Quick 'n' Easy

Here is one way to make a cipher alphabet that is easy to remember and use.

First think up a 13-letter phrase which has NO repeated letters, like:-

i must have word

and write it down, spaced out.

i m u s t h a v e w o r d

Then under it, using the same spacing, write the rest of alphabet in order,

In this case, it would produce:-

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

Now to change a plain letter into a cipher letter, you need only find the plain letter on one of the lines, and the cipher letter is the one immediately above or below it.

For example s changes to g (and g changes to s) y to r and so on.

We will put this message into cipher:-

You must be the only one to read this

The complete working would look like this:-

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

To send it, we group it into 5's (with an extra letter on the end to make it up to size).

It also usual to write messages in capital letters, making them easier to read.

RXFCF GJIPJ KPXVA RXVPJ XYPLZ JKBGX

Other Systems ~ 2

A Polybius Chequerboard

A Polybius chequerboard (or checkerboard) is simply a grid of squares which is filled-in with letters (or numbers if necessary). An example is shown on the right. The one most often seen is a 5 by 5, but it can be any size and does not have to be square. In the case of a 5 by 5 one letter has to be left out. It can be any one of the lesser-used letters (j, q, x, z). Traditionally it has been j with i being used if j should be required.

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

Next a means is needed of identifying the separate cells of the chequerboard so that each is uniquely matched to its letter. The simplest way is to number the columns and rows and then give the two numbers which locate the cell. This is done on the right so that (2,1) is the letter b (3,5) is x and so on. Usually the brackets are not used and they become simply 21 and 35. Note the need to get them in the correct order 21 (= b) is not the same as 12 (= f).

	1	**2**	**3**	**4**	**5**
	a	b	c	d	e
	f	g	h	i	k
	l	m	n	o	p
	q	r	s	t	u
	v	w	x	y	z

Clearly it would not be a good idea to put the letters on the chequerboard in the regular way we have so far - it would be far too easy to guess. Any order that is easy to remember would be better than that. Some examples are

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

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

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

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

To see how this system might be used we set up a chequerboard like that on the right. Now the rows and columns are identified by capital letters and we read the letter on the side first and then the top.

	A	**D**	**F**	**G**	**X**
A	v	w	x	y	z
D	u	g	h	i	k
F	t	f	**a**	b	l
G	s	e	d	c	m
X	r	q	p	o	n

So, AG is y and GA is s

And we will put this message into cipher

Attack starts at dawn

In the usual way we write down the plain text of the message and the cipher text underneath.

a	t	t	a	c	k	s	t	a	r	t	s	a	t	d	a	w	n
FF	FA	FA	FF	GG	DX	GA	FA	FF	XA	FA	GA	FF	FA	GF	FF	AD	XX

The final message is grouped in 5's as usual with nulls (if necessary) to make up the size.

FFFAF AFFGG DXGAF AFFXA FAGAF FFAGF FFADX XGAFX

This cipher (known as the ADFGX) was actually used by the Germans in the later years of the First World War but, only as a first stage. The cipher text given above would have been re-ciphered by another (different) method before sending. It was also developed into the ADFGVX cipher which was very much stronger. Though even that one was broken eventually.

Polybius (a Greek historian) seems to have been the first to suggest the use of a square as above to help with signalling in about 150 BC. It was only later used as a basis for producing ciphers. It is likely that Polybius did not have the idea of a cipher in mind, but was only concerned with how a message could be sent over a distance by use of signals (lighted torches in his case) with a way of matching the letters of the message to the signal.

Other Systems ~ 3

A Self-referenced Chequerboard

To make this chequerboard first set up a 5 by 5 grid. It does not actually need to be drawn, just so long as the separate cells can be visualised.

Think of a keyword. Long ones are best, but it should be easy to remember.

Write it in on the grid, putting one letter in each cell, and leaving out any repeated letters We will use the keyword MATHEMATICS which, without the repeated letters is MATHEICS and is shown in place in the first grid on the right.

M	A	T	H	E
I	C	S		

Next fill in all the other cells with the remainder of the alphabet, writing them in some memorable order, and leaving out one of J, Q, X or Z since they are little used and only 25 letters can be put in.

On the right, the filling-in, starting with B has been done by writing down and up the columns and Q has been left out.

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

To change any letter into cipher, first find the letter on the chequerboard, then identify another two letters from it. The first in the same row, the second in the same column.

