Simple Cipher Messages ~ 1

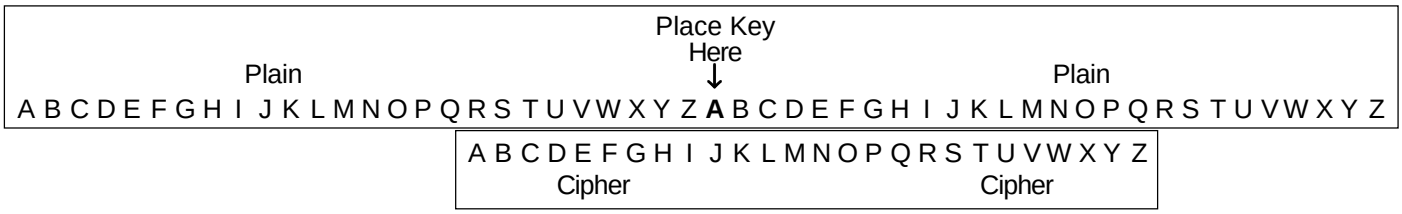
Ciphers are used to make the contents of a message secret, so that it cannot be read by anyone who for whom it is not intended. There many ways of doing this, varying from the extremely simple to the very complicated. Indeed, modern methods of ciphering are so complex that putting the original message into cipher format for the sender, and the work of recovering it by the receiver, are jobs that can only be done by a computer.

Here we will look at the simplest of all cipher methods where each letter of the real message has been changed into another letter. This is known as a substitution cipher.

One caution to be observed in all this work is, that there are always two sets of letters in use. One set is that of the real message which is referred to as the 'plain text', while the other set is that of the cipher letters being used. So take care to stop and think whether you going from plain to cipher, or cipher to plain.

Just about the simplest way of setting up a way of changing from plain to cipher (and back again) is by writing the alphabets on two slips of paper like that shown below, so that one can be moved relative to the other. To know how they should be placed, one letter on the cipher slip would be identified as the **key** and that letter would be placed opposite the middle A of the plain alphabets.

Two plain alphabets are needed so as to cover all possible positions of the cipher slip.



Suppose this message:-

(J) LXVNC XVHQN UYJCX WLNIA has been received.

The (J) tells us what key has been used. Normally of course the key would not be sent with the message, or else anyone could decipher it. The person for whom the message was intended would have to be told the key by some other means. This has always been a problem with sending messages in cipher.

In this case, the slips containing the two alphabets are placed as shown above with the J of the cipher slip in line with the middle A of the plain slip, and making sure that they do not move while the work is going on.

Now it is only necessary to look up each letter of the cipher message in turn on the cipher slip and write down the letter which is opposite to it on the plain slip. Written down in full the procedure would look like this:-

Cipher message: L X V N C X V H Q N U Y J C X W L N I A
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Plain message: C O M E T O M Y H E L P A T O N C E Z R

which can be re-spaced to read COME TO MY HELP AT ONCE

the Z and R at the end are merely nulls to make up the 5-group.

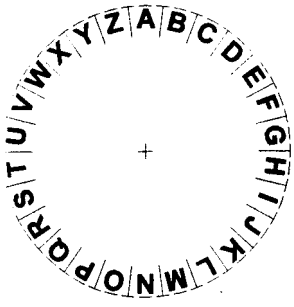
Making slips as suggested above is not the only way of doing it. The same result can be obtained by writing out the necessary alphabets with one shifted relative to the other the correct amount. Like this:-

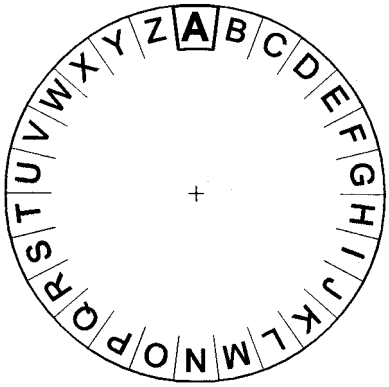
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

