KEELOQ®
Programming Systems

USER'S GUIDE

KEELOQ® Programming System User's Guide

KEELOQ PROGRAMMING SYSTEM USER'S GUIDE

KEELOQ PROGRAMMING SYSTEM USER'S GUIDE

Table of Contents

KEELOQ PROGRAMMING SYSTEM USER'S GUIDE

Chapter 1. KEELOQ® Code Hopping

Introduction

The KEELOQ programming system programs the KEELOQ range of encoders. The programming system is intended for customers who require volume programming and high security in the factory environment. The hardware is intended for use with an IBM® compatible computer, and consists of a standard PC bus card, a smart card reader, a smart card, an internal hardware probe and controlling software.

System Requirements

The KEELOQ programming system software is intended for use on an IBM compatible computer running under the MS-DOS® operating system. The software does not function properly in a DOS™ box under Windows NT®. The software does function properly in either a Windows® or Windows 95® DOS box.

Key Generation

The key generation algorithm generates keys for transmitters, based on the serial numbers allocated to those transmitters and on the manufacturer's code. The generated keys are programmed into the transmitters, along with serial numbers, the transmitter configuration and synchronization information.

Manufacturers can choose their own manufacturer’s key. A manufacturer’s key is 64 bits in length and should be chosen so that no obvious patterns exist in the number. Combinations to be avoided include successive identical digits or repeating patterns, ascending or descending sequences (e.g. 12345 or 54321), and numbers associated with the company (i.e. telephone or registration numbers). Separate manufacturer's codes can be used for separate product lines. However, compatibility between transmitters from one product line and receivers from another will be sacrificed.

The integrity of the manufacturer's code must be well protected. When learning schemes that derive the key from the serial number are used, an outside party with the manufacturer's code may be able to make transmitters that can be learned on that manufacturer's security systems.

To enable the manufacturer to protect the key with a minimum of effort, a smart card-based security system has been implemented. In the smart card, the manufacturer's code is stored in encrypted form, along with a PIN (Personal Identification Number) and a PIK (Primary Issuer Key). A program is supplied to enable the manufacturer to personalize the smart cards for the system, including the assignment of the PIN and the PIK for each smart card.

The programming hardware alternatively includes provision for internal authentication, effectively taking over the functions of the smart card and dispensing with the need for a smart card reader. Although this arrangement is more convenient than external smart cards, the additional level of security introduced by the use of a smart card in safe-keeping is lost. The manufacturer should tailor the in-house security arrangements according to the perceived threat and the need to protect the manufacturer's code. If smart cards are to be used, each manufacturing station requires a separate smart card, and cards from different programming stations are not interchangeable.

A smart card can only be personalized once. Once the PIK and PIN have been chosen, they can never be changed. The manufacturer's code is also stored on the smart card, but can be altered as often as required. If there is a need to change either the PIK or the PIN, the smart card has to be replaced.

The internal authentication system, on the other hand, can be reconfigured as often as required. The only condition is that the existing PIK must be available whenever such a change is made.

Both the valid smart card (if used) and the PIN are required to start the system at the commencement of each programming session. After start-up, the smart card can be returned to secure storage. The system will continue to function until power is interrupted to the system, or the operator quits the program.

The PIN should only be known by the shift supervisor or other senior personnel. Ideally, the PIN should be known to one senior staff member, while another staff member should have exclusive access to the smart card. This system reduces the risk of the same person getting access to both the PIN and the smart card. The PIK is used to control access to the smart card, and should only be known to the company's computer system supervisor.

Note: If three successive incorrect attempts at entering the PIN are made, or if the PIK is entered incorrectly, the card is locked. To unlock the card, both the PIN and the PIK are required.

Without the PIN and smart card even the theft of the programming hardware from the production line will not jeopardize the manufacturer's code.

Chapter 2. Installation

Key Generation Module

The key generation module consists of a standard ISA bus card. The card should be installed in a vacant slot in the computer to be used for programming.

If there are no other accessory cards in the computer, the software will search for and find the card regardless of switch settings. However, if the user has other cards in the computer, the address should be set up on jumpers SW1 to SW3 before the card is installed. An unused address should be selected from the table below to ensure that there are no conflicts with existing hardware.