So, if the plain text letter is K we may use a first letter from B L U X and a second letter from A C J G. This means the cipher for K could be any one of

BA	BC	BJ	BG
LA	LC	LJ	LG
UA	UC	UJ	UG
XA	XC	XJ	XC

And we are in the strong position of always being able to use sixteen different ways of ciphering any single plain text letter. This variety enables us to hide the frequency of some of the more common letters (like E T A O N) from anyone trying to break the cipher message.

> **Hint.** *Though there are sixteen different ways of ciphering any single plain text letter, notice there are only four different first letters and four different second letters, and that is a weakness. So, when making a selection of which cipher-pair to use, first of all use the four which have all their first and second letters different (like* BA LC UJ XC *in the above example for* K*) and then start again on another four.*

We will use this system (and the above chequerboard) to encipher this message

Help delayed hold on

In the usual way we write down the plain text of the message and the cipher text underneath.

h e l p d e l a y e d h o l d o n
TV TW UN GV JM AZ BO HK RW HX YF MR PT KT RB GL RS

Notice how the repeats E D L H O of the plain text have all 'disappeared'

The final message is grouped in 5's as usual with nulls (if necessary) to make up the size.

TVTWU NGVJM AZBOH KRWHX YFMRP TKTRB GLRST

Other Systems ~ 4

The Playfair Cipher

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

This cipher was originally based on a 5 by 5 chequerboard and that is the size used here. This one has been filled in by starting with the key phrase COUGH IS VERY BAD and the rest of the letters of the alphabet follow on (but would be better mixed up), leaving out Z.

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

It is must remembered, and drawn if necessary, that the array is cyclic. That means it can be extended by repetition in any direction, by repeating the rows and columns over and over. In fact, it is only ever necessary to be able to visualise it as far as that shown on the right, where it has been extended by one row and column on each edge.

To encipher a message with this system, it is done in 2-letter groups (digraphs). If a group would have both letters the same, insert another letter between them. Use different letters taken from the less-used varieties (Q, J, X, V, K, Y, U, B), and make sure the word cannot be mistaken for anything else. For example BALLOON could become BA LV LO ON, and there would be no need to split the OO because they would be in different groups.

Each digraph in turn now has to be found on the chequerboard, and they must meet one of three possible conditions: both in the same row, both in the same column, each in a different row and column. The rules for converting each plain digraph into a cipher digraph are these**:**
If both lettters are

in the **same row** take the two letters lying immediately to the **right** of each
Examples: SE becomes VR, DY is FB, AD is DF, CH is OC, YF is BY

in the **same column** take the two letters lying immediately **beneath** each
Examples: OB becomes SK, ME is WD, IY is YJ, SQ is BO, VT is AU
Note in the above cases in may be necessary to make use of the extensions which have been made around the edges.

not in the same row or column, imagine them lying on the corners of a rectangle. Find the two letters which are on the other two corners of the same rectangle. Take care with their order. Each of them (1st plain with 1st cipher, 2nd with 2nd) must be in the same row.
Examples: OD becomes GB, BE is DS, IW is EP, NS is KR

We will put this message into cipher using the Playfair system and the above chequerboard

We expect fresh attack will be on Southern front

WE EX PE CT FR ES HA T*Q* TA CK WI L*X* LB EO NS OU TH ER NF RO NT
GD RW WI UP NF RV UF WT UL OJ PE NT KA SG KR UG XU RI XN SH LX

Notice the *Q* and the *X* used to split the doubled letters. The final cipher message, grouped into 5's and with 3 nulls added is

GDRWW IUPNF RVUFW TULOJ PENTK
ASGKR UGXUR IXNSH LXEGW

The rules for deciphering are much the same but, for the rows change **right** to **left**, and for the columns change **beneath** to **above**.

The Playfair cipher was the first (workable) digraphic cipher. It was invented by Sir Charles Wheatstone in the middle of the 1800's but was popularised by his friend Lyon Playfair who was the 1st Baron Playfair of St. Andrews, a scientist and prominent Member of Parliament.

Hiding the Frequencies

The most important tool in breaking all ciphers is the frequency with which the letters of the plain text must have occurred. For example, in English (and many other languages), the most commonly used letter is E. In writing of any length, if the frequencies of the various letters are counted, E will provide about 12% of them. That means that about one letter in every eight is an E, and helps in breaking a simple (single letter for letter) substitution cipher.