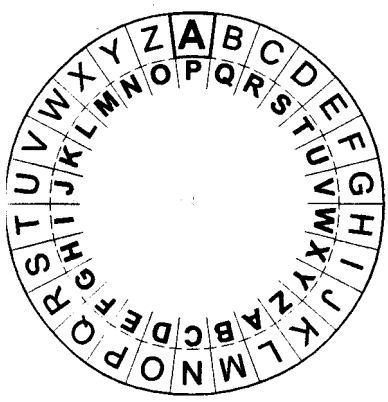
Simple Cipher Messages ~ 2

Writing out the two alphabets each time would be tedious, and the slips are a little awkward to use. A more compact way of doing the same thing is to write the two alphabets on two 'wheels' like the two shown to the left of the diagrams below. Then put the smaller on top of the larger, and fasten them through the centre so that one can be turned relative to the other. This is shown on the right.

In this case it is necessary to decide which is the cipher alphabet and which is the plain. It does not matter but, having decided which is which, you must keep to it. Here, we will declare the inner wheel to be the cipher alphabet, that is why in the final assembly on the right, the **A** on the outer (plain text) wheel has been given some prominence to show where the key letter (on the inner wheel) must be placed. The diagram is set to work with a key of P.







Use the right-hand diagram to decipher this message:-

(P) IWTPI IPRZL XAAQT BPSTD CUGXS PNGQM

Exercise 9

Using either strips, cipher-wheels, or merely by writing out the two necessary alphabets each time, decipher these messages for which the (key) is given.

1. (D) EHUHD GBWRP RYHRX WRIBR XUSOD FHTNJ
2. (Y) GUGJJ KCCRW MSMLQ SLBYW YRDMS PKXNM
3. (K) PSXNY EDXKW OYPZO BCYXM KBBIS XQZVK XCHZN
4. (N) LBHEA NZRVF XABJA GBGUR CBYVP RNFNF CLQOE
5. (G) SUTKE CORRH KYKTZ ZUVGE LUXHX OHKYV
6. (Q) RECRM YBBRU IUJJE WEEVV QJIUL UDFCM UTDUI TQOHV

Even without the key, it still not difficult to recover the original message. There are only 26 possibilities. Just keep trying them, and within the first group (of 5 letters) it should be possible to see if it is worth continuing or not. Try deciphering these.

7. VJGIQ NFYKN NCTTK XGQPU WPFCA
8. ITSTY QJYFS DTKDT ZWLFS LXUJF PYTUT QNHJR
9. IAAPK QPOEZ AYDQN YDWPJ KKJPK LWOOY KZAOX
10. CPMPW DLCPC PLOJE ZLEEL NVNTE JRPEZ FEYZH

Simple Cipher Messages ~ 3

The previous method used the cipher alphabet written in its proper order which makes it very easy indeed for anyone to recover the original message, since there are only 26 ways of matching the cipher alphabet to the plain-text alphabet. Only 25 in fact, since one of the ways would mean every letter changed into itself!

So, an immediate improvement can be made to the security if the cipher alphabet is mixed up. For example, suppose this message was found:-

BUHHY VTUUK ITUIY AIVEY

We might know, or find out, or even guess, that cipher H stood for plain E, but if we use this 'fact' to set our cipher wheels (key D) as before and decipher the message we get:-

YREEV SQRRH FQRFV XFSBV

which still makes no sense.

The cipher that was actually used to make this message was:-

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

and now the message can be read. Try it.

How will the person receiving the message know just how the cipher alphabet was mixed up? After all, there are over four hundred billion billion ways of writing down 26 letters in any order!

One way is by using a "scrambling key".

To do this, both the sender and the receiver agree on a particular word beforehand.

Suppose the agreed word to be OCTAHEDRON. The first thing to do is to write it without any of the repeated letters (O in this case) so we have OCTAHEDRN, and then write on the end of that all the letters of the alphabet, in order, which are not contained in that word. That then is the cipher alphabet to be used. In this case making

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

Exercise 10

Decipher these messages. Each has been enciphered by use of the (scrambling key) given.

