Copyright © 2008, Wimborne Publishing Ltd
(Sequoia House, 398a Ringwood Road, Ferndown, Dorset BH22 9AU, UK)
and TechBites Interactive Inc.,
(PO Box 857, Madison, Alabama 35758, USA)

All rights reserved.

The materials and works contained within EPE Online — which are made available by Wimborne Publishing Ltd and TechBites Interactive Inc — are copyrighted.

TechBites Interactive Inc and Wimborne Publishing Ltd have used their best efforts in preparing these materials and works. However, TechBites Interactive Inc and Wimborne Publishing Ltd make no warranties of any kind, expressed or implied, with regard to the documentation or data contained herein, and specifically disclaim, without limitation, any implied warranties of merchantability and fitness for a particular purpose.

Because of possible variances in the quality and condition of materials and workmanship used by readers, EPE Online, its publishers and agents disclaim any responsibility for the safe and proper functioning of reader-constructed projects based on or from information published in these materials and works.

In no event shall TechBites Interactive Inc or Wimborne Publishing Ltd be responsible or liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or any other damages in connection with or arising out of furnishing, performance, or use of these materials and works.

READERS' TECHNICAL ENQUIRIES

We are unable to offer any advice on the use, purchase, repair or modification of commercial equipment or the incorporation or modification of designs published in the magazine. We regret that we cannot provide data or answer queries on articles or projects that are more than five years' old. We are not able to answer technical queries on the phone.

PROJECTS AND CIRCUITS

All reasonable precautions are taken to ensure that the advice and data given to readers is reliable. We cannot, however, guarantee it and we cannot accept legal responsibility for it. A number of projects and circuits published in EPE employ voltages that can be lethal. You should not build, test, modify or renovate any item of mains-powered equipment unless you fully understand the safety aspects involved and you use an RCD adaptor.

COMPONENT SUPPLIES

We do not supply electronic components or kits for building the projects featured; these can be supplied by advertisers in our publication Practical Everyday Electronics. Our web site is located at www.epemag.com

We advise readers to check that all parts are still available before commencing any project.

www.epemag.com

To order you copy for only $18.95 for 12 issues go to www.epemag.com

Constructional Project

PIC MINI-ENIGMA

NICK DOSSIS

Share encrypted messages with your friends – true Spymaster entertainment!

PIC Mini-Enigma was born out of the author's interest in both encryption techniques and PIC microcontrollers. The initial idea was to create a PIC-based unit that would enable the user to type in a brief text message, which can then be encrypted at the press of a button.

By the same token, if the encrypted message was typed into the unit it could be decoded into the original text message. This would enable two people to send secret messages to each other and be safe in the knowledge that the text would be very difficult to decipher without using the unit.

The design also has the unique capability of allowing the user to download a message to the data EEPROM (electrically erasable programmable read only memory) of a second PIC, housed in a tiny box, such as a matchbox. The information from the "matchbox" memory can then be retrieved by the other person at a later time by using their own Mini-Enigma unit.

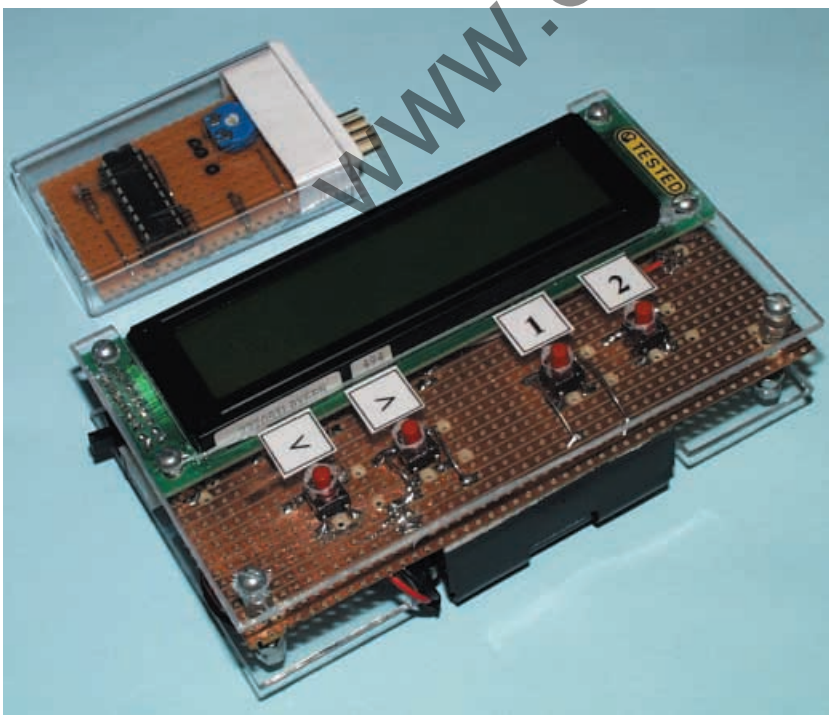
DATA SWAPPING

At the time that the idea was conceived, the author was playing around with the PIC16F84 and an alphanumeric liquid crystal display (l.c.d.). After connecting the l.c.d. to the PIC and programming it to show a line of text, it was discovered that some of the characters were being displayed incorrectly.

Further investigation showed that two of the data lines from the PIC to the l.c.d. had inadvertently been swapped over. It was this error which had caused the incorrect text to appear on the screen.

This gave rise to thoughts about the way the l.c.d. requires an ASCII-coded data byte to be sent to it to cause the required letter to be displayed. Naturally, by suitably altering the order of the bits that make up the byte, a different character could be displayed instead.

This seemed to be an ideal way of encrypting a line of text within the PIC, and is the basis of the program that controls this project.