Table 2.1 Selection of Bus Card Base Address

SW3	SW2	SW1	Base Address
In	In	In	100_{16}
In	In	Out	140_{16}
In	Out	In	180_{16}
In	Out	Out	$1C0_{16}$
Out	In	In	200_{16}
Out	In	Out	240_{16}
Out	Out	In	280_{16}
Out	Out	Out	Not allowed

The key generation card has been issued with a unique serial number. This number should be visible on your card.

The smart card reader should also be installed near the computer at this time. The reader is required to conduct the initial setup routine, even if the user elects not to use smart cards during routine operations. To install the reader in a standard disk drive bay, remove its metal cover.

Probe

The probe hardware consists of a probe interface card, a ribbon cable and a probe cable. The interface card needs to be plugged into an open slot in the production PC. The probe interface card connects to the Key Generation module in connector marked J1 using the ribbon cable supplied.

The probe cable is plugged into the DB9 male connector on the interface card. The probe head has four spring loaded pins. A table detailing the DB9 pinout can be found at the end of the document.

Status and control lines are provided to simplify the automation of the programming process. These will be described in the next section.

Footswitch (Optional)

A footswitch (not included) or other external input device is recommended for hands-free manual programming. A keyboard is too fragile for the typical production line, and leaves only one hand free to program the PC board. If a footswitch is used, both hands are available for stabilizing the board and for holding the probe. External input is also required in the case of automated programming processes. The external input device should be connected between line 1 (Footswitch Input) and line 4 (Ground) of the DB-9 male connector. (Chapter 5 describes all the probe interface card's DB9 pinouts.)

Lines 3 and 8 are status lines giving information about the programming process. These lines can be used in conjunction with the footswitch input (line 1) to automate the programming process. If programming has been successful, pin 3 will be asserted for 500 ms, while an unsuccessful programming operation is indicated by pin 8 being asserted for a similar period. The outputs can be connected directly to automatic test equipment. Alternatively, a bicolor LED can be installed between these two lines. After successful programming, the LED will turn green. An unsuccessful operation will be indicated by a red indication. There is no need for an additional current limiting resistor as one is provided on the interface board.

Software

The KEELOQ programming system software is intended for use on an IBM compatible computer running under the MS-DOS operating system. The software does not function properly in a DOS box under Windows NT. The software does function properly in either a Windows or Windows 95 DOS box.

The software is supplied on a disk not in compressed format, and can be copied directly to the hard disk directory where it will be used. For example, if a directory named *KEELOQ* needs to be created on disk C, and the disk supplied is in drive B, the procedure is as follows:

```
c:
cd\
md keeloq
cd keeloq
copy b:.
```

The files occupy about 1313 kilobytes of space on the hard disk. If sufficient space is available, all the files will be copied into the *KEELOQ* directory.

Using Multiple Configuration Files

The configuration file will always be stored in the **current** directory. If the programming software is run from a different directory, a new configuration file may have to be set up. Several configuration files can then exist in different directories on the hard disk. This situation provides flexibility for manufacturers with different product ranges.

Note: This can be dangerous if not managed properly.

It is suggested that a batch file should be created to run the programming software. This batch file should be in a directory which is included in the *path* environment variable in DOS. An example of such a batch file would be:

```
c:
cd\prod1
\keeloq\txrxprgm
```

The transmitter programming software in the KEELOQ directory will be started when the batch file is executed, and the configuration file in *c:**prod1* will always be used.

If the user intends to use a floppy disk during manufacturing, a user copy of the distribution disk should be made as the distribution disk should be stored for backup purposes.

Several computers can be used simultaneously for manufacture. However, separate key generation hardware modules and smart card readers will be required. In addition, the user will have to pay attention to proper serial number management. Ideally, serial numbers should not be duplicated on different production runs. The 28-bit serial number length provides for 456 million serial numbers before duplication becomes necessary.

It is recommended that the user should make backups of the configuration file after every programming session. Failing to do this may cause the user to lose track of the last serial number programmed if the hard disk fails.

Smart Card Initialization

The system is supplied with two blank smart cards. During the installation, the smart card must be initialized. A program is supplied for this purpose. The filename for this program is sc_init.exe, and it can be started by typing sc_init while in the relevant directory (*c:\keeloq* in the example). The smart card must be initialized, even if the manufacturer decides not to use the smart card for access control. The initial setup session cannot be started without the smart card.