1. (WATER) QLLJW KYTLL HPPML FIQDR AOLQD
2. (MYSELF) MSRCK JQQNL MGHKT ELPRB MJVWP EQANE
3. (DELIGHT) WGRNN MEGJB GVGWA DSWGI GRBQG
4. (ANYTHING) VBHKR BHYAR QAVAX RBHJC YHVCF FMFAX

One weakness of this method is that, after a certain point, the plain and cipher alphabets match. This is easily overcome with tricks like writing the second part of the cipher backwards, like this:-

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

Writing the plain alphabet backwards is another trick, and many others can be devised. The important thing is to keep the rules simple and memorable.

Simple Cipher Messages ~ 4

It can be useful to have a set of mixed-up cipher alphabets all ready to use, and the beginnings of a sheet providing just that is shown here.

Polyalphabetic Cipher Table
Plain Text

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

The complete sheet contains 26 cipher alphabets, each on it own line. At each end of the line is a single letter (the key) to identify that line and alphabet. The plain text letter corresponding to each cipher letter is found at the head of the table.

Given this message

(C) WGIVD GIQYV UJMOL

we know that the cipher alphabet to use is that on line C of the table. Since this is the last (readable) line in the portion of the table given above, the message can easily be deciphered. When working from the full version of the table it is helpful to lay a ruler or another sheet of paper across the table to help keep the search for the needed cipher letter on the correct line.

Exercise 11

Using the full table of polyalphabetic ciphers, decipher these messages.

1. (Y) YJIQP OAHOQ LHGQO ALEKN OQWEH LFGSR
2. (A) UXCDC ROKXF DZNTZ HCUZR DRPCB LRKCN ZVOTA
3. (K) GJJLV PCIUB XJVEH PQOPX TBPCJ LQELB LVQPW
4. (P) LIVZB ERSUJ VAVZS UJDJA RRAMX IORBW JNAZJ
5. (D) YXXYP QDOCC VUBRM WEMSX AYXIY DGXSU EIYFT
6. (Q) BJCVF EZVQZ JKAMK QGBKF FKOVF KFFQX LLVIB

Even without knowing what the key is, it is not difficult to decipher these messages provided that the full table of cipher alphabets is available. Try these:-

7. UREBE POAVP MSSLC CMZEX VUCLM BQBYQ BWLVG
8. WCQZI ORSKM QTILZ CHRIB MHMQR
9. FVFLL DCNQT ZNCWU ZPOCQ PZOWZ JUZKZ LLCKU
10. JXTGN DXLSM CYGSH QGNYU SCLGY MXTGL MCPXE

Put these messages into cipher, and group into fives, adding nulls where necessary. The key to be used is given at the beginning of each message.

11. (M) PREPARE TO RESIST ATTEMPT ON LIFE OF KING
12. (X) POLICE INTEND TO ARREST YOU TOMORROW

Simple Cipher Messages ~ 5

So far, each of our cipher messages has been written using the same cipher alphabet throughout its length. This is not at all secure and can be broken easily. A very much higher degree of security can be obtained by using a variety of cipher alphabets, and this is not at all difficult to do in a systematic way. One way is to use a keyword which has been agreed between the sender and receiver of the message beforehand. We will look at this system in action.

This message has been received and the agreed keyword is known to be HEXAGON.

UFYDO WOVYB QMLSG SNFHD OQGBU LECGG PCZMK

The message is written out, and the keyword is written out above the message, taking care to match letter positions, and repeating it as often as necessary for the length of the message.

HEXAG ONHEX AGONH EXAGO NHEXA GONHE XAGON
UFYDO WOVYB QMLSG SNFHD OQGBU LECGG PCZMK

Now each letter of the message is deciphered using the cipher alphabet indicated by the letter immediately above. So, U needs the **H** cipher alphabet, F needs the **E** cipher alphabet, Y needs the **X**, D needs the **A**, O needs the **G**, W the **O**, O the **N**, V the **H**, and so on.