ENIGMATIC

The original Enigma unit was a coding machine used in the Second World War by the Germans. It was a very complex machine, which amongst other features contained interchangeable connecting wires and rows of scramblers, which changed their position every time a letter was encoded.

This method ensured that there was hardly any duplication of encoded text because the letters were altered automatically after every encryption. It took the British several years to crack Enigma's coding technique.

The Mini-Enigma described here does not profess to be the miniature equivalent of the original machine. However, the encryption technique uses a coding method that alters the way individual letters are encrypted. To the untrained eye, it is very difficult to crack the code.

ENCRYPTION METHOD

The method of encryption, which is documented in the assembly program, utilises a codeword set by the user and which is stored in the Enigma's data EEPROM. This means that the way in which the message is encrypted can be altered and so deciphering the text will only be possible by using the same codeword that was used to encrypt the original message. The codeword can be up to eight digits long.

First, regard alphabet letters A to Z as numerical values from 1 to 26. Then, for example, if the codeword is set as ABCD this would have an equivalent numerical value of 1234 (see Table 1). Now suppose the message BYEBYE needs to be encrypted, the process is as follows:

Since the codeword is ABCD, its first letter, A, has an allocated value of 1. This is added to the allocated value of the first letter of the message, B, i.e. B + 1 = C. C thus becomes the code letter for B at this point of the encryption.

The second letter of the message has the value 2 added to it as it is the alphabet value of second character of the combination. This converts the letter Y into letter A.

www.epemag.com

This procedure repeats itself until the last letter of the codeword has been reached. The process then begins again by starting back at the first number of the codeword.

In this fashion, the message BYEBYE becomes encrypted as CAHFZG. See Example 1.

Example 1:

Message	B	Y	E	B	Y	E
Codeword	A	B	C	D	A	B
	1	2	3	4	1	2
Encryption	C	A	H	F	Z	G

It can clearly be seen that the encryption method is very secure because although the original message contains two identical words, the encrypted version does not give any clues that this is the case. Remember also that the Mini-Enigma can be programmed to accept an 8-digit codeword comprising any of the 26 letters of the alphabet, therefore making the possibility of somebody decoding the encrypted message even harder.

It should be noted that the encrypted message is totally dependent on the codeword. Mini-Enigma units which have been programmed with different codewords will encrypt the message in a totally different way. An example of this is outlined in Example 2 when the codeword is changed to BCDE.

Example 2:

Message	B	Y	E	B	Y	E
Codeword	B	C	D	E	B	C
	2	3	4	5	2	3
Encryption	D	B	I	G	A	H

The basis of the software is to either add or subtract the individual codeword values to the ASCII code which is sent to the l.c.d. Coding the text adds the value and decoding the text subtracts the value.

The problem encountered when using this method was that ASCII codes 27 to 38 are not letters and therefore there had to be software routines incorporated to bypass these values when an addition or subtraction occurred.

DATA TRANSFER

As mentioned earlier, the unit also includes the facility for downloading an encrypted message into the data EEPROM of a second PIC, housed in a separate box, from hereon referred to as the "Matchbox" unit.

The data transfer uses a unique protocol which was specifically designed for this project and allows the encrypted ASCII code of each character to be transmitted serially from the unit to the PIC inside the Matchbox.

The connections between the Mini-Enigma unit and the Matchbox are via a 4-pin connector. These connections comprise the +5V and 0V supply, plus data and clock lines.

For all intents and purposes, the data is transmitted over two wires, data and clock. Because the Matchbox is controlling the data transfer and its clock is running at a slower speed than the Mini-Enigma, this ensures that the data transfer runs without errors. There is specific handshaking associated with the protocol, which is written into the software of both units.

When the Matchbox is first energised, it waits for either a "load" or "save" instruction from the Mini-Enigma.

Lines:	Clock	Data
Load:	0	1
Save:	1	0

Table 1 – ASCII and Codeword Values used in the Enigma Unit

	Letter	ASCII Code	Codeword value		Letter
1	A	0100 0001	0000 0001	1	A
2	B	0100 0010	0000 0010	2	B
3	C	0100 0011	0000 0011	3	C
4	D	0100 0100	0000 0100	4	D
5	E	0100 0101	0000 0101	5	E
6	F	0100 0110	0000 0110	6	F
7	G	0100 0111	0000 0111	7	G
8	H	0100 1000	0000 1000	8	H
9	I	0100 1001	0000 1001	9	I
10	J	0100 1010	0000 0010	2	J
11	K	0100 1011	0000 0011	3	K
12	L	0100 1100	0000 0100	4	L
13	M	0100 1101	0000 0101	5	M
14	N	0100 1110	0000 0110	6	N
15	O	0100 1111	0000 0111	7	O
16	P	0101 0000	0000 0000	0	P
17	Q	0101 0001	0000 0001	1	Q
18	R	0101 0010	0000 0010	2	R
19	S	0101 0011	0000 0011	3	S
20	T	0101 0100	0000 0100	4	T
21	U	0101 0101	0000 0101	5	U
22	V	0101 0110	0000 0110	6	V
23	W	0101 0111	0000 0111	7	W
24	X	0101 1000	0000 1000	8	X
25	Y	0101 1001	0000 1001	9	Y
26	Z	0101 1010	0000 0010	2	Z

Once it has received its instruction, the Matchbox program is then diverted to the relevant routine. The basis of the protocol is shown later in Table 2.

ENIGMA CIRCUIT

The circuit diagram for the Mini-Enigma is shown in Fig.1.

The heart of the system is the PIC16F84 microcontroller, IC2. Its oscillator is run in *RC* (resistor-capacitor) mode, with potentiometer VR2 presetting the speed. The capacitance is that inherent in the PIC itself and a separate capacitor is not used.

