCQJ WUAJY AGW CGO MHAM VUEE FJOTOGM YCQJ DCTOJGNOGM

See next slide for what you know about the above encrypted text.

* Many *Cryptography Decrypted* fundamental crypto concepts s are covered in the beginning of his disruptive book *Applied Cryptography*.

Shuffle Cipher Puzzle - 2

Decrypt This

```
MHOJO AJO MVC MYFOK CR OGSJYFMUCG CGO MHAM VUEE FJOTOGM YCQJ
_____ ___ ___ _____ __ __________ ___ ____ ____ _______ ____

KUKMOJ RJCN JOAWUGD YCQJ WUAJY AGW CGO MHAM VUEE FJOTOGM
______ ____ _______ ____ _____ ___ ___ ____ ____ _______

YCQJ DCTOJGNOGM
____ __________
```

First thing: Compute Letter frequency Counts of encrypted text . . .

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
_____ ___ ___ _____ __

OGSJYFMUCG CGO MHAM VUEE
__________ ___ ____ ____

FJOTOGM YCQJ
_______ ____

KUKMOJ RJCN JOAWUGD YCQJ
______ ____ _______ ____

WUAJY AGW CGO MHAM VUEE
_____ ___ ___ ____ ____

FJOTOGM YCQJ DCTOJGNOGM
_______ ____ __________
```

Letter frequency Counts

15 O	3 Q
13 J	3 T
12 M	3 H
10 G	3 V
10 C	3 W
6 A	3 K
6 U	2 R
6 Y	2 D
4 E	2 N
4 F	1 S

Letter Frequency Language **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**

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

letterfrequency.org/

Substitute ‘E’ for each ‘O’ . . .

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
__E_E __E ___ ___E_ __

OGSJYFMUCG CGO MHAM VUEE
E__________ __E ____ ____

FJOTOGM YCQJ
__E_E__ ____

KUKMOJ RJCN JOAWUGD YCQJ
____E_ ____ _E_____ ____

WUAJY AGW CGO MHAM VUEE
_____ ___ __E ____ ____

FJOTOGM YCQJ DCTOJGNOGM
__E_E__ ____ ___E___E__
```

Letter frequency Counts

15 O	3 Q
13 J	3 T
12 M	3 H
10 G	3 V
10 C	3 W
6 A	3 K
6 U	2 R
6 Y	2 D
4 E	2 N
4 F	1 S

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
__E_E __E ___ ___E_ __

OGSJYFMUCG CGO MHAM VUEE
E__________ __E ____ ____

FJOTOGM YCQJ
__E_E__ ____

KUKMOJ RJCN JOAWUGD YCQJ
____E_ ____ _E_____ ____

WUAJY AGW CGO MHAM VUEE
_____ ___ __E ____ ____

FJOTOGM YCQJ DCTOJGNOGM
__E_E__ ____ ___E___E__
```

Letter frequency Counts

15 O ⇢ E

13 J ⇢ ? T A R

12 M ⇢ ? T A R

• • •

English word most often 3 letters *

the and for are but not…

⇢ substitue ‘R’ fits best for ‘J’

⇢ then ‘T’ for ‘M’

* letterfrequency.org the and for are but not you all any can had her was …

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
T_ERE _RE T__ TY_E_ __

OGSJYFMUCG CGO MHAM VUEE
E__RY_T___ __E T___ ____

FJOTOGM YCQJ
_RE_E_T YOUR

KUKMOJ RJCN JOAWUGD YCQJ
___TER ____ RE_____ Y__R

WUAJY AGW CGO MHAM VUEE
___R_ ___ __E T___ ____

FJOTOGM YCQJ DCTOJGNOGM
_RE_E_T YOUR ___ER__E_T
```

We know that

1. Shuffle passwords mostly don't use Y or Z. * Y is Y and Z is Z

2. Most common 4 letter word beginning with 'Y' is YOUR

   so C → O Q → U

* See in program lessons & Encryption Basics II video

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
T_ERE _RE T_O TY_E_ O_

OGSJYFMUCG CGO MHAM VUEE
E__RY_T_O_ O_E T__T ____

FJOTOGM YCQJ
_RE_E_T YOUR

KUKMOJ RJCN JOAWUGD YCQJ
___TER _RO_ RE_____ YOUR

WUAJY AGW CGO MHAM VUEE
___R_ ___ O_E T__T ____

FJOTOGM YCQJ DCTOJGNOGM
_RE_E_T YOUR ___ER__E_T
```

C → O Q → U

Then 'H' guess H and 'A' guess A
(repeated letters should & do happen!)

'G' guess N

* See in program lessons & Encryption Basics II video

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
THERE ARE TWO TY_E_ O_

OGSJYFMUCG CGO MHAM VUEE
EN_RY_T_ON ONE THAT ____

FJOTOGM YCQJ
_RE_ENT YOUR

KUKMOJ RJCN JOAWUGD YCQJ
_I_TER _RO_ REA_IN_ YOUR

WUAJY AGW CGO MHAM VUEE
_IARY AN_ ONE THAT ____

FJOTOGM YCQJ DCTOJGNOGM
_RE_ENT YOUR ___ERN_ENT
```

English word most often 4 letters *

with have this will your from they know want. . .

Since already found T, A, Y, N, Y
Decrypted VUEE can't contain any of those letters. WILL fits nicely.

