



SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(11) (21) Patenttihakemus - Patentansökan	964035
(51) Kv.lk.6 - Int.kl.6	
H 04N 7/16, 7/169	
(22) Hakemispäivä - Ansökningsdag	08.10.96
(24) Alkupäivä - Löpdag	29.09.94
(41) Tullut julkiseksi - Blivit offentlig	05.12.96
(86) Kv. hakemus - Int. ansökan	PCT/GB94/02116
(32) (33) (31) Etuoikeus - Prioritet	
08.04.94 GB 9407038 P	

(71) Hakija - Sökande

1. **Amstrad Public Limited Company**, Bretwood House, 169 Kings Road, Brentwood, Essex CM14 4EF, United Kingdom, (GB)

(72) Keksijä - Uppfinnare

1. **Davies, Donald Watts**, Fair Winds, 15 Hawkewood Road, Sunbury on Thames, Middlesex TW16 6HL, United Kingdom, (GB)

(74) Asiamies - Ombud: **Papula Rein Lahtela Oy**, Fredrikinkatu 61 A, 6.krs, 00100 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

Menetelmä ja laite salatun viestin lähetykseen ja vastaanottoon
Förfarande och anordning för sändning och mottagning av ett krypterat meddelande

(57) Tiivistelmä - Sammandrag

Ensimmäinen ja toisen salaustjärjestelmän kanssa yhteensopiva salattu signaali generoidaan muodostamalla salausdatasiinaali liittyen kuhunkin salausjärjestelmään. Erosignaali saadaan kahdesta salausdatasiinaalista ja salattava signaali salataan yhden salausjärjestelmän mukaisesti. Lähtöön annetaan salattu signaali, kaksi salaussignaalia ja erosiinaali. Dekooderissa, joka on yhteensopiva esimerkiksi ensimmäisen salausjärjestelmän kanssa, vastaanotetaan salattu data, toinen salausdatasiinaali ja erosiinaali. Näin dekooderi voi muodostaa ensimmäisen salausdatasiinaalin toisesta salausdatasiinaalista ja erosiinaalista ja siten dekodata salatun signaalin.

En med ett första och ett andra krypteringssystem kompatibel krypterad signal genereras genom att bilda en krypteringsdatasiignal som hänför sig till vart och ett krypteringssystem. Differenssignalen erhålls ur två krypteringsdatasiignaler och signalen som skall krypteras krypteras enligt det ena krypteringssystemet. Till utgången ges den krypterade signalen, två krypteringssignaler och differenssignalen. I en deko-der, vilken är kompatibel med till exempel det första krypteringssystemet, mottages det krypterade data, den andra krypteringssignalen och differenssignalen. På så sätt kan dekodern bilda den första krypteringsdatasiignalen från den andra krypteringsdatasiignalen och från differenssignalen och på så sätt dekodera den krypterade signalen.