What can be done to overcome this potential weakness? Modern cipher systems usually involve whole blocks of text at a time so that the presence of E (or any other letter) is not shown directly in the ciphering. There is another way frequencies can be hidden.

Look at the chequerboard on the right. It holds 100 letters but they are not present in equal amounts. There are12 E's 9 T's and so on, down to 1 Q and no Z's.

So, the most frequently occurring letters can be ciphered in more than one way.

The numbers on the left and at the bottom of the array are used (as coordinate pairs) to give the position of the letter. The bottom number is read first, the one on the left second.

25 would represent E, as would 84, 58, 71, 03 and several others.

9	n	t	e	w	r	o	t	f	p	i
8	a	i	h	s	n	e	l	t	m	b
7	t	o	e	c	t	d	i	a	o	s
6	r	q	a	n	g	s	e	o	l	u
5	h	y	e	i	o	r	k	p	g	e
4	u	d	t	s	a	m	n	h	e	t
3	e	x	i	e	h	d	r	c	n	a
2	w	r	f	l	e	o	a	y	t	h
1	o	a	n	c	s	h	r	e	i	d
0	s	u	e	t	i	a	o	n	l	v
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

To see the system at work we will use the chequerboard to encipher this message

It would be easy to break this in a simple cipher
as the E and T are used too often

The working is

I	T	W	O	U	L	D	B	E	E	A	S	Y	T	O	B	R	E	A	K	T	H
67	47	02	76	10	68	53	98	27	84	08	56	72	82	45	98	12	25	62	65	30	43

I	S	I	N	A	S	I	M	P	L	E	C	I	P	H	E	R	A	S	T	H	E
81	41	18	64	44	97	23	54	89	80	29	73	35	75	05	71	63	26	38	69	74	95

E	A	N	D	T	A	R	E	U	S	E	D	T	O	O	O	F	T	E	N
42	50	70	57	19	93	06	66	96	34	03	91	94	59	52	87	22	78	58	48

The only repeated cipher group is for B, so the frequency count would be very 'flat' and the message unbreakable without some other knowledge. Grouped in 5's with two nulls at the end, it would be sent as

67470 27610 68539 82784 08567 28245 98122 56265 30438
14118 64449 72354 89802 97335 75057 16326 38697 49542
50705 71993 06669 63403 91945 95287 22785 84832

The ADFGVX Cipher

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	1	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

The chequerboard on the right provides a way of changing the plain text letters and numbers a, b, c, d, … x, y, z, 1, 2, 3, … 9, 0 into the cipher letters A D F G V X. It always takes two cipher letters to identify each element of the plain text, and the cipher letter on the left side is always put before the one on the top so, FX is d and not 7 (which would be XF).

Encipherment is in two parts.

The message to be enciphered is

Major Smith is a spy

Part one is the 'standard' substitution method using the above chequerboard.

m	a	j	o	r	s	m	i	t	h	i	s	a	s	p	y
DA	DG	FV	AD	VX	GD	DA	GF	XG	GV	GF	GD	DG	GD	VA	GG

Part two first requires the ciphered message to be put into rows and columns, with one letter in each column, and each column numbered. We will use eight columns giving four rows.

1	2	3	4	5	6	7	8
D	A	D	G	F	V	A	D
V	X	G	D	D	A	G	F
X	G	G	V	G	F	G	D
D	G	G	D	V	A	G	G

Now a **key** is used. This requires the column numbers to be put in some different order. We will use 3 1 6 5 2 8 4 7. The columns are now re-arranged in the order of the key.

3	1	6	5	2	8	4	7
D	D	V	F	A	D	G	A
G	V	A	D	X	F	D	G
G	X	F	G	G	D	V	D
G	D	A	V	G	G	D	G

and the rows are read off from left to right, starting with the top row, to make the cipher message to be sent. Grouped in 5's with nulls added to make up the last group it is

DDVFA DGAGV AGXFD GGXFG GDVDG DAVGG DGAXV

Reading that by using the chequerboard but not using the key to re-order the columns shows the message starting

kvo5ho7au0 ...

which makes little sense! Given that the chequerboard and the key could be changed frequently it was believed to be a very secure system.

This cipher was used by the Germans in WW1 and it produced one of the famous triumphs of cryptanalysis.. The cipher was broken by Lieutenant Georges Painvin of the French Army in 1918 (the last year of the war) and, together with some other information, resulted in the Germans losing a crucial battle (on June 9th) in what was to be their last push to capture Paris.

