COM-1014 TRIPLE DES ENCRYPTION / DECRYPTION

Key Features

- In-line Triple Data Encryption Algorithm (TDEA).
- Can be used as encryption or decryption device.
- Maximum throughput:
  142 Mbit/s (TDEA / EBC mode)
  47 Mbit/s (TDEA / CBC outer code)
- Key length: 192 bit.
- Supports ECB and CBC modes.
- Compliant with FIPS PUB 46-2, 46-3, 81.
- Single 5V supply
- Connectorized 3"x 3" module for ease of prototyping. Standard 40 pin 2mm dual row connectors (left, right, bottom)
- Interfaces with 5V and 3.3V logic.

For the latest data sheet, please refer to the **ComBlock** web site: www.comblock.com/download/com1014.pdf.
These specifications are subject to change without notice.

For an up-to-date list of **ComBlock** modules, please refer to www.comblock.com/product_list.htm .

Electrical Interface

Input Module Interface	Definition
DATA_IN[7:0]	Input data. Format: parallel 8-bit wide or 1-bit serial. MSB is transmitted first. Alternatively contains an initialization vector IV if IV_FLAG is '1'.
SAMPLE_CLK_IN	Input signal sampling clock. One CLK-wide pulse. Read the input signal at the rising edge of CLK when SAMPLE_CLK_IN = '1'. Maximum throughput is one 64-bit block every 18 CLKs (ECB mode) or every 54 CLKs (CBC mode).
SOF_IN	Start of frame input. One CLK-wide pulse. Aligned with SAMPLE_CLK_IN. Indicates the start of a 64-bit wide data block to be encrypted or decrypted. Required in decryption mode. Can be internally generated in encryption mode when not provided at the input interface.
SOC_IN	Start of chain input. One CLK-wide pulse. Aligned with SAMPLE_CLK_IN and SOF_IN. Used in cipher block chaining (CBC) mode to indicate the start of a new chain. Ignored in EBC mode.
IV_FLAG	Input flag indicating whether DATA_IN contains data (0) or the initialization vector IV (1) used for cipher block chaining mode (CBC). Ignored in EBC mode. Once all 64-bit of the initial vector are loaded, the flag should go low. This new

MSS • 18221 Flower Hill Way #A • Gaithersburg, Maryland 20879 • U.S.A.
Telephone: (240) 631-1111 Facsimile: (240) 631-1676 www.ComBlock.com
 Issued 4/1/2003

	initialization vector will be used at the next start of chain. If no IV is loaded prior to a start of chain, the previous IV is used.
SAMPLE_CLK_IN_REQ	Output. One CLK-wide pulse. Requests for input samples to the module upstream. For flow-control purposes.
CLK_IN	Input reference clock for synchronous I/O and processing. Yields internal CLK clock. Typically 40 MHz.
Output Module Interface	**Definition**
DATA_IN[7:0]	Output data. Format: parallel 8-bit wide or 1-bit serial. MSB is transmitted first.
SAMPLE_CLK_OUT	Output sampling clock. One CLK-wide pulse. Read the output signal at the rising edge of CLK when SAMPLE_CLK_OUT = '1'.
SOF_OUT	Start of frame output. One CLK-wide pulse. Aligned with SAMPLE_CLK_OUT. Indicates the start of a 64-bit wide data block.
SOC_OUT	Start of chain output. One CLK-wide pulse. Aligned with SAMPLE_CLK_OUT and SOF_OUT. Used in cipher block chaining (CBC) mode to indicate that a chain has been reset with a new initialization vector IV. Can be ignored in EBC mode.
SAMPLE_CLK_OUT_REQ	Input. One CLK-wide pulse. Requests for output samples from the module downstream. For flow-control purposes.
Power Interface	4.75 – 5.25VDC. Terminal block. Power consumption is approximately proportional to the CLK frequency. The maximum power consumption at 40 MHz is 300mA.

Configuration (via Serial Link / LAN)

Complete assemblies can monitored and controlled centrally over a single serial or LAN connection.

The module configuration parameters are stored in non-volatile memory.

Parameters	**Configuration**
Input format	0 = 1 bit serial 1 = 8-bit byte REG0 bit 1
Output format	0 = 1 bit serial 1 = 8-bit byte REG0 bit 2
Encrypt / Decrypt	0 = encrypt. 1 = decrypt. REG0 bit 3
Mode	0 = ECB. 1 = CBC. REG0 bit 4
Key1	Key for encryption pass 1. 64 bit. REG1 bit 7-0 REG2 bit 15 - 8 REG3 bit 23 - 16 REG4 bit 31 – 24 REG5 bit 39 – 32 REG6 bit 47 – 40 REG7 bit 55 – 48 REG8 bit 63 - 56
Key2	Key for encryption pass 2. 64 bit. REG9 bit 7-0 REG10 bit 15 - 8 REG11 bit 23 - 16 REG12 bit 31 – 24 REG13 bit 39 – 32 REG14 bit 47 – 40 REG15 bit 55 – 48 REG16 bit 63 - 56
Key3	Key for encryption pass 3. 64 bit. REG17 bit 7-0 REG18 bit 15 - 8 REG19 bit 23 - 16 REG20 bit 31 – 24 REG21 bit 39 – 32 REG22 bit 47 – 40 REG23 bit 55 – 48 REG24 bit 63 - 56

Monitoring (via Serial Link / LAN)

Parameters	**Monitoring**
Version	Returns '1014x' when prompted for version number.