If the user elects not to use the smart card for routine operation, the internal authentication device must be set up separately, as described in the last part of this section. However, the smart card initialization described below is still required, as initial access to the configuration software is controlled by the smart card.

On start-up, the smart card is checked. If the card has been personalized before, the system issues a warning and aborts the personalization procedure.

The user is then prompted for a PIK of up to 11 characters. All considerations regarding allowed characters and choices of a PIK are the same as those for a PIN, except that the length limitation is 11 rather than 6 characters. Rules for the composition of a PIN are discussed in the following paragraph.

A PIN of up to six characters must then be entered. All alphabetic characters (*a* to *z* and *A* to *Z*), numeric characters (*0* to *9*) and three special characters ("-", "." and a space) are allowed. The PIN is not case sensitive (i.e. *Pass-1*, *PASS-1* and *pass-1* are all the same PIN). The PIN should not be chosen in an obvious way. Names and real words are not to be used. A distortion of a real word is both easy to remember and difficult to guess. Examples (generated by a password generation program) are *descow*, *ebuibi*, *osceti*, *keisdu* and *enisca*. **Do not use these examples!**

The program is terminated after displaying the outcome of the operation (successful or otherwise) and asking whether another smart card needs to be personalized.

If the manufacturer elects not to use the smart card routinely, the program ad_init.exe should be used to set up the internal authentication device.

When the program is started by typing ad_init on the command line, the program will check whether the system has been used before. If it has, the user will be asked to enter the existing PIK before being given access to the program.

The user is then prompted for a new PIK and PIN. The rules governing the choice of PIK and PIN are identical to those described above for the smart card. The PIK and PIN are stored in EEPROM on the programming board. They are stored in encrypted form to prevent access from outside.

When the internal authentication device is reinitialized, the manufacturer's code is cleared. All programs will report errors when trying to read the key from EEPROM. The configuration software must be run again to redefine the key.

Important: A specific smart card can only be used with that key generation module which was used when the manufacturers code was written into the smart card.

KEELOQ PROGRAMMING SYSTEM USER'S GUIDE

Chapter 3. Configuration Software

The configuration program (setup.exe) allows the user to configure the programming system for the products the user is using. The software allows the user to:

- Test the programming system hardware
- Select the access control method (with or without a smart card)
- Select the system encoder
- Select the system decoder
- Change the encoder setup
- Change the decoder setup (key generation type, number of transmitters per decoder etc.)
- Select, read or change the manufacturer's code
- Select the serial number range to be programmed

Options are stored in a file in the current directory on the hard disk. The manufacturer's key, along with the PIN and the PIK, is stored in encrypted form on the smart card (or in on-board EEPROM if internal authentication is used). These keys cannot be accessed from outside.

The configuration software is started by executing *setup.exe*. The user is prompted to insert the smart card and enter the PIN. The PIN is not displayed on the screen as it is entered, but asterisks will appear in the input field to provide feedback on valid keystrokes. If an incorrect PIN is entered, the user will be prompted to try again. If three successive incorrect attempts are made, access to the smart card is denied. The smart card can only be unlocked by a user with the PIK. After the third attempt, the user will be prompted to enter the PIK. Once the PIK has been successfully entered, the user is prompted to enter the PIN. Access will then again be granted.

If a valid configuration file does not exist in the current directory, the program will use default values and issue a warning to that effect.

The opening menu lists all the possible operations available. On the lower portion of the screen, the current values of all the parameters are shown. Any of these parameters can be changed by making appropriate choices from the main menu.

The available choices are discussed below.

Hardware Test

Hardware test is used to test the key generation system. The smart card must be in the reader during this test. The smart card, the key generator IC, the encryption IC and the key generation card are all tested, and the results are displayed on the screen. The serial number and firmware version of the key generation card is also displayed.

System Options

Selecting system options from the main menu allows the user to set-up the encoder/decoder system that he is going to be using. The most important part of this setup is the selection of the encoder / decoder pair that make up the system. The user can select between

- Manufacturer's Code
- Encoder Type
- Encoder Configuration
- Decoder Type
- Decoder Configuration

Encoder Type

The user can select among five KEELOQ encoders currently available. These include the HCS200, HCS300/1, HCS360, and HCS361. There is also a USER encoder type if a more advanced setup is required.