More economically, for the working, it is better to decipher all the letters needed by a single cipher alphabet at once. So, having selected the **H** cipher alphabet to start off, work through the message and decipher the U, V, G, Q, G. Then select the **E** alphabet and decipher F, Y, S, G, G. Then the **X** alphabet, the **A**, the **G**, the **O**, and the **N**, in their turn. Until finally the message stands revealed as

I AMSU RROUN DEDHE LPISU RGENT LYNEE DEDPL

which in plain language is

I AM SURROUNDED HELP IS URGENTLY NEEDED (PL)

Exercise 12

Using the table of polyalphabetic ciphers, and the (keyword) given, decipher these messages.

1. (LIFE) IVOXH IDGCN CPYVY UTNLM OSQDE
2. (SHARK) BHAGI THNSL WMCXZ GEXGX WXNMK LJZZN
3. (FROLIC) CQWDA JVGWH IKBCZ BFZBY VJKVS LJXVM LNZNO
4. (JAWBONE) IDYLW YERDT QSCPG ZSEIU TAXLW JBGFC XOBIA
5. (HYDROGEN) SESJV GGEBG PMYCV MEURC IIYOZ JOGBZ
6. (NEIGHBOUR) NETBG LWJYI UNKUO MRNHI AHEQK JTMSO MTDWQ
7. (GOLF WIZARD) GXZBQ XMCUE VBYEQ NFDGP XJCPA ONKGV
8. (ANDREW SMITH) MICPA LTCCK VNNRX MQTGX HUNXY MVYEG FWCUG

Using the (keyword) given, put these messages into cipher, and group into fives, adding nulls where necessary.

9. (BLISTER) TAKE CARE YOU ARE NOT FOLLOWED TO MEETING
10. (BREAKOUT) YOU MUST ARRANGE FOR VAN CARRYING PRISONERS TO BE STOPPED

Simple Cipher Messages ~ 6

Cipher Strips *(St Cyr Slides)*

To make a St Cyr Slide cut out two of the strips, one Plain, one Cipher. On the Cipher strip, make slits along the two vertical lines. Feed the Plain strip through the two slits to achieve this effect.

Key Here ↓

Plain Plain

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

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

Cipher Cipher

Key Here ↓

Plain Plain

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

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

Cipher Cipher

Key Here ↓

Plain Plain

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

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

Cipher Cipher

Key Here ↓

Plain Plain

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

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

Cipher Cipher

Key Here ↓

Plain Plain

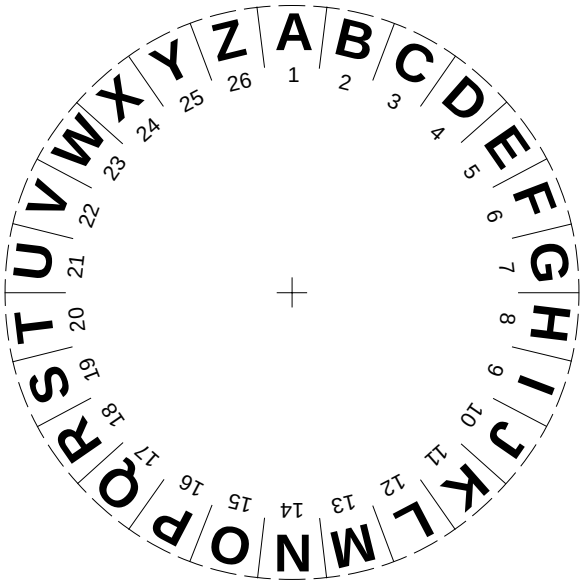
B C D E F G H I J K L M N O P Q R S T U V W X Y Z **A** B C D E F G H I J K L M N O P Q R S T U V W X Y Z