Even though communication between the Mini-Enigma and the additional Matchbox memory uses serial data transfer, software routines ensure that the exact timing is not too critical. Consequently, crystal control is not needed.

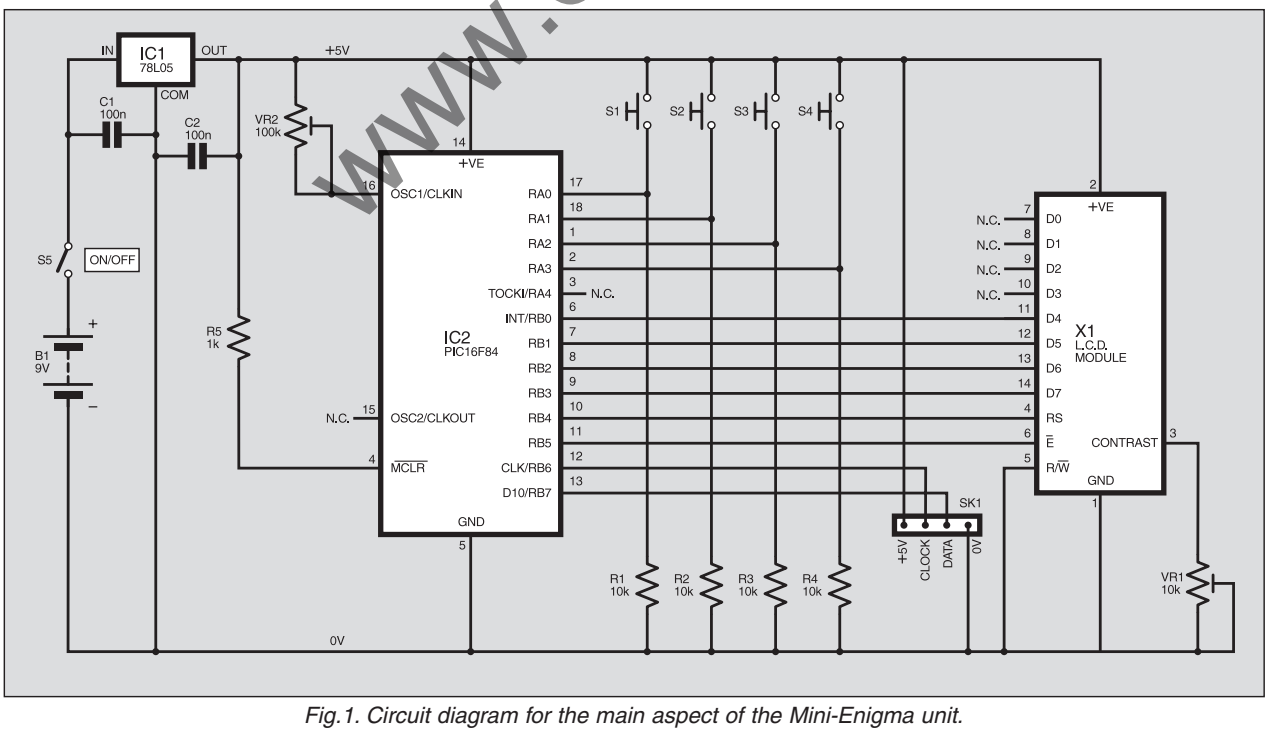


Fig.1. Circuit diagram for the main aspect of the Mini-Enigma unit.

www.epemag.com

The PIC is connected via port pins RB0 to RB5 to a 20-character × 2-line alphanumeric liquid crystal display (l.c.d.), X1. This is controlled in standard 4-bit mode. Preset potentiometer VR1 controls the screen contrast.

PIC port pins RA0 to RA3 are held normally-low by resistors R1 to R4 and are taken high whenever the relevant pushbutton switch, S1 to S4, is pressed.

Communication with the Matchbox memory unit is via clock pin RB6 and data pin RB7.

The circuit is powered by a 9V PP3 battery, via on/off switch S5. Regulator IC1 reduces the supply to +5V, as required by the PIC and l.c.d. Capacitors C1 and C2 decouple and smooth the supply.

MATCHBOX MEMORY CIRCUIT

The circuit diagram for the additional Matchbox memory unit is shown in Fig.2. It consists primarily of another PIC16F84 microcontroller, IC3. It does not require a battery because it receives its power from the host Mini-Enigma via the 4-way connector.

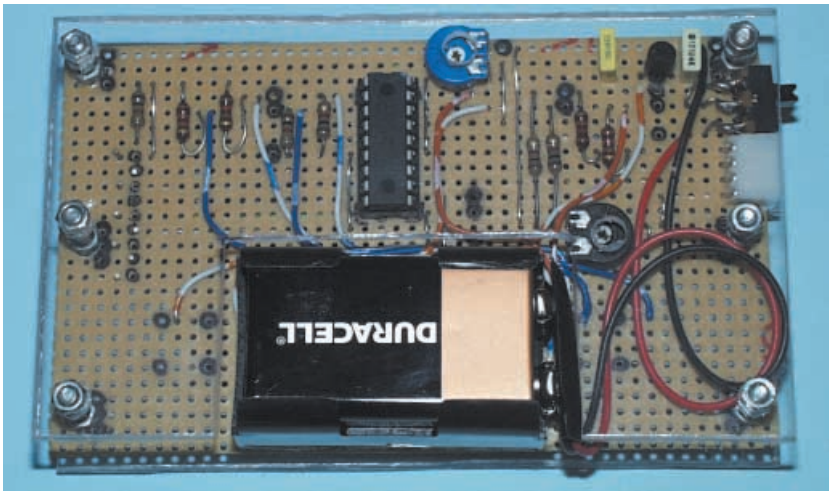
The clock and data lines are held normally-low via resistors R6 and R7, but are under control of the Mini-Enigma when the two units are connected.