Decoder Type

The user can select among the KEELOQ decoders that are currently available. These include the three Microchip software decoders (Normal, Secure and Simple decoders), and the firmware devices (HCS500, HCS509 and HCS512). The programming system has been changed to simplify the process of setting up encoder and decoder pairs.

KEELOQ key generation can be summarized as three main parts. A source, manufacturer's code and an algorithm as shown in Figure 3.1. The decoders, that the programming station is able to support, use different key generation methods.

Table 3.9 summarizes the key generation algorithms supported by the various decoders and lists the encoders that can be supported using each decoder/ key generation algorithm.

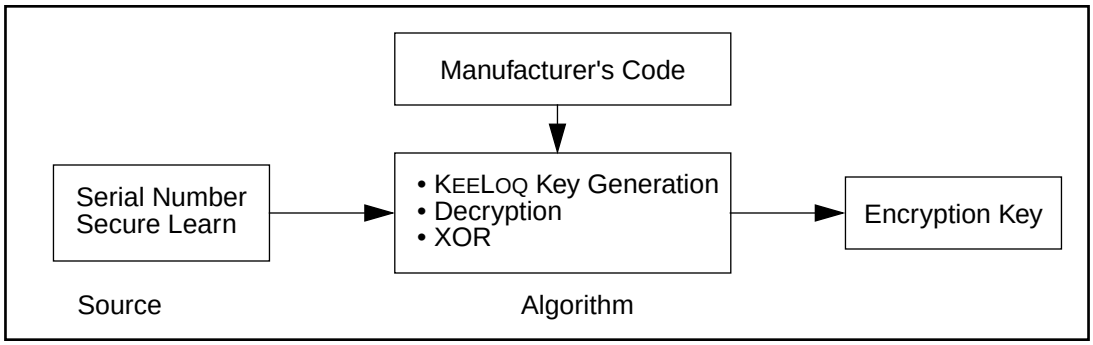

Figure 3.1 Generation

Configure Encoder

The configuration of the chosen encoder can be changed using this option. Please refer to the relevant data sheets for an explanation of the available options. The encoder options available are given in the tables below.

Table 3.1 HCS200 Options

Option	Description
Transmission Baud Rate :	Selects basic pulse width of the transmitted data.
400us, All	Basic pulse width of 400 μs and all code words transmitted.
200us, 1 of 2	Basic pulse width of 200 μs and 1 in 2 code words transmitted.
Low Voltage Trip Point :	Selects the voltage at which the VLOW bit is set in a transmission.
Low	Approximately 3.8V.
High	Approximately 8.4V.

Table 3.2 HCS300 Options

Option	Description
Transmission Baud Rate	Selects the basic pulse width and blanking options of the transmitted data.
400us, All	Basic pulse width of 400 μs and all code words transmitted.
200us, 1 of 2	Basic pulse width of 200 μs and 1 in 2 code words transmitted.
100us, 1 of 2	Basic pulse width of 100 μs and 1 in 2 code words transmitted.
100us, 1 of 4	Basic pulse width of 100 μs and 1 in 4 code words transmitted.
Low Voltage Trip Point	Selects the voltage at which the VLOW bit is set in a transmission.
Low	Approximately 2.0V.
High	Approximately 3.8V.
Counter Overflow	Selects how many times the counter can overflow before all the overflow bits are cleared.
None	Both overflow bits are cleared.
Once	One overflow bit is set.
Twice	Both overflow bits are set.
Auto-shutoff Timer	The auto-shutoff timer stops the encoder transmitting after about 25 seconds if the encoder is inadvertently activated in a purse or pocket, preventing the battery from going flat.
Disabled	
Enabled	

Table 3.3 HCS360 Options

Option	Description
Code Word Blanking	Selects whether alternate code words are transmitted or not.
Disabled	All code words are transmitted
Enabled	Every other code word is transmitted
Transmission Speed	Selects the basic pulse width of the encoder
400us	Basic pulse width of 400 µs.
200us long	Basic pulse width of 200 µs, long time-out (approximately 25 s) if time-out is enabled, long delay till delayed mode activated (approximately 3 s) if delayed mode is enabled.
200us short	Basic pulse width of 200 µs, short time-out (approximately 15 s) if time-out is enabled, short delayed mode (approximately 1.5 s) if delayed mode is enabled.
100us	Basic pulse width of 100 µs.
Delay Mode	Selects whether delayed transmissions are possible or not.
Disabled	
Enabled	
Encoder Time Out	The auto-shutoff timer stops the encoder transmitting after about 25 seconds if the encoder is inadvertently activated in a purse or pocket, preventing the battery from going flat.
Disabled	
Enabled	
Counter Overflow	Selects whether the counter overflow bit is set or cleared.
Disabled	
Enabled	

