SIMREX Corporation

SIMCRYPT

Instruction Manual

Standalone Encryption Device for RS-232 Serial Data

Firmware Release 5.1

SIMREX MAN.SIMCRYPT, Rev 2.0
DECEMBER 2005

SIMREX Corporation
Your Trusted Wireless Solution Provider
www.simrex.com

Introduction

The SIMREX Corporation SimCrypt module is a standalone encryption device that can be used to secure asynchronous serial data used by any device that communicates using an RS-232 serial port. Even if a message is intercepted, the high encryption strength of AES 256 virtually guarantees that it will be unusable to anyone but the intended recipient.

Features

- 1200 bps to 57.6kbps operation
- Supports true full-duplex up to 19,200 baud
- 128 bit and 256 bit AES Encryption
- Block or Streaming encryption modes
- Conforms to ModBus timing requirements
- User configurable encryption key
- Password protected user interface
- Bypass mode for live system cutover
- Low current draw – less than 50 mA @ 12 VDC

A SimCrypt device is required at each end of a link for secure communications to take place. Each unit must have the identical encryption key.

SimCrypt encryption units may be added to an existing system without service interruption or integrated outright as part of a new system. In a new system, the SimCrypt units would be configured in encrypted mode at the time of install.

If upgrading an existing live system to encryption using SimCrypt, it may take time to install many field units. The mode at installation in this case should be PassThrough Mode. PassThrough Mode will pass all data through Simcrypt unchanged (unencrypted) so that both nodes with and without installed SimCrypt units will operate normally. When all the SimCrypt units have been installed, a command can be broadcast from the base unit's SimCrypt configuration menu that will simultaneously turn on the encryption in all units in the field.

Installation

The ‘PWR’ LED is on whenever the unit is powered.
The ‘ENC’ LED flashes when data is being encrypted.
The ‘DEC’ LED flashes when data is being decrypted.

Installation of the SimCrypt device is straight forward.

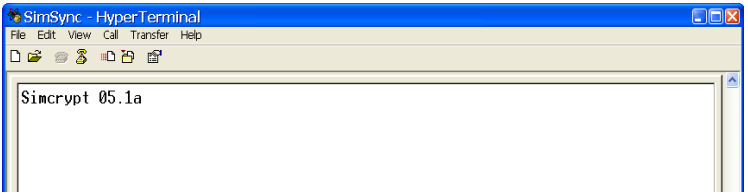
1. Unplug both ends of the serial cable that is currently carrying data from your serial device (RTU/PLC/HOST) to the DCE (radio) port.

2. Connect the port on the SimCrypt labeled ‘Encrypted’ to the DCE (radio) port.

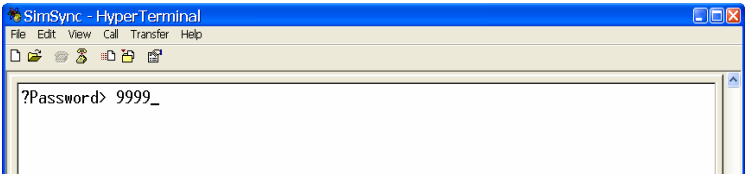
3. Re-connect your serial data device to the SimCrypt ‘Plain Data’ port.

4. Apply DC power to the SimCrypt unit.

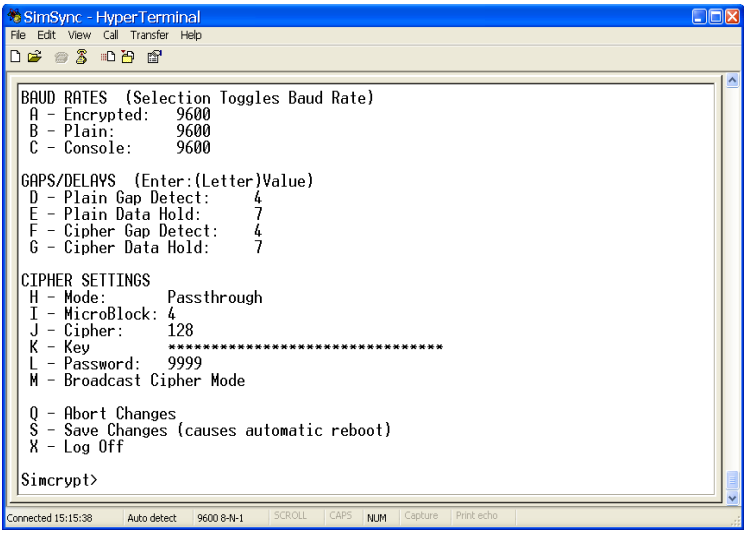
With terminal program connected via serial cable to the CONFIG port set to 9600, 8, N, 1, the first thing shown on the terminal screen is the version of firmware loaded into the unit.



