PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/06, 9/00 — A1

(11) International Publication Number: WO 00/31916

(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/GB99/03891

(22) International Filing Date: 23 November 1999 (23.11.99)

(30) Priority Data:
9825644.9 23 November 1998 (23.11.98) GB

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

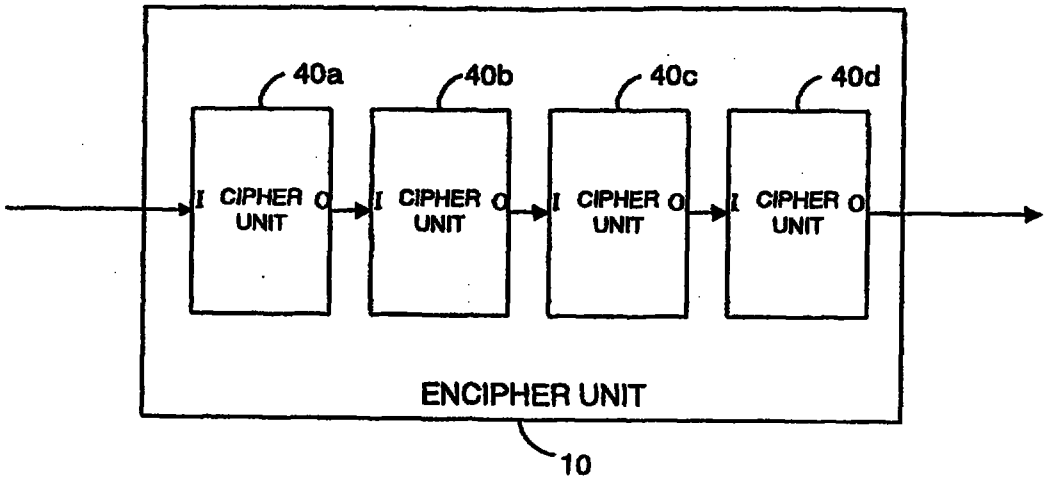
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BILCHEV, George [BG/GB]; 33 Elmers Lane, Ipswich IP5 2GW (GB).

(74) Agents: BERESFORD, Keith, Denis, Lewis et al.; Beresford & Co., 2-5 Warwick Court, High Holborn, London WC1R 5DJ (GB).

(81) Designated States: CA, SG, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A CIPHER



(57) Abstract

A cipher is disclosed for enciphering and deciphering a signal which comprises a plurality of sequentially coupled cipher units, each cipher unit being operable to carry out a reversible operation on the signal. The couplings between cipher units can be randomly configured using a cipher code. The cipher code can be secretly shared between the encipher and decipher. A signal which is enciphered using this technique is thus deciphered using a randomly selected cipher circuit as described by the cipher code.