Table 3.4 HCS361 Options

Option	Description
Code Word Blanking	Selects whether alternate code words are transmitted or not.
Disabled	All code words are transmitted
Enabled	Every other code word is transmitted
Transmission Speed	Selects the basic pulse width of the encoder
Slow	400 µs if 1/3, 2/3 transmission format selected, otherwise 200 µs.
Fast	200 µs if 1/3, 2/3 transmission format selected, otherwise 100 µs.
Transmission Format	Selects between a one-third/two-thirds transmission format and a one-sixth/two-sixths transmission format.
1/3, 2/3 1/6, 2/6	
Sync Pulse Modulation	Selects whether the high part the synchronization pulse is modulated.
Disabled	
Enabled	
Delay Mode	Selects whether delayed transmissions are possible or not.
Disabled	
Enabled	
Encoder Time-out	The auto shut-off timer stops the encoder transmitting after about 25 seconds if the encoder is inadvertently activated in a purse of pocket, preventing the battery from going flat.
Disabled	
Enabled	
Counter Overflow	Selects whether the counter overflow bit is set or cleared.
Disabled	
Enabled	

Configure Decoder

The decoders, that the programming station is able to support, use different key generation methods. The production software supports the following KEELOQ decoders:

- MCHIP Normal (Software decoder of ANGxx)
- MCHIP Secure (Software decoder of ANGxx)
- MCHIP Simple (Software decoder of ANGxx)
- HCS500
- HCS509
- HCS512

Note: The MCHIP Normal and MCHIP Simple decoders do not have any selectable options that need to be set up.

Table 3.5 MCHIP Secure

Option	Description
Algorithm Used:	Select which learn algorithm must be used to calculate the encoder's encryption key.
Decryption	The KEELOQ Decryption Algorithm Selected
XOR	The Fix Code XOR Algorithm Selected

Table 3.6 HCS500

Option	Description
Secure Learn:	Enable secure learn on the HCS512 decoder
Yes	Secure Learn Enabled
No	Normal Serial Number Learn Enabled
Algorithm Used:	Select which learn algorithm must be used to calculate the encoder's encryption key. This option is only relevant if secure learn is selected.
Decryption	The KEELOQ Decryption Algorithm Selected
XOR	The Fix Code XOR algorithm Selected

Table 3.6 HCS500 (Continued)

Option	Description
Repeated Transmissions:	Enabling the acceptance of repeated transmissions on the HCS500 decoder. This option should be disabled in stand-alone applications
Enabled	Repeated transmission ignored by HCS500
Disabled	Repeated transmission ignored by HCS500

Table 3.7 HCS509

Option	Description
First Learn Position:	This select which will be the first learn position in the HCS509 decoder.
Master, User #1, User #2, User #3, Learn position User #4, User #5, User #6	Learn position
First Programming position:	Indicate for the encoder/decoder programming software where to program the first transmitter into.
Master, User #1, User #2, User #3, User #4, User #5, User #6	Learn position
Number of Transmitters:	Indicate the number of transmitters that will be programmed into the decoder during production.
1 to 6	Number of preprogrammed transmitters
Test Transmitter:	Indicates if the test transmitter must be programmed into the HCS509 decoder.
Yes	Test transmitter programmed into decoder during production.
No	No test transmitter programmed into the decoder during production

Table 3.8 HCS512

Option	Description
Secure Learn	Enable secure learn on the HCS512 decoder
Yes	Secure Learn Enabled
No	Normal Serial Number Learn Enabled
Algorithm Used	Select which learn algorithm must be used to calculate the encoder's encryption key. This option is only relevant if secure learn is selected.
Decryption	The KEELOQ Decryption Algorithm Selected
XOR	The Fix Code XOR Algorithm Selected
SLEEP	Enable SLEEP mode on the HCS512 decoder

The decoders, that the programming station is able to support, use different key generation methods. the following table summarizes the supported learn methods.