Press ‘Enter’ to bring up the password prompt. The factory default password is **9999**. Type that in and press ‘Enter’ to show the main menu. Remember to change your password using the “L” command. If your password is lost or forgotten, a re-flash of the unit is needed to reset the password.



This is the main menu that is shown when the password is entered correctly.



BAUD RATES

Valid baud rates usable on the 'Plain' and 'Encrypted' serial ports for guaranteed full-duplex gapless performance are 1200, 2400, 4800, 9600, and 19200 baud. Note that flow control is not implemented on these ports currently. Because of this, 38400 and 57600 baud can only be used to send small messages, up to 256 bytes. In contrast, a continuous data stream can be sent at up to 19200 baud in true full-duplex mode provided all baud rates across the system are set to the same rate.

To change a baud rate, simply enter the letter choice, and press 'Enter'. This will toggle the baud rate to the next highest supported rate. When it reaches 57600, the next toggle will reset it to 1200 baud.

GAPS/DELAYS

The Gap Detect and Data Hold settings help to assure that serial data remains gap free if you are dealing with equipment that expects gap free data, like Modbus-RTU. The Gap detect parameters are used to force transmission of partially filled encryption blocks (EVEN IN STREAMING MODE). The delay parameters are used to ensure seamless data delivery due to gaps caused by the Gap Detect process..

Note: These parameters will most likely not need to be changed for baud rates up to and including 19200. These parameters will result in less than 30 ms end to end latency at 9600 bps and higher data rates. The above parameters are explained below.

D – Plain Gap Detect

This parameter sets the number of ms that the encryption routine will wait for additional Plain text bytes to fill a block or microblock of data that is being prepared for encryption. When the Gap Detect timer has expired due to a lack of further Plain Text data, the remaining bytes in the process buffer are encrypted and sent. Note that even in streaming mode, it is possible to gain some processor efficiency by using larger microblocks. This parameter has been defaulted to 4 ms to reflect that we are looking for a gap larger than the 3.5 character maximum gap that MODBUS data allows at 9600 bps. If system latency is paramount and it is known that intercharacter gaps do not exist in the user data, this parameter may be reduced. This parameter only introduces latency in the case that a block or microblock are partially filled and there is no further data. To compensate for the potential gap in the cipher text caused by this parmeter, the Cipher Data Hold parameter is used.

G – Cipher Data Hold

The 'Cipher Data Hold' is used to maintain a seamless mode of operation without intercharacter gaps in cipher data packets. The Cipher Data Hold process delays (in ms) the first part of and encrypted data message from being sent out the 'Encrypted Data' port. When a new user message begins, the first encrypted block or microblock of data is put into a delay buffer to be held for Cipher Data Hold delay time. After the delay time expires, the cipher data is released to the cipher port at the prescribed port speed. As long as this delay buffer does not empty out, none of the succeeding cipher data is delayed. If the buffer empties out, the next cipher data packet receives the delay and the process restarts.

By setting a 'Cipher Data Hold' of 7 ms, this will remove the gap (plus some margin of safety for internal process gaps) in data produced by the 4 ms 'Gap Detect' mechanism

described above. Since the amount of data hold is greater than the gap produced, all data packets sent out the 'Encrypted Data' port should now be gapless.

Unfortunately, some latency is produced by this technique. With the default 'Gap/Hold' settings, at 9600 baud with a 4 byte block size, the amount of latency between plain data in and encrypted data out is about 12 ms. At 19,200, this latency is reduced to 7-8 ms.

F – Cipher Gap Detect

This setting is used for the same purpose as the Plain Gap Detect and has the exact same latency effects. The delay is set in ms. The Cipher Gap Detect process also resets the encryption init vector in the case of lost communications or dropped data bytes on the radio channel. This allows full encryption resynchronization by the next user data packet.

For the least amount of end to end latency, it's best to use the smallest numbers that will result in reliable communications.

E – Plain Data Hold

Just as the 'Cipher Data Hold' is used to overcome the gapping effect of the 'Clear Text Gap Detect' and to close gaps in the encrypted data, the 'Plain Data Hold' does the same thing for data being decrypted and sent out of the Plain Data port.

CIPHER SETTINGS

H – Encryption Mode

There are 3 valid 'Mode' settings….'Passthrough', 'Block Mode' and 'Streaming Mode'. To change, enter 'H' and press 'Enter'. This will step to the next mode each time.

> **Block Mode** – Encryption is done using 15 byte blocks. In this mode, an additional housekeeping byte is added to each 15 byte block to make a total of 16 bytes per block that are encrypted. EVERY block that is transmitted is 16 bytes long including the extra byte. At the decryption end, the housekeeping bytes are stripped off.
>
> **Streaming Mode** – Any number of bytes will be sent in each block, between the 'I' value and 16.
>
> **Passthrough** – Encryption is turned off and data is just sent directly through.