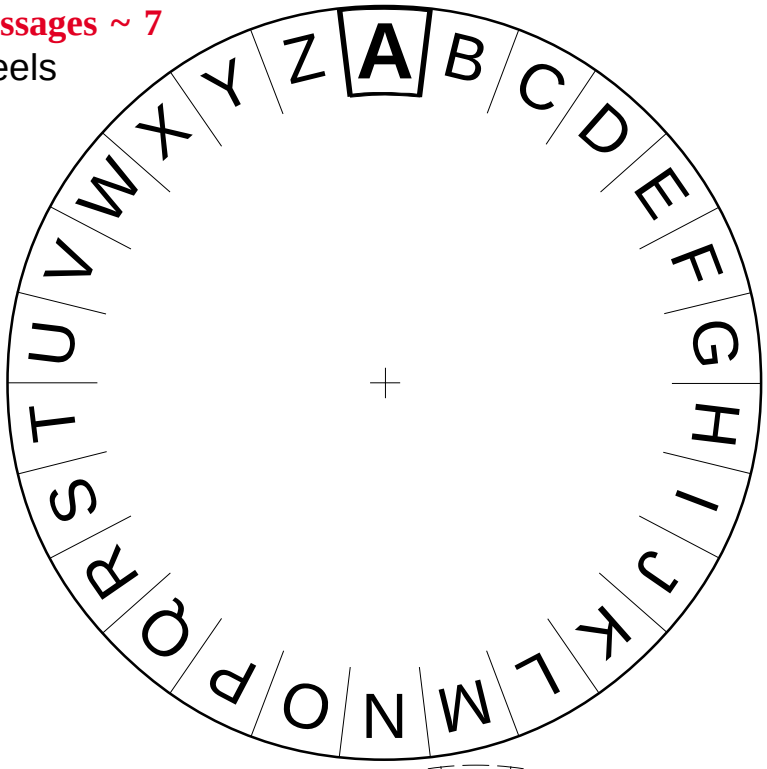
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

