ROMÂNIA
OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI

BREVET DE INVENŢIE (19) RO (11) 84795

(12) DESCRIEREA INVENŢIEI

(21) Cerere de brevet nr: **113232**
(22) Data înregistrării: **06.01.1984**
(61) Complementară la invenţia brevet nr:
(45) Data publicării: **28.06.2002**

(86) Cerere internaţională(PCT) nr.: data:
(87) Publicarea cererii internaţionale nr.: data:
(89)

(51)**Int.Cl.**[7]: **H 04 L 9/00;** H 04 K 1/02

(30) Prioritate:
(32) Data:
(33) Ţara:
(31) Certificat nr.

(71) Solicitant: **MINISTERUL APĂRĂRII NAŢIONALE - U.M. 02512, BUCUREŞTI, RO**
(73) Titular: **MINISTERUL APĂRĂRII NAŢIONALE , BUCUREŞTI, RO**
(72) Inventator: **BĂCANU CODIN DUMITRU, BUCUREŞTI, RO; STRÂMBU OVIDIU NICULAE, BUCUREŞTI, RO; SIMU ADRIAN NICOLAE, BUCUREŞTI, RO**

(54) APARAT DE SECRETIZARE AUTOMATĂ A DATELOR

(57) **Rezumat:** Invenţia se referă la un aparat pentru secretizarea automată a datelor ce utilizează un algoritm de generare a şirurilor pseudoaleatoare de caractere şi integrează funcţia de secretizare în cadrul procedurilor de teletransmitere prin intermediul unor protocoale de secretizare multifuncţionale cu compatibilitate faţă de terminalele reţelei de teletransmisie, alcătuit dintr-o unitate centrală cuprinzând un microprocesor, un generator al impulsurilor de tact, un amplificator al magistralei de date, un amplificator al magistralei de adrese şi un formator al semnalelor de control, prin unitatea centrală fiind cuplată la posturile de intrare-ieşire, la un decodificator furnizor de semnale de selecţie a unei memorii fixe, la o memorie de lucru şi la o memorie de salvare destinată depozitării informaţiilor necesare reluării funcţionării aparatului consecutiv întreruperilor tensiunii de alimentare.

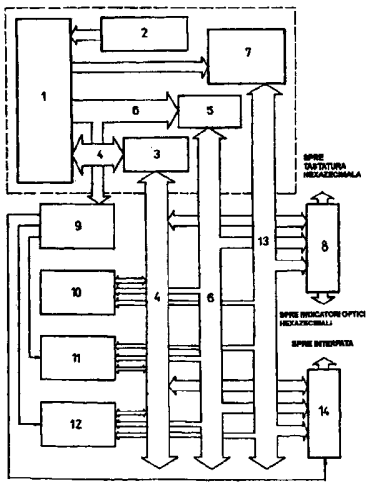

Fig. 1

(19) RO (11) 84795

Invenția se referă la un aparat destinat secretizării automate a informației vehiculate într-o rețea de teleprelucrare a datelor, conectarea aparatului în lanțul de transmisie, realizându-se fără modificarea procedurilor de teletransmisie existente sau terminalelor între care se realizează teletransmisia.

Sunt cunoscute aparate de securizare automată ce utilizează generatoare de semnale pseudoaleatoare şi logici de generare a cuvintelor cheie pe baza unor logaritmi.

Aceste aparate prezintă avantajele complexității schemei raportate la gradul oferit de protecție la descifrare, cât şi al compatibilității limitate cu diverse mijloace de transmisie.

Aparatul conform invenției, care utilizează un algoritm de generare a şirurilor pseudoaleatoare de caracter şi integrează funcția de secretizare în cadrul procedurilor de teletransmitere prin intermediul unor protocoale de secretizare multifuncționale cu compatibilitate față de terminalele rețelei de teletransmisie, este alcătuit dintr-o unitate centrală cuprinzând un microprocesor, un generator al impulsurilor de tact, un amplificator al magistralei de date, un amplificator al magistralei de adrese şi un formator al semnalelor de control, unitatea centrală fiind cuplată la posturile de intrare-ieşire la un decodificator furnizor de semnale de selecție a unei memorii fixe, la o memorie de lucru şi la o memorie de salvare, destinată depozitării informațiilor necesare rulării funcționării aparatului consecutiv întreruperilor tensiunii de alimentare.

Se dă, în continuare, un exemplu de realizare a invenției în legătură cu figura care reprezintă schema bloc funcțională a structurii logice şi de calcul.