Apply same reason to encrypted RJCN ; that is 'FROM' fits

* other sources: scottbryce.com/cryptograms/stats.htm,
en.wikipedia.org/wiki/Most_common_words_in_English

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
THERE ARE TWO TY_E_ OF

OGSJYFMUCG CGO MHAM VUEE
EN_RY_TION ONE THAT WILL

FJOTOGM YCQJ
_RE_ENT YOUR

KUKMOJ RJCN JOAWUGD YCQJ
_I_TER FROM REA_IN_ YOUR

WUAJY AGW CGO MHAM VUEE
_IARY AN_ ONE THAT WILL

FJOTOGM YCQJ DCTOJGNOGM
_RE_ENT YOUR ___ERN_ENT
```

for ’F’ try ‘P’

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

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
THERE ARE TWO TY_E_ OF

OGSJYFMUCG CGO MHAM VUEE
EN_RY_TION ONE THAT WILL

FJOTOGM YCQJ
_RE_ENT YOUR

KUKMOJ RJCN JOAWUGD YCQJ
_I_TER FROM REA_IN_ YOUR

WUAJY AGW CGO MHAM VUEE
_IARY AN_ ONE THAT WILL

FJOTOGM YCQJ DCTOJGNOGM
_RE_E_T YOUR ___ERN_ENT
```

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

KU**K**MOJ
_I_TER

K repeats try ‘B’, ‘D’, . . . ‘S’ fits best

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
THERE ARE TWO TY_ES OF

OGSJYFMUCG CGO MHAM VUEE
EN_RY_TION ONE THAT WILL

FJOTOGM YCQJ
_RE_ENT YOUR

KUKMOJ RJCN JOAWUGD YCQJ
SISTER FROM READING YOUR

WUAJY AGW CGO MHAM VUEE
DIARY AN_ ONE THAT WILL

FJOTOGM YCQJ DCTOJGNOGM
_RE_E_T YOUR G__ERN_ENT
```

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

W fits with ‘D’IARY and then in REA’D’ING

Shuffle Cipher Puzzle - 2

```
MHOJO AJO MVC MYFOK CR
THERE ARE TWO TYPES OF

OGSJYFMUCG CGO MHAM VUEE
EN_RYPTION ONE THAT WILL

FJOTOGM YCQJ
PRE_ENT YOUR

KUKMOJ RJCN JOAWUGD YCQJ
SISTER FROM READING YOUR

WUAJY AGW CGO MHAM VUEE
DIARY AND ONE THAT WILL

FJOTOGM YCQJ DCTOJGNOGM
PRE_ENT YOUR G__ERN_ENT
```

Guess

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

Shuffle Cipher Puzzle - 2

THERE ARE TWO TYPES OF

ENCRYPTION. ONE THAT WILL

PREVENT YOUR

SISTER FROM READING YOUR

DIARY AND ONE THAT WILL

PREVENT YOUR GOVERNMENT

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

Shuffle Cipher Puzzle - 2

A ‘Crib’ is a kind of ‘Known-plaintext attack’*. It can make cryptanalysis much faster.

Like a cryptologist quote, might contain ENCRYPTION.

```
MHOJO AJO MVC MYFOK CR
T_ERE _RE T_O T__E_ OF

OGSJYFMUCG CGO MHAM VUEE
ENCRYPTION ONE T__T _I__

FJOTOGM YCQJ
_RE_ENT YO_R

KUKMOJ RJCN JOAWUGD YCQJ
___TER FRO_ R____NG YO_R

WUAJY AGW CGO MHAM VUEE
___RY _N_ ONE T__T _I__

FJOTOGM YCQJ DCTOJGNOGM
_RE_ENT YO_R GO_ERN_ENT
```

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

* https://en.wikipedia.org/wiki/Known-plaintext_attack

Of Note:

The methods used to decrypt the previous **only** work w/ encryption methods that use 1 encrypted letter for each clear letter.
ie. **Every** 'E' is alwaysrepresented by **same** encrypted letter.

Multi-Shift Cipher (Vigenere) does not do this.
Vigenere cryptanalysis is beyond the scope of this course; for more info:
www.cs.virginia.edu/~cmt5n/Classwork/Crypt/Shaun/vigenerecrypt.html

Other ways to cryptanalyze this message...
Search for Mark Twain quotes that have 'school board'
Or notice that the same encrypted alphabetwas used in Puzzle 2 and 3.

MultiShift (Vigenere) Cryptanalysis

Wiki

http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

Practical Crypt

http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher/

North Kentucky University

http://www.nku.edu/~christensen/section%2012%20vigenere%20cryptanalysis.pdf

Shuffle Cipher Puzzle - 3

Decrypt This

BFRWB HRUHCR BER SWJR XWQ QUV XWIB BERJ BU BFRWB QUV

Spies tell you:

‘B’ is ‘T’ (not ‘E’)
‘Q’ is ‘Y’

Your observation shows duplicate words:

BFRWB and **QUV**

8	B
7	R
5	W
4	U
3	Q
2	E
2	F
2	H
2	V
2	J
2	X

Shuffle Cipher Puzzle – 3 Answer

After substitution of letters:

BFRWB HRUHCR BER SWJR XWQ QUV XWIB BERJ BU BFRWB QUV

treat -eo--e the -ame way yo- wa-t them to treat yo-

‘H’ appears twice

Remaining:

b, c, d, f, g, i, j, k, l, n, p, q, s, u, x, z

Used:

a, e, h, m, o, r, t, w, y