I – MicroBlock

This number is only valid if the encryption mode is set to 'Streaming'. This is the maximum number of bytes transmitted in each block. There is no housekeeping byte in this blocking process and larger blocks are more processor efficient. Smaller blocks however have lower latency as a microblock must be filled before the first data is

encrypted/decrypted. A microblock size of 4 at data rates of 9600 bps and above will provide end to end latencies of less than 26 ms. At data rates of less than 9600 bps, microblock sizes of 1 byte are advisable to minimize latency. At data rates of 38.5 and 57kbps, microblock sizes of 8 have been found to be appropriate.

J – Cipher

This is used to set the encryption strength, 128 bit or 256 bit. This is not a valid entry while in 'Passthrough' mode. To toggle between 128 and 256, enter 'J' and press 'Enter'.

K – Encryption Key

This is a 32 character string used for the encryption seed. The valid characters are 0 –> 9 and A –> F, the Hex characters. The alpha characters are NOT case sensitive, a -> f = A -> F.

To change the key enter 'k', then one space, then enter the new 32 hex character key.

M – Broadcast Cipher Mode

This command is used to change the mode of remote SimCrypt units from 'Passthrough' to either 'Block' or 'Streaming' mode. This is a one-time command. Once the remote units have the encryption turned on, you can not remotely turn it off.

For example, in a system that has one Base (or Master) unit and ten Remote (client) units, before enabling encryption,

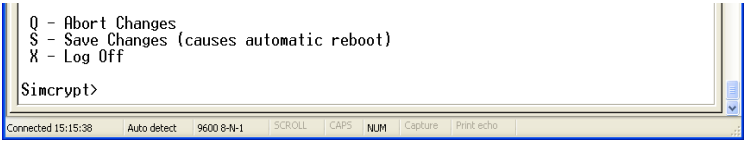
you would set up all eleven encryption units to use ‘Passthrough’ mode and enter a common ‘Key’. This way, the system can be deployed while the network is still operational.

To enable encryption on the system, you would first log into the base unit’s SimCrypt. Set the ‘Mode’, ‘MicroBlock’ size (if applicable), and the ‘Cipher’ strength, 128 or 256 bit to what is desired in the system. ‘Save’ the settings, which causes a unit reboot. After the SimCrypt has re-booted, log back into the console port. Send the ‘Broadcast Cipher Mode’ by simply entering ‘m’, then press ‘Enter’. This sends a command to the remote units telling them to turn on the encryption. Additionally, the ‘Mode’, ‘Cipher’, and ‘MicroBlock’ settings are sent to the remotes and the remote units then configure themselves according to the message information. They then save the setting’s and re-boot themselves.

The Key MUST BE PRE-SET for this to work properly. The command is sent un-encrypted along with the encryption settings. The Key is NOT transmitted.

IT IS RECOMMENDED THAT THERE BE NO OTHER NETWORK TRAFFIC WHEN THIS COMMAND IS ISSUED.

Q – Abort Changes



Any changes previously made to the configuration in this session will be discarded.

S – Save Changes

All changes made will be saved to the non-volatile memory, and a reboot will be issued. When the unit is booted again, the new settings will be in affect.

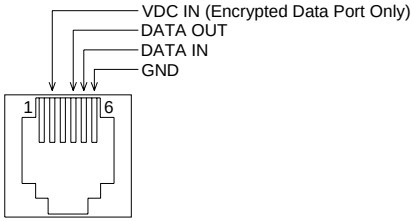
X – Log Off

Any changes previously made to the configuration in this session will be discarded, and the Console screen will return to the Login prompt.

APPENDIX A – Specifications

To Be Added

APPENDIX B – Connector Wiring



(View from front of RJ-11 Connector)

Above is the pin-out for each user connector.

Note that the VDC IN pin is only on the 'Encrypted Data Port'. This can be used to power the SimCrypt directly from an interfaced device, if that device provides accessory power on its RS-232 interface connector. This connector is reverse voltage protected and will tolerate 9 to 30VDC.

There is diode protection inside the SimCrypt to prevent internal DC voltage from appearing on this pin when the rear power connector is used.

IF THE OPTIONAL POWER INPUT PIN IS USED, BE SURE TO NOT APPLY POWER TO THE SIMCRYPT USING THE POWER CONNECTOR ON THE BACK OF THE UNIT.

SIMREX Corporation
5490 Broadway St.
Lancaster, NY 14086
Ph: 716-206-0174 Fax: 716-204-0476
www.simrex.com