Conform invenției, în figură sunt reprezentate principalele elemente ce compun structura logică şi de calcul precum şi legăturile funcționale dintre aceste elemente. Componenta principală a structurii este unitatea centrală formată dintr-un microprocesor **1**, un generator de impulsuri de tact **2**, un amplificator **3** al magistralei de date **4**, un amplificator **5** al magistralei de adrese **6** şi un formator **7** al semnalelor de control de citire a memoriei, de scriere a memoriei, de citire a porturilor **8** de intrare-ieşire şi de scriere a porturilor de intrare-ieşire. Un codificator **9** este destinat generării semnalelor de selecție a memoriilor şi a dispozitivelor de intrare-ieşire. O memorie fixă **10** asigură memorarea permanentă a informațiilor necesare funcționării aparatului, iar o memorie **11** de lucru are destinația de a memora mărimile variabile rezultate şi comenzile primite pe timpul funcționării aparatului. În componența acestei structuri intră şi o memorie de salvare **12** destinată depozitării, la anumite momente ordonate de către microprocesor, a mărimilor necesare reluării funcționării aparatului în cazul întreruperii accidentale sau voite a tensiunii de alimentare.

Comenzile date de formatorul **7** sunt transmise prin magistrala de comenzi **13**.

La cuplarea aparatului sau la acționarea tastei de inițializare, se execută autotestul ce verifică executarea corectă a algoritmului de generare a şirului de caracter pseudoaleator pe parcursul a 512 paşi de generare. Dacă rezultatul este pozitiv, aparatul este gata pentru introducerea comenzilor referitoare la modul şi viteza de lucru, cât şi la cheie. Comenzile de lucru ale aparatului se referă la modul de introducere a cheii, tipul terminalului de transmitere a datelor folosit şi viteza de transmitere în canalul de transmisiuni. Cu privire la modul de introducere a cheii, acesta poate fi dintr-o memorie fixă unde cheia a fost stocată, în prealabil, reluarea funcționării anterioare întreruperii tensiunii de alimentare

cu regimul de cheie în continuare şi introducerea manuală a cheii făcându-se prin intermediul tastaturii hexazecimale, ceea ce presupune executarea unui număr de tastări plus două tastări de control a corectitudinii introducerii cheii.

După executarea corectă a comenzilor enumerate mai sus, aparatul trece într-o stare de aşteptare a întreruperilor provocate de sosirea caracterelor de la terminalul deservit sau de la modem în vederea reducerii dialogului cu acestea conform protocolului de secretizare comandat.

Tastatura hexazecimală este cuplată la un port de intrare-ieşire de 8 biţi. Codificarea tastei apăsate se face pe baza intersecţiei unei linii cu o coloană dintr-o matrice 4 x 4, iar decodificarea acesteia se face pe baza unei liste de coduri anterioare memorate în memoria fixă.

Cei patru indicatori optici hexazecimali sunt conectaţi doi câte doi la magistrala de date formând două porturi de ieşire. Stingerea şi aprinderea acestor indicatori este comandată cu ajutorul a 4 biţi ai unui port de ieşire utilizată pentru vizualizarea mai sugestivă a mesajelor.

Aparatul este astfel conceput încât orice informaţie introdusă de la tastatura hexazecimală este introdusă în memoria de lucru şi vizualizată pe indicatorii optici hexazecimali.

Generarea şirurilor pseudoaleatoare de caracter se execută conform unui algoritm complex şi sub controlul unor chei de secretizare. Rezultatul fiecărei iteraţii a algoritmului se memorează în memoria de lucru pentru a putea fi utilizat la mixarea cu textul clar. Controlul executării paşilor de generare a caracterelor este preluat de un numărător pe trei octeţi. În timpul lucrului, octetul cel mai puţin semnificativ al acestui caracter este folosit pentru controlul intern al unor operaţiuni ale protocoalelor de secretizare, iar ceilalţi doi octeţi sunt vizualizaţi cu ajutorul indicatorilor optici hexagonali pentru a permite operaţiunea de sincronizare manuală a paşilor de secretizare şi controlul funcţionării apatratului.

Principalele caracteristici ale algoritmului de generare a şirurilor pseudoaleatoare de caractere sunt lungimea cheii iniţiale de 256 de biţi, lungimea perioadei de repetiţie a şirului generat de caractere, utilizarea de componente tuternic neliniare ce îi conferă o mare rezistenţă criptografică, înaltul grad aleator al şirurilor generate, independenţa statistică a şirurilor generate cu chei diferite cu distanţă Hamming minimă şi menţinerea la cote superioare a aleatorismului şirului generat indiferent de gradul de aleatorism al cheilor iniţiale.

Pentru a preveni transmiterea în linie a mesajelor incorect secretizate sau a introducerii cheilor de către persoane neautorizate, aparatul execută o serie de controale asupra funcţionării anumitor componente şi asupra introducerii comenzilor sau a cheilor de lucru. În cazul depistării unei neconcordanţe logice, funcţionarea aparatului este blocată iar pe indicatorii optici hexazecimali se vizualizează cu intermitenţă următoarele tipuri de erori:

- eroare de operaţie în tastarea comenzilor;
- poziţionarea incorectă