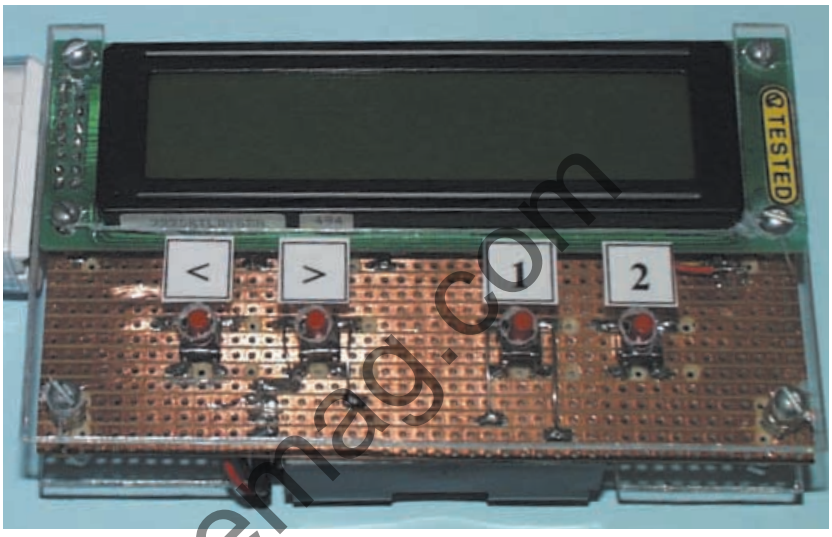
This PIC runs at a slower speed than the one in the Mini-Enigma, as set by capacitor C3 and variable by preset VR3.

ENIGMA BOARD

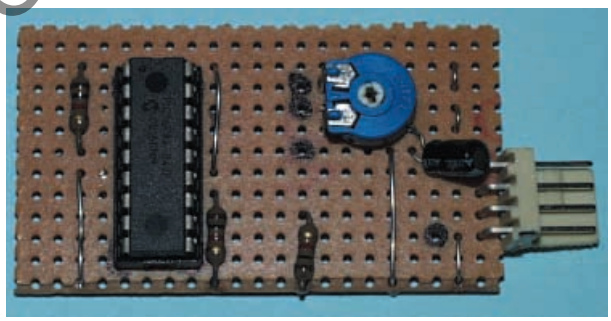
The component layout and track cutting details for the Mini-Enigma and its Matchbox unit are shown in Fig.3. Ensure that all the track cuts are made. Use 22s.w.g. plastic covered solid copper wire for the link connections. Dual-in-line (d.i.l.) sockets should be used for the PICs.

Referring to Fig.3a, solder the components onto the stripboard in the following order: d.i.l. socket, links, resistors, 1mm terminal pins, voltage regulator, capacitors, on/off switch S5, edge connector, pushbutton switches S1 to S4, and the battery lead.





Note that the published Mini-Enigma has fewer resistors than shown in the top photograph.



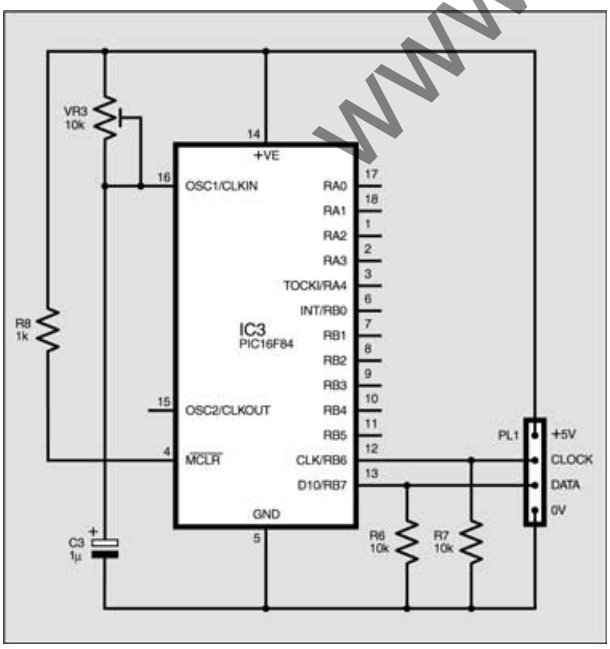


Fig.2. Circuit diagram for the "Matchbox" unit.

Note that switches S1 to S4 plus four additional link wires are soldered on the track-side of the stripboard.

Once the basic stripboard assembly is complete, use double-sided tape to stick the battery holder onto the back of the stripboard. Then connect the longer wires that route around the battery.

Do not wire-up the l.c.d. or plug in the PIC yet.

Check that the component layout and solder joints are sound. If at any stage of testing the results are not correct, disconnect the battery immediately. Re-check the component positions and solder joints, and then restart the checks.

Apply power to the stripboard and check that +5V appears at various components according to the circuit diagram. If all is well following this initial power check, disconnect the battery, connect the l.c.d., making sure that there is enough slack in the cable to assemble the unit, and then insert the preprogrammed PIC (assembly file E2.ASM). With power applied again, do another check that 5V is still present as required.