Table 3.9 Supported Decoder Learn Methods

Decoder Supported	Encoders Supported	Algorithm Supported	Sources Supported
MCHIP Normal	All HCSxxx	Decryption	28 Bit Serial Number
MCHIP Secure	All HCSxxx	Decryption XOR	Seed Transmission
MCHIP Simple	All HCSxxx	None	Fixed Key
HCS500	All HCSxxx	Decryption XOR	28 Bit Serial Number Seed Transmission
HCS509	All HCSxxx	Keygen	24 Bit Serial Number
HCS512	All HCSxxx	Decryption XOR	28 Bit Serial Number Seed Transmission

SQTP Options

Table 3.10 SQTP

Option	Description
SQTP Prod:	Enabling of SQTP Production. For more detail read the SQTP Users Guide.
Enabled	System locked for SQTP Production
Disabled	System not locked for SQTP Production
Serial NumberType:	Select which index to serial number mapping must be used.
Index Number	Sequential serial numbers equal to the current index number
Non-Sequential Serial	Non-sequential serial numbers derived from the current serial number.
Fixed Serial	User defined serial number.
Fixed Serial Number:	User entry of the fixed serial number to be used when the serial type is fixed serial.
Decimal User Input Field	

Index Number Range

Index number range selects the range of index numbers to be used during programming. The range needs to be specified between 1 and 268,435,455 (HCS200, HCS300, HCS360 and HCS361). If the advance user defined encoder is used and extended serial numbers option is enabled (HCS360 and HCS361), the range must be between 1 and 4,294,967,296. The index number is mapped to the actual serial number by one of the following methods which must be setup as part of the SQPT settings.

- Serial number = Index Number (Sequential serial numbers)
- Serial number = Non-sequential number that is derived from the index number
- Serial number = Fixed Number (Serial number the same for all encoders)

Manufacturer’s Code

Manufacturer's code enables change or inspection of the manufacturer's code. Access to this option is controlled, and the user will be prompted for the PIK. The smart card must be inserted while this option is being used. The code is specified as a sixteen digit hexadecimal number. A symbolic name of up to 19 characters (including spaces) can be assigned to a specific code. This name will be displayed on the screen whenever the code is being used. However, the option of having separate codes for separate product lines may be useful later. For example, a specific product range might have a manufacturer's code named *Access Control 1*. A different product range might have a code named *Garage door 3*. Each code will consist of a 16-digit hexadecimal number (64 bits). The relevant code name will be displayed on the screen during programming.

Recommendations on selecting a suitable manufacturer's code can be found in Section 1 (Introduction) of this document.

The user will be given the option of displaying the existing manufacturer's code, or of entering a new manufacturer's code. In either case, the user will be prompted for the PIK, which must be entered correctly.

Codes should be entered as a single string of valid hexadecimal digits. The code will be displayed as two groups of eight digits. If invalid characters (e.g. G, H, I, *) are entered, the code will not be accepted.

File

File is used to save the selected configuration to disk. The configuration file is named *setup.cfg*, and is always stored in the **current** directory.

Exit Program

If unsaved changes have been made to the configuration file, the user will be asked whether the updated file should be saved. If the file is not saved, newly selected options may be lost.

Notes:

Chapter 4. Programming Software

Transmitter Programming

Stand-alone transmitter programming is done with *txprgm.exe*. This program will be used when transmitters and decoders are to be programmed on separate production lines, and brought together after programming. The associated receivers (HCS500, HCS509, and HCS512 only) will have to be programmed separately with *rxprgm.exe*.

On start-up, the user is prompted to insert the smart card (if used) and enter the PIN. If the PIN has been correctly entered, the smart card can be removed, and the system can be used normally until the program is terminated, or the system power is lost.

Once access has been granted, a screen with the version number of the software and the current value of all the parameters will be displayed. The values of all the selected parameters are displayed in the lower quarter of the screen and should be checked by the supervisor.

Once the user has entered the program, the manufacturer's key name and the current serial number are both displayed on the screen. The user is prompted to connect the probe and press any key. At this point, the probe should be placed on the transmitter to be programmed, and any keyboard key except *Escape* pressed. Alternatively, if a footswitch is connected, the footswitch can be used to initiate the programming process.

A successful programming process is indicated by a message (*Programmed OK*) on the screen. If any problems are encountered, three shorter beeps will sound, and an error message (*Programming Error*) displayed on the screen. After a successful operation, the serial number is incremented and the configuration file updated.