Operations

Electronic Codebook (ECB) Mode

The Electronic Codebook (ECB) mode is a basic block cryptographic method which transforms 64-bits of input to 64 bits of output using a 64-bit key. This means that the same plain text block input will produce the same text block output with a fixed key. See NIST FIPS 81 specifications for details.

Cipher Block Chaining (CBC) Mode

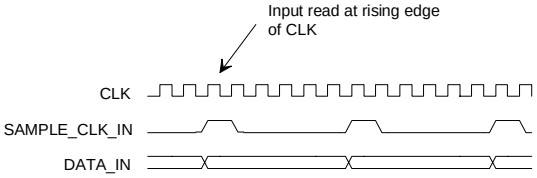
In the Cipher Block Chaining (CBC) mode, data is organized in blocks of N*64 bits, where N is an integer. The first 64-bit data block is xored with an initial vector IV. All subsequent input blocks are xored with the encrypted output of the previous block. See NIST FIPS 81 specifications.

CBC is used as an outer code to the Triple Data Encryption Algorithm.
Because one has to wait for the first block to be fully encrypted before encrypting the following block, this implementation of CBC is about three times slower than the ECB mode.

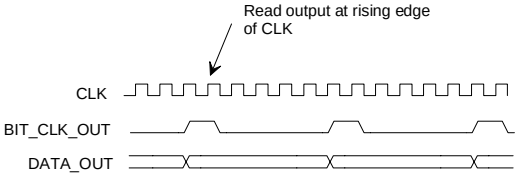
Timing

The I/O signals are synchronous with the rising edge of the reference clock CLK (i.e. all signals transitions always occur after the rising edge of the reference clock CLK). The maximum CLK frequency is 40 MHz.

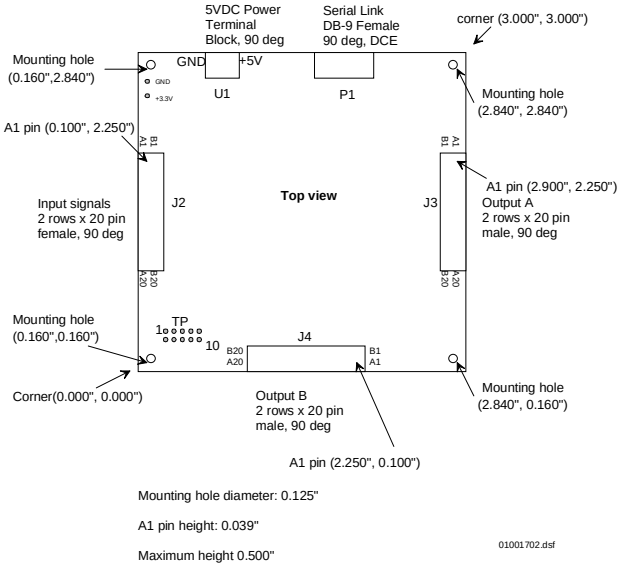
Input



Output



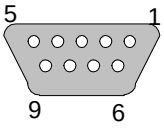
Mechanical Interface



Pinout

Serial Link P1

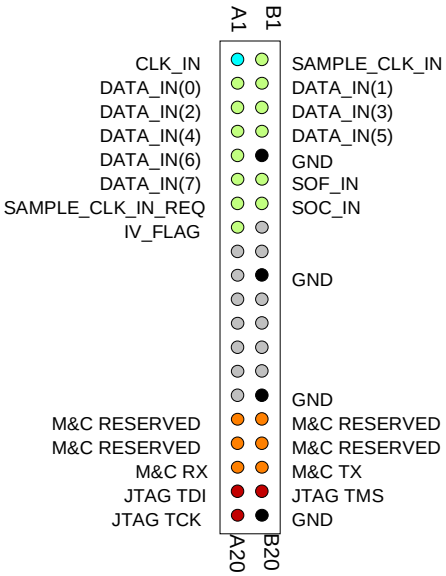
The DB-9 connector is wired as data circuit terminating equipment (DCE). Connection to a PC is over a straight-through cable. No null modem or gender changer is required.



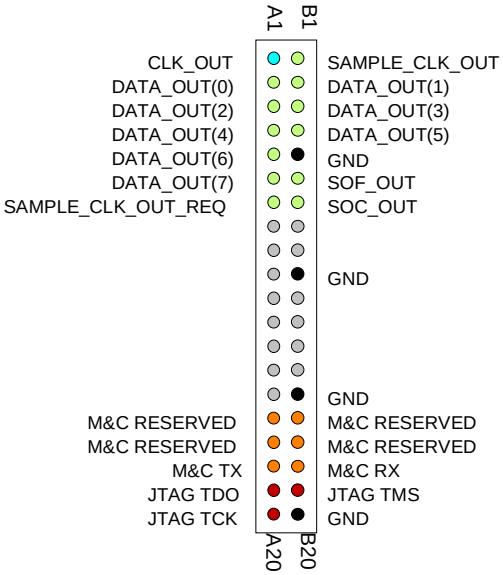
DB-9 Female

2 Transmit
3 Receive
5 Ground

Input Connector J2



Output Connectors J3, J4



I/O Compatibility List

(not an exhaustive list)

Input	Output
COM-1014 Triple DES encoder (back to back mode).	COM-1014 Triple DES encoder (back to back mode).
COM-7001 Turbo Code decoder	COM-7001 Turbo Code encoder

ComBlock Ordering Information

COM-1014 Triple DES Encryption / Decryption..

MSS • 18221 Flower Hill Way #A •
Gaithersburg, Maryland 20879 • U.S.A.
Telephone: (240) 631-1111
Facsimile: (240) 631-1676
E-mail: sales@comblock.com