Check that the PIC's input pins 1, 2, 17 and 18 are normally low, and that pressing the pushbutton switches makes the relevant pins go high.

www.epemag.com

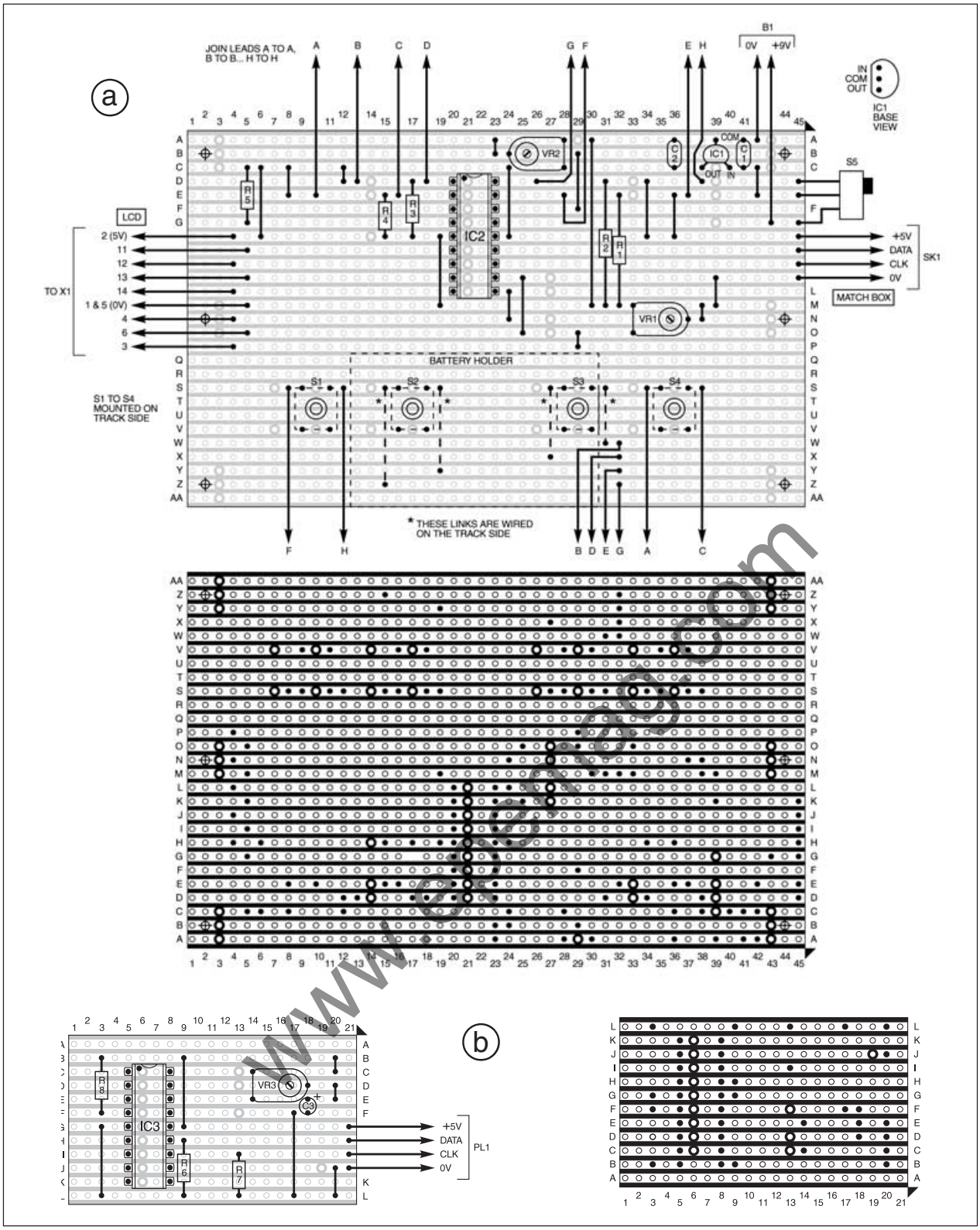


Fig.3. Stripboard component layouts and details of underside copper track breaks for the Mini-Enigma (a) and Matchbox unit (b). Note that in Fig.3a switches S1 to S4 and four link wires are mounted on the trackside. The lettered links should be made using insulated solid hook-up wire, linking like-lettered points (i.e. A to A, B to B, etc.).

Adjust the l.c.d. contrast control, VR1, until the start-up screen is seen clearly. The screen display modes are discussed later.

Adjust the clock rate control, VR2, until the unit works at a satisfactory speed for pushswitch presses. In the prototype, this was with VR2 set for a resistance of about 10kΩ to 15kΩ.

MATCHBOX MEMORY BOARD

Referring to Fig.3b, assemble the Matchbox memory board.

The small piece of stripboard used was intended to be small enough to fit snugly inside a standard size matchbox. A matchbox was felt to be suitable because it is inconspicuous and conceals the electronics, an ideal cover for the budding spy!

However, the author found that the stripboard is also the ideal size to fit inside an empty Tic-Tac box, the clear box matching the theme of the Enigma unit. So this is the enclosure that was used in the prototype.

www.eprint.com

COMPONENTS

Resistors
R1 to R4, R6, R7 10k (6 off)
R5, R8 1k (2 off)
All 0·6W metal film

See SHOP TALK page

Capacitors
C1 to C2 100n ceramic, 0·2in pitch
C3 1μ radial elect. 16V

Potentiometers
VR1, VR3 10k min. horiz. skeleton preset (2 off)
VR2 100k min. horiz. skeleton preset

Semiconductors
IC1 78L05 +5V 100mA voltage regulator
IC2, IC3 PIC16F84 microcontroller, each separately pre-programmed (2 off)

Miscellaneous
S1 to S4 push-to-make switch, p.c.b. mounting 0·2in x 0·3in pitch, 6mm to 7mm "push actuator" (see text) (4 off)
S5 min s.p.c.o. slide switch, p.c.b. mounting
SK1 4-way edge connector, female, p.c.b. mounting
PL1 4-way edge connector, male, p.c.b. mounting
X1 2-line x 20-characters per line alphanumeric l.c.d., with standard HD44780 controller
Stripboard, 0·1in pitch, 45 holes x 27 strips; stripboard, 0·1in pitch, 21 holes x 12 strips; 18-pin d.i.l. socket (2 off); 25mm 6BA nuts and bolts (see text); clear acrylic perspex sheet (2mm x 117mm x 70mm) (2 off); 9V PP3 battery and connecting clip; Tic-Tac box (see text).
Software: Available as stated in *Shoptalk*.