The letters ADFGVX were chosen because in sending messages over the radio in Morse code, those particular letters were the ones most likely not to be confused with each other.

Book Ciphers

This requires the two people who wish to communicate with each other to have identical copies of the same book. Then consider the alphabet to be numbered. A = 1, B = 2, … Z = 26 etc. and define addition of letters by using their number equivalents.
For instance, C + H = K (3 + 8 = 11) and that can be done for all the letters of the alphabet.

To make use of this, and save the bother of changing the letters into and out of numbers all the time, we compile a table which shows the results of adding any two letters. The letters to be added are identified as the Additive text and the Plain text, and the answer is the Cipher text.

Plain text

Additive text +	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	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	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	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	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	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	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	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	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	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	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	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	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	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

First identify a starting place in the book, say page 147, line 36, at the 25th letter, and that is then our Additive text, which can go on for as long as required. Ours starts at 'n' and goes

"… ng of a great adventure that was to result in many …"

Starting with 'n' it is added, letter by letter, to the Plain text of the message to make the Cipher
Let the message be Keep watch to the South and be clever. It could be done like this

Add.txt. n g o f a g r e a t a d v e n t u r e t h a t w a s t o r e
Plain K E E P W A T C H T O T H E S O U T H A N D B E C L E V E R
Cipher Y L T V X H L H I N P X D J G I P K M U V E V B D E Y K W W

Sending YLTVX HLHIN PXDJG IPKMU VEVBD EYKWW

Of course the recipient of the message needs to know where the Additive text starts (like 147-36-25 or even 1473625) and that is best communicated by some other means.

Deciphering is done in a similar way, but this time the table needs to be used differently. Having found the Additive text letter on the left, go along that row until the Cipher letter is found, and go up to the Plain text letter. This is a running-key cipher and is very secure.

Other Systems ~ 8

Symbol Ciphers

Cipher messages are usually written with letters and numbers, but apparently meaningless symbols can also be used. Here is such a message

♥ * * § ♠ § ♥ Ξ Ψ ♠ # ♠ # Φ Φ ‡ # ♦ % !

If you have difficulty in reading that try using this table.

A = #	F = @	K = Δ	P = ∞	U = ✠
B = $	G = †	L = Φ	Q = ♣	V = ✡
C = &	H = ‡	M = Ω	R = ♦	W = ⌘
D = %	I = §	N = Ξ	S = ♥	Y = ✪
E = *	J = ¶	O = Ψ	T = ♠	X/Z = ✠

Now while there might be a time and place for such things, it is not a very handy cipher system if it has to be written by hand. First, a copy needs to kept since it is scarcely possible to memorise it, and that would be a damning piece of evidence if caught for spying! Then, it might get lost or be stolen. And symbols are not easy to draw, so they might be confused. What is really needed is a symbol cipher that is easy to memorise, even if it needs to be written down each time in order to use it. After all, it can always be destroyed once the need for it has passed. For that reason, just such a cipher was invented many centuries ago. It became known as

The Pig Pen Cipher

First of all a grid is drawn and the letters of the alphabet are filled-in. Some examples of how it might be done are these.

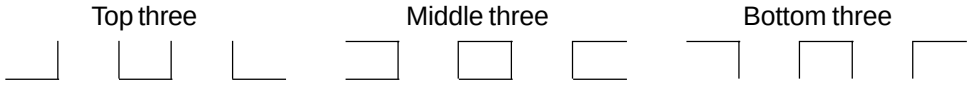
A B C	D E F	G H I
J K L	M N O	P Q R
S T U	V W X	Y Z

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

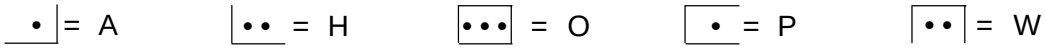
N I G	H T C	L U B
W A V	E F O	R M S
P D Q	J K	X Y Z

Now two things need to be signalled. One is which of the nine cells of the grid is needed, and the other is, which of the letters in that cell is the correct one to take.

The nine different cells can be indicated by their distinctive shapes. They are



The letter to be used is shown by putting 1, 2 or 3 dots in the shape meaning it is the first, second or third letter that is meant. So, based on the left hand grid



Here is a message in Pig Pen cipher which uses the right hand grid