[A] TIIVISTELMÄ - SAMMANDRAG

SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(11) (21) Patenttihakemus - Patentansökan 953232

(51) Kv.lk.6 - Int.cl.6

H 04L 9/26

(22) Hakemispäivä - Ansökningsdag 29.06.95

(24) Alkupäivä - Löpdag 30.12.93

(41) Tullut julkiseksi - Blivit offentlig 29.06.95

(86) Kv. hakemus - Int. ansökan PCT/AU93/00687

(32) (33) (31) Etuoikeus - Prioritet

30.12.92 AU 6577 PL

(71) Hakija - Sökande

1. **Telstra Corporation Limited**, 242 Exhibition Street, Melbourne, VIC 3000, Australia, (AU)

(72) Keksijä - Uppfinnare

1. **Taylor, Richard**, 29 Sherbrooke Lodge Road, Sherbrooke, VIC 3789, Australia, (AU)

(74) Asiamies - Ombud: **Berggren Oy Ab**

(54) Keksinnön nimitys - Uppfinningens benämning

Menetelmä ja laite koodijonon muodostamiseksi
Förfarande och anordning för generering av en chifferström

(57) Tiivistelmä - Sammandrag

Järjestelmä digitaalisen viestin salaamiseksi ja salauksen purkamiseksi käsittää lineaarisen ohjaus-alijärjestelmän (4) näennäissatunnaisen datajonon muodostamiseksi, epälineaarisen takaisinkytkentä-alijärjestelmän (6) koodijonon muodostamiseksi mainitun näennäissatunnaisen datajonon perusteella, ja salausprosessorin (26) viestin salaamiseksi tai sen salauksen purkamiseksi yhdistämällä se mainittuun koodijonoon, jolloin epälineaarinen takaisinkytkentäjärjestelmä käsittää epälineaarisen takaisinkytkentä-prosessointivälineen (10) takaisinkytkentäjonon (12) muodostamiseksi soveltamalla epälineaarista funktiota mainitun näennäissatunnaisen datajonon ainakin yhteen arvoon ja takaisinkytkentäjonon ainakin yhteen aikaisempaan arvoon, sekä koodijonon muodostamisvälineet (10) mainitun koodijonon muodostamiseksi summaamalla mainitun näennäissatunnaisen datajonon parien arvojen tulot ja mainitun takaisinkytkentäjonon arvo, jolloin arvoparit valitaan niin, että parin kummankin elimen jonoasemien välinen erotus on erilainen jokaisen parin osalta.

System för chiffrering och dechiffrering av ett digitalt meddelande bestående av ett linjärt subsystem (4) för att generera en pseudoslumptalssekvens; ett olinjärt återkopplat subsystem (6) för att generera en chifferström ur nämnda pseudoslumptalssekvens; och en chiffreringsprocessor (26) för att chiffrera och dechiffrera ett meddelande genom att kombinera det med nämnda chifferström, varvid det olinjära återkopplade subsystemet omfattar olinjära återkopplade processorgan (10) för att generera en återkopplingssekvens (12) genom att tillämpa en olinjär funktion på minst ett värde ur nämnda pseudoslumptalssekvens och minst ett tidigare värde ur återkopplingssekvensen; samt organ (10) för att generera nämnda chifferström genom att summera produkter av värdepar ur nämnda pseudoslumptalssekvens med ett värde ur nämnda återkopplingssekvens, varvid värdeparen väljs så att skillnaden i sekvensposition mellan vardera leden i ett par är olika för varje par.