Approx. Cost Guidance Only

£25 *excluding case*

The 4-way edge connector is fitted to the stripboard so that it protrudes through the hole in the Tic-Tac box, although the hole needs to be made a little larger to stop the box fouling on the Enigma's on/off switch when the two units are plugged together.

Solder components onto stripboard in order of d.i.l. socket, link wires, resistors and edge connector. Do not insert the PIC yet. Check the assembly for errors.

Adjust VR3 (PIC clock rate) for an effective resistance of about 3·1kΩ to 3·8kΩ.

Before inserting the PIC, plug the unit into the Enigma's connector (space limitations may make it necessary to switch on the Enigma first). Check that +5V is present as indicated in the circuit diagram.

If the checks are satisfactory, disconnect the unit from the Enigma and insert the second preprogrammed PIC (assembly file EEPROM.ASM).

ENCLOSURE

The author wanted the Mini-Enigma to look a little bit different from the usual constructional projects, but did not find the standard types of enclosure to be suitable. Consequently, the prototype was built using two pieces of 2mm thick clear acrylic perspex which form the "bread" of the stripboard sandwich.

Referring to Fig.4, cut the two pieces of perspex to the same size. Cut the slots and drill to match the mounting holes in the stripboard and l.c.d. Drill additional holes in the front piece of perspex to allow the pushbutton switches (S1 to S4) to protrude through. The whole unit is transparent allowing the electronics to be visible.

Cut a space in the back piece of perspex to allow access to the PP3 battery without having to take the unit to pieces. The 4-way female serial connector is mounted on the side of the stripboard and is positioned so that the Matchbox memory unit is able to be plugged into the Mini-Enigma.

The on/off slide switch, S5, is also mounted at the side.

The whole sandwich can now be combined into one unit, using 6BA bolts and with additional nuts to create spacers between the l.c.d. and the stripboard. Labels can now be secured above the

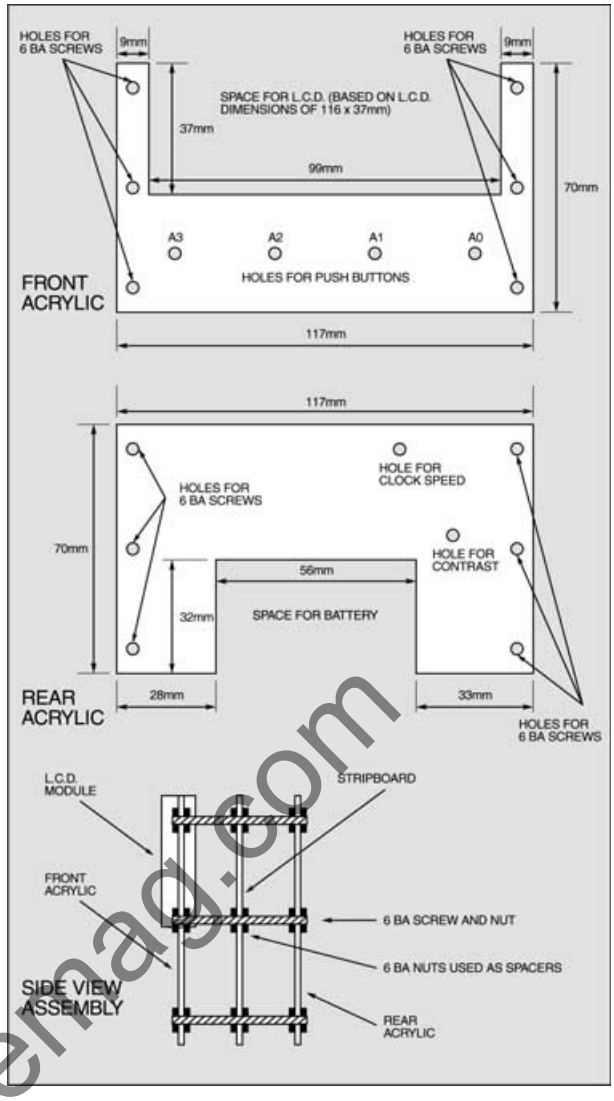
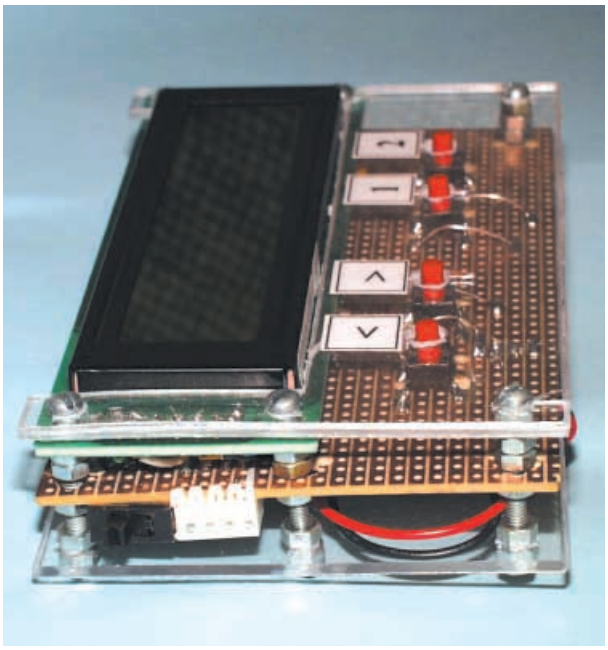


Fig.4. Construction details of the perspex plates and how they "sandwich" the Mini-Enigma stripboard.