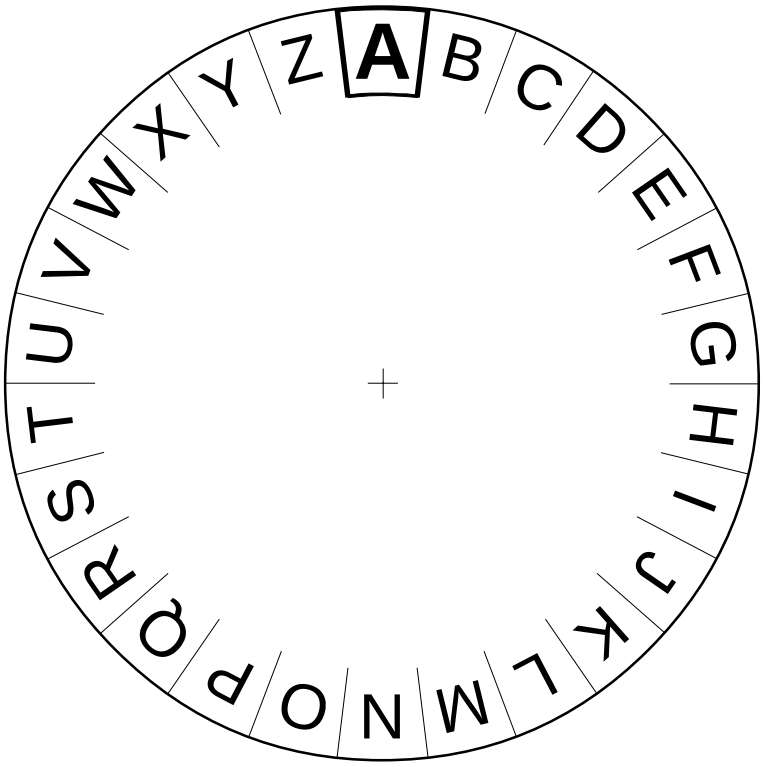
Cipher Cipher

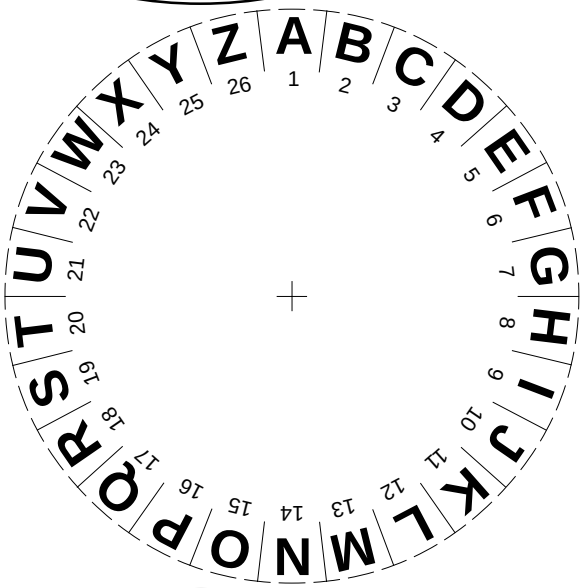
Simple Cipher Messages ~ 7

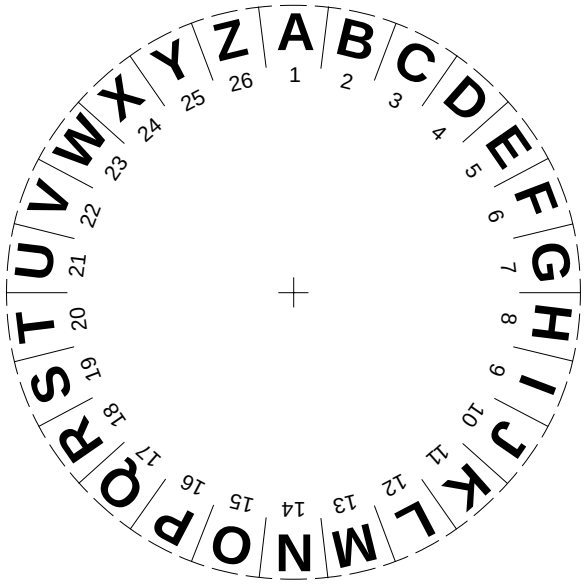
Cipher Wheels

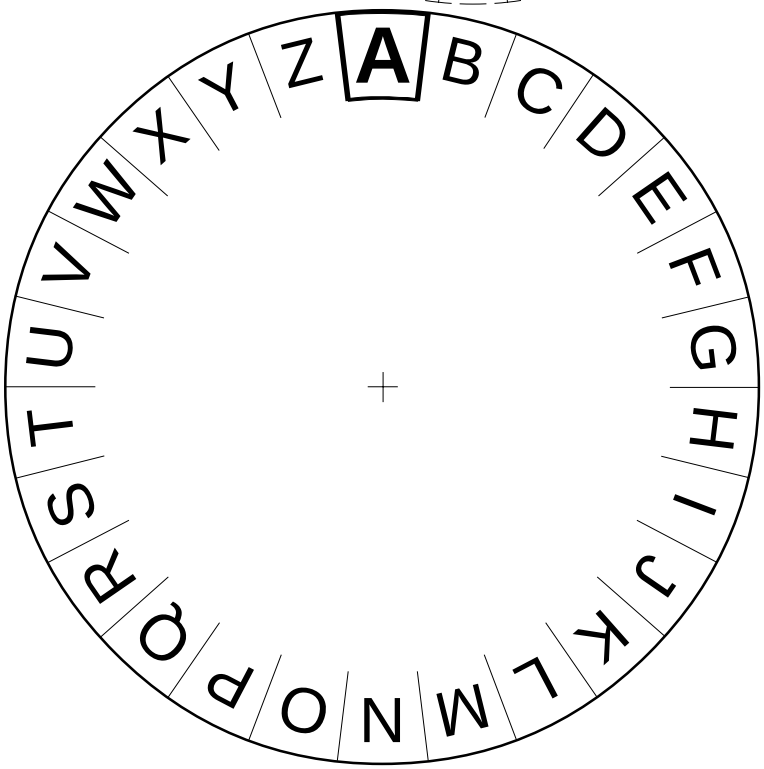












Simple Cipher Messages ~ 8

Polyalphabetic Cipher Table

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

Simple Cipher Messages ~ 9

Circle Divider (26)