The program is terminated by pressing the *Escape* key.

Receiver Programming

HCS500, HCS509, and HCS512 receiver programming is done with *rxprgm.exe*. PICmicro™ microcontrollers and EEPROM based decoders (MCHIP) don't require programming since the manufacturers key is securely stored in protected code space. This program will be used when transmitters and decoders are to be programmed on separate production lines, and brought together after programming. The associated transmitters will have to be programmed separately with *txprgm.exe*.

On start-up, the user is prompted to insert the smart card (if used) and enter the PIN. If the PIN has been correctly entered, the smart card can be removed, and the system can be used normally until the program is terminated, or the system power is lost.

Once access has been granted, a screen with the version number of the software and the current value of all the parameters will be displayed. The values of all the selected parameters are displayed in the lower quarter of the screen.

Once the user has entered the program, the manufacturer's key name is displayed on the screen. The user is prompted to connect the probe and press any key. At this point, the probe should be placed on the receiver to be programmed, and any keyboard key except *Escape* pressed. Alternatively, if a footswitch is connected, the footswitch can be used to initiate the programming process.

A successful programming process is indicated by a message (*Programmed OK*) on the screen. If any problems are encountered, three shorter beeps will sound, and an error message (*Programming Error*) displayed on the screen. After a successful operation, the configuration file is updated.

The program is terminated by pressing the *Escape* key.

Note: Before attempting to program HCS500, HCS509 or HCS512 decoders the decoder should be powered up with it's clock running.

Chapter 5. Probe Connections

Probe Interface DB9 Connections

Table 5.1 DB9 Pin Labeling

DB9 Pin Number	Pin Name	Probe Cable Mnemonic
1	Footswitch Input	
2	Not used	
3	OK/LED Green	
4	Ground	GND
5	Probe Power	V_{DD}
6	Not used	
7	Clock	CLK
8	Error/LED Red	
9	Probe Data	DATA

The connection between the probe and the various encoders look as follows:

Table 5.2 HCS200/HCS300/HCS360 Probe (4-pin, 4-wire Probe)

Probe Pin	Description	HCS200 Pin	HCS300 Pin	HCS360 Pin
1	GND	5	5	5
2	V_{DD}	8	8	8
3	CLK	3	4	4
4	DATA	6	6	6

Table 5.3 HCS509/HCS512 Probe (4-pin, 4-wire Probe)

Probe Pin	Description	HCS509 Pin	HCS512 Pin
1	GND	5	5
2	$\overline{MCLR}$	4	4
3	CLK	12	12
4	DATA	13	13

Notes:

Glossary

Term	Description
Auto-shutoff Timer	The auto-shutoff timer allows the encoder to stop transmitting if the transmitter is accidentally pressed in a purse or pocket. This prevents the battery going flat.
Code Word Blanking	The encoders can be set such that every alternate word is not transmitted. That lowers the duty cycle of the transmitter and allows more power to be transmitted per transmitted word and still stay within FCC limits.
Delayed Mode	The HCS360, HCS361 and NTQ106 transmitters have a delayed mode. The transmitted word is changed if the transmitter is activated for more than approximately three seconds. This can be used to activate a panic function for example.
Encoder Time-out	See ‘Auto-shutoff’.
Low Voltage Trip Point	The HCS encoders have a bit in the transmission which is set when the supply voltage drops below a set voltage.
Manufacturer’s code	A 64-bit word unique to each manufacturer. The manufacturer’s code is used produce a unique secret encryption key in each encoder.
PIK	Primary Issuer’s Key—11-character long key used to allow the manufacturer’s key to be written or changed.
PIN	Personal Identification Number—6-character long key used to allow the programming station to read the manufacturer’s key before programming begins.
Smart Card	A smart card is a memory card with access control features used to securely store the manufacturer’s key.

Term	Description
Serial Number	28-bit number transmitted unique to each encoder. The serial number is transmitted unencrypted each time the encoder is activated. The serial number identifies the encoder to the decoder.
Sync Pulse Modulation	When using PWM.
Transmission Baud Rate	A KEELOQ transmission is pulse width modulated. Each data bit consists of three sections, each T_E ms long. Changing the baud rate changes the length of T_E and hence the length of the transmission.

