

APPENDIX (to document PA/81317)

- a) ISO Entry Name To be allocated by NCC - {iso standard 9979 b-crypt (1)}
- b) Proprietary Entry Name B-CRYPT
- c) Intended Range of Applications

- 1. Confidentiality
- 2. Authentication - As detailed in ISO 9798. B-CRYPT may be used as a non-reversible function to support authentication exchange.
- 3. Data Integrity - As detailed in ISO 9797.
- 4. Hash Function - As detailed in ISO 10118 Part 2

- d) Cryptographic Interface Parameters

- 1. I/P Size 64 bits
- 2. O/P Size 64 bits
- 3. Keylength 64 bits (8 bits even parity, 1 bit per byte of key)
- 4. IV Size 64 bits
- 5. Symmetric Keystream Generator, primarily for Additive Stream Cipher (ASC) mode

- e) Test Words -

The following data are represented as hexadecimal numbers.
The most significant byte first.

INPUT DATA				
CRYPTOVARIABLE:	C3B8	A52B	F95F	8EB1
INITIALISATION VECTOR:	8E61	D8CE	40CA	FA36
OUTPUT DATA				
	E548	A35C	9F16	CD7D
	A5E0	DEB0	3CE8	91D5
	0AD9	B429	2590	9104
	EAF1	16A5	B1D2	8C22
	9C30	4FE9	2D07	2C02
	CED2	ED7E	3FF1	C6B7
	3473	6F3E	05B9	9BFE
	0DEA	DE4F	4609	08DA
	DB53	E464	C9B8	506E
	BB5D	E462	A76F	FF50

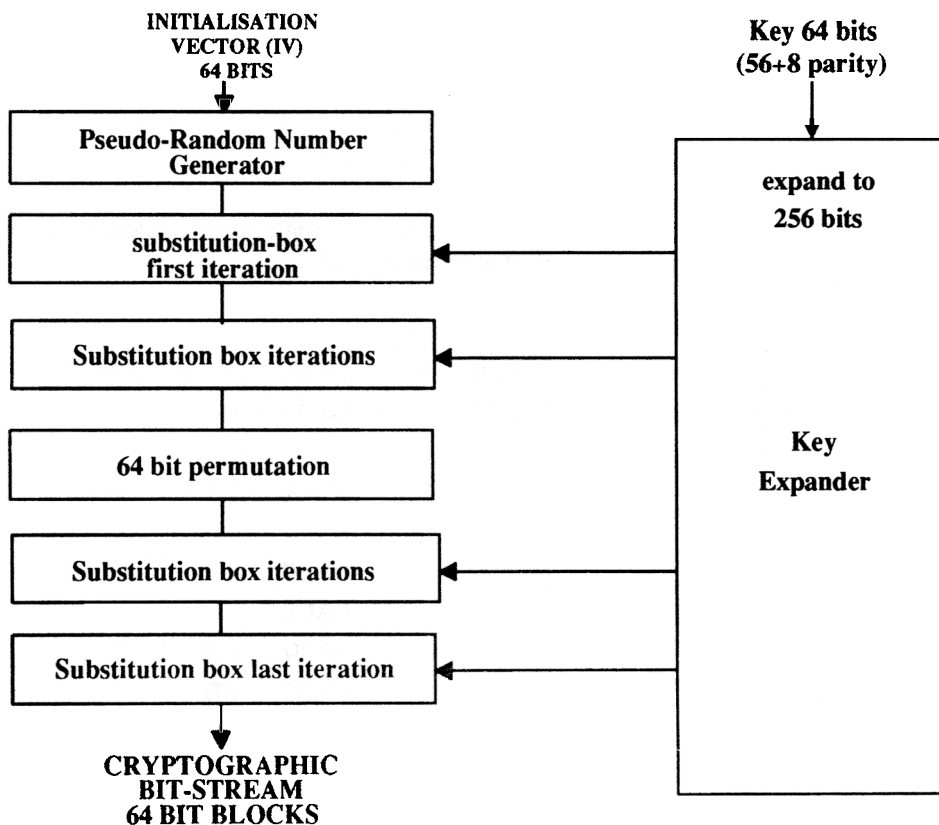
- f) Name of Sponsoring Authority BSI
- For Information, contact Philip Amey
BT/D&P/DSL
Room 303, St Vincent House
1 Cutler Street
Ipswich, IP1 1UX
UK

- g) Dates of Registration & Modification Allocated by NCC - 19 August 1992

- h) Whether the Subject of a National Standard Not a National Standard
- i) Patent Licence Restriction No
- j) List of references See ISO 8372 and ISO 9160 for information on modes of operation and physical layer aspects.
- k) Description of Algorithm

B-CRYPT is designed for use in communication and computer security products. The exact details of the B152 algorithm will not be generally published.

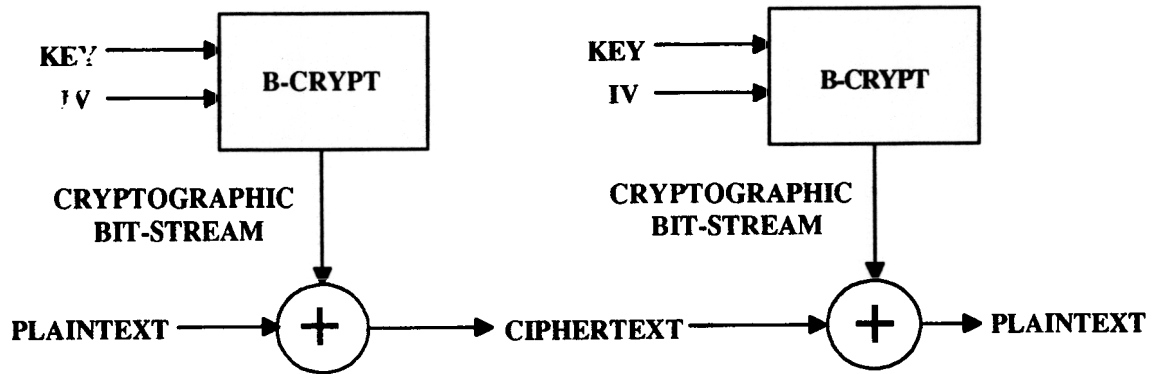
OUTLINE OF THE STRUCTURE OF THE B-CRYPT ALGORITHM



B-CRYPT is a VLSI implementation of the B152 algorithm, designed by BT Cryptographic Products to provide privacy in a wide range of telecommunication services using a block mode transmission protocol. In particular it can be used in digital terminals for telephony and data, communicating office products, and in securing network management. The device produces a sequence of 64-bit blocks of pseudo-random bit-stream, using a key and a 64-bit initialisation vector. Key variables are of 64 bits, formatted with every eighth bit representing even parity for the previous seven. Normally, the device operates in the Additive Stream Cipher mode.

1) Modes of Operation

PREFERRED MODE OF USE - ADDITIVE STREAM CIPHER



Secondary

1. Cipher Feedback
2. Cipher Block Chaining

m) Other Information

B-CRYPT has been implemented in 2 micron CMOS technology and operates in excess of 20 Mbits per second