End view of the assembled Mini-Enigma "sandwich".

www.epemag.com

pushswitches, showing from left to right the legends "<", ">", "1", "2" (see photos).

CODE CHECKS

When assembly and checking are complete, insert the pre-programmed PICs, follow the operating instructions discussed presently and check that data can be interchanged between units.

First code a line of text on the main unit and then save it into the Matchbox. Switch everything off and then attempt to load the data back into the Enigma. If problems are experienced when transferring data, adjust the speed of the Matchbox using preset VR3 and try again.

From experience there is quite a narrow "window" for the resistance value, found to be around 3kΩ to 4kΩ. It should be noted, however, that once data transfer has been achieved successfully VR3 should never need to be adjusted again.

OPERATING TECHNIQUE

When the Enigma is first switched on, the Start-up screen appears:

Start-up screen.

Pressing any key changes the display to show Screen 1, in which instructions are given on the lower line:

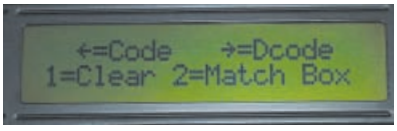
Pressing switch "<" or ">" causes the current letter of the codeword or message you wish to record, as shown on the top line and underlined, to rotate down ("<") or up (">") through the alphabet. When the required letter is reached, press switch "1" (Enter) to select it. The underline then moves to the next character cell and the required letter can again be reached by using "<" or ">", and selected by "1".

Screen 1, for entering a message or codeword.

If a wrong letter is entered this can be rectified by again pressing switch "1" before pressing "<" or ">". This deletes the last letter entered.

A message of up to 40 characters can be entered onto the top line if required. Once 20 characters have been entered, both lines of the screen rotate to the left so that the text can be followed on the screen, with the instructions being duplicated so that they can be seen at all times.

Once the codeword or message has been completed switch "2" (Next) can be pressed, to take you to Screen 2:

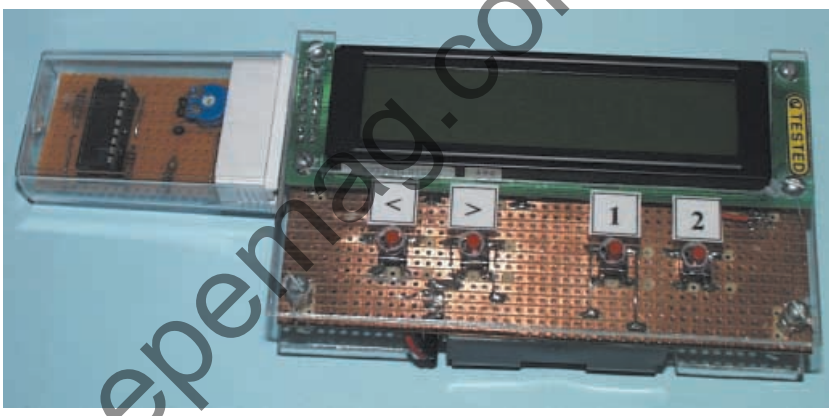


Screen 2, function choice.

Table 2 – Data Save and Load Routines

Step	Mini-Enigma	Matchbox Unit
1.		Wait for Save signal
2.	Send Save signal	
3.		Accept Save signal
4.		Send high clock signal
5.	Receive high clock signal	
6.	Send data bit X	
7.		Accept bit X
8.	Wait for low clock signal	
9.		Process data and send low clock signal
10	Receive low clock signal	
11.		Loop back to step 4 until 8-bit word is complete
12.		Store 8-bit word in EEPROM memory
13	Loop back to step 5 until 8-bit word is complete	

Step	Mini-Enigma	Matchbox Unit
1.		Wait for Load signal
2.	Send Load signal	
3.		Accept Load signal
4.	Pause	
5.		Retrieve EEPROM memory
6.	Wait for high clock signal	
7.		Send high clock signal and data bit X
8.	Accept high clock signal and data bit X	
9.		Send low clock signal
10.	Accept low clock signal	
11.		Loop back to step 5 until 8-bit word is complete
12.	Loop back to step 6 until 8-bit word is complete	
13.	Store data in indirect file memory	



Matchbox unit plugged into Mini-Enigma.

If the unit has been powered up for the first time, or if the codeword is to be altered, press switch "2" (now indicated as Match Box). This will take you to Screen 3:

Screen 3. Second choice of functions.

Pressing "1" (codeword) then shows a screen display such as the following:

Screen 4. Choice of codeword saving or retention.

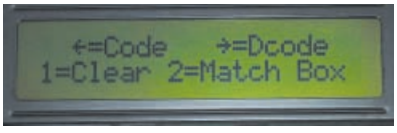
The top line shows the new codeword just created via Screen 1 (e.g. ABCD). The second line shows the current codeword already stored in the Enigma's EEPROM (e.g. ZYA). Pressing the "<" switch stores the top line codeword into the EEPROM as the new codeword, overwriting the existing one. However, pressing the ">" switch instead causes the new codeword to be ignored, while retaining the existing one.

In either instance, the switch press causes Screen 1 to be displayed again.

A text message can then be "keyed in" using the "<", ">" and "1" keys, e.g.:

Screen 1 again, for message entering.

Once complete, pressing switch "2" once more displays Screen 2:



Screen 2 again, this time for choice of message function

www.epemag.com

If the text entered is a normal message and you wish to encrypt it, press "<". If the text entered is encrypted and you wish to discover the original message, press ">". If you wish to abort, pressing "1" clears the memory and returns to Screen 1, allowing you to enter some new text.