WORLDWIDE SALES & SERVICE

AMERICAS

Corporate Office
Microchip Technology Inc.
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 602-786-7200 Fax: 602-786-7277
Technical Support: 602 786-7627
Web: http://www.microchip.com

Atlanta
Microchip Technology Inc.
500 Sugar Mill Road, Suite 200B
Atlanta, GA 30350
Tel: 770-640-0034 Fax: 770-640-0307

Boston
Microchip Technology Inc.
5 Mount Royal Avenue
Marlborough, MA 01752
Tel: 508-480-9990 Fax: 508-480-8575

Chicago
Microchip Technology Inc.
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 630-285-0071 Fax: 630-285-0075

Dallas
Microchip Technology Inc.
14651 Dallas Parkway, Suite 816
Dallas, TX 75240-8809
Tel: 972-991-7177 Fax: 972-991-8588

Dayton
Microchip Technology Inc.
Two Prestige Place, Suite 150
Miamisburg, OH 45342
Tel: 937-291-1654 Fax: 937-291-9175

Los Angeles
Microchip Technology Inc.
18201 Von Karman, Suite 1090
Irvine, CA 92612
Tel: 714-263-1888 Fax: 714-263-1338

New York
Microchip Technology Inc.
150 Motor Parkway, Suite 416
Hauppauge, NY 11788
Tel: 516-273-5305 Fax: 516-273-5335

San Jose
Microchip Technology Inc.
2107 North First Street, Suite 590
San Jose, CA 95131
Tel: 408-436-7950 Fax: 408-436-7955

Toronto
Microchip Technology Inc.
5925 Airport Road, Suite 200
Mississauga, Ontario L4V 1W1, Canada
Tel: 905-405-6279 Fax: 905-405-6253

ASIA/PACIFIC

Hong Kong
Microchip Asia Pacific
RM 3801B, Tower Two
Metroplaza
223 Hing Fong Road
Kwai Fong, N.T., Hong Kong
Tel: 852-2-401-1200 Fax: 852-2-401-3431

India
Microchip Technology Inc.
India Liaison Office
No. 6, Legacy, Convent Road
Bangalore 560 025, India
Tel: 91-80-229-4036 Fax: 91-80-559-9840

Korea
Microchip Technology Korea
168-1, Youngbo Bldg. 3 Floor
Samsung-Dong, Kangnam-Ku
Seoul, Korea
Tel: 82-2-554-7200 Fax: 82-2-558-5934

Shanghai
Microchip Technology
RM 406 Shanghai Golden Bridge Bldg.
2077 Yan'an Road West, Hong Qiao District
Shanghai, PRC 200335
Tel: 86-21-6275-5700
Fax: 86 21-6275-5060

Singapore
Microchip Technology Taiwan
Singapore Branch
200 Middle Road
#10-03 Prime Centre
Singapore 188980
Tel: 65-334-8870 Fax: 65-334-8850

Taiwan, R.O.C
Microchip Technology Taiwan
10F-1C 207
Tung Hua North Road
Taipei, Taiwan, ROC
Tel: 886 2-717-7175 Fax: 886-2-545-0139

EUROPE

United Kingdom
Arizona Microchip Technology Ltd.
Unit 6, The Courtyard
Meadow Bank, Furlong Road
Bourne End, Buckinghamshire SL8 5AJ
Tel: 44-1628-851077 Fax: 44-1628-850259

France
Arizona Microchip Technology SARL
Zone Industrielle de la Bonde
2 Rue du Buisson aux Fraises
91300 Massy, France
Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79

Germany
Arizona Microchip Technology GmbH
Gustav-Heinemann-Ring 125
D-81739 Müchen, Germany
Tel: 49-89-627-144 0 Fax: 49-89-627-144-44

Italy
Arizona Microchip Technology SRL
Centro Direzionale Colleoni
Palazzo Taurus 1 V. Le Colleoni 1
20041 Agrate Brianza
Milan, Italy
Tel: 39-39-6899939 Fax: 39-39-6899883

JAPAN

Microchip Technology Intl. Inc.
Benex S-1 6F
3-18-20, Shinyokohama
Kohoku-Ku, Yokohama-shi
Kanagawa 222 Japan
Tel: 81-45-471- 6166 Fax: 81-45-471-6122

7/29/97

MICROCHIP