If either the "<" or ">" switches are pressed, the screen then shows two lines of text, the top line is the original text which was entered (either manually or via the matchbox), and the bottom line is the coded or decoded version.

An original message (top) and its encryption (lower).

Pressing the "<" or ">" switches while viewing the text shifts the screen left or right. This is particularly useful when the message contains more than 20 letters.

Once the viewing of text has been finished, press "2", which returns the display to Screen 2. This causes the coded or decoded text (as just shown on line 2) to be stored in the Enigma's memory. Coding or decoding can be carried out again if wished. Pressing "1" clears the memory and returns to Screen 1.

TRANSFERRING DATA

A 40-digit encrypted message can be "saved" to a Matchbox memory unit for future retrieval. The procedure for this is as follows:

Type in the required message and proceed to Screen 2 to encrypt the message. Once the encrypted message is on the screen, press "2" to return to Screen 2. As said earlier, this has the effect of storing the encrypted message in the Enigma's memory. Plug the Matchbox memory into Enigma and then press "2" again, which then produces the following message on Screen 3.

Screen 3 again, offering choice of data transfer function.

Pressing the appropriate key begins the data transfer either to ("<" save) or from (">" load) the Matchbox memory. The following screen appears just prior to loading commencing:

Screen immediately prior to loading a Matchbox message.

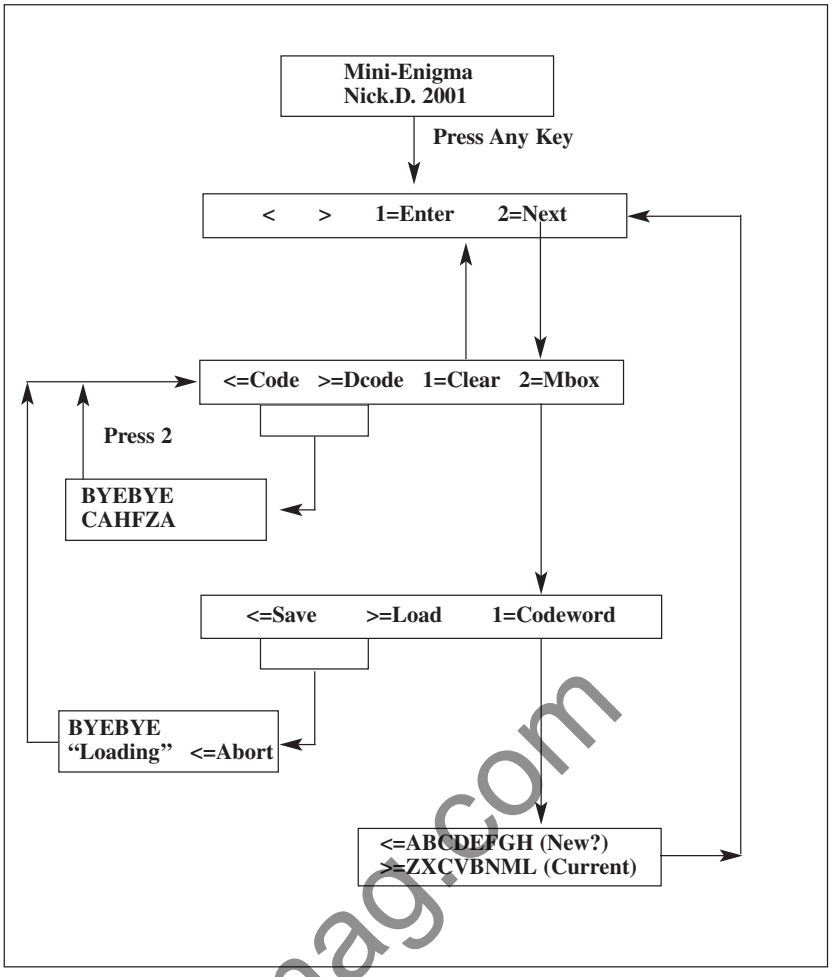
When loading or saving data, each letter transferred appears on the screen starting on line 1. If the message is shorter than 40 characters then the data transfer finishes once the final letter of the message has been received. The program does this by looking for ASCII code 128 (binary 1000000). If this character is recognised as being transferred then both programs end the data transfer.

The data transfer takes about 100 seconds for all 40 characters, and once complete the l.c.d. reverts back to Screen 2. This allows the user either to clear the Enigma's memory and start again, or to decode the received message. Once the data transfer has been completed, the Matchbox unit can either be unplugged and passed onto a friend, or it can be left plugged into the Enigma where another load or save can be performed.

If problems are experienced when loading or saving to the memory unit, pressing the "<" key aborts the transfer. If for some reason problems still exist, remove the memory unit and re-boot the Mini-Enigma unit by switching off and then switching back on.

Be aware that sometimes the first bit (bit 7) of the first character transferred becomes corrupted (i.e. it is made high instead of low), the software in the Enigma clears bit 7 of all characters before it shows them on the l.c.d. to eliminate this problem.

An encrypted message from the Matchbox unit (top and its decoded meaning (lower).



The logic flow chart for using Mini-Enigma.

A late model of the Enigma, circa 1947.

ACKNOWLEDGEMENTS

John Becker, *PIC Tutorial* series March to May '98. The author says he did not start reading the *Tutorial* until Dec '00, but by Feb '01 he had written the basics of the code for this project.

Simon Singh, *The Codebook*, published by The 4th Estate, which gives excellent descriptions of many different encryption techniques and includes the history of the original Enigma unit.

Jack Chisnall, the author's late Grandfather who bought him his first copy of *Everyday Electronics* in the mid 1970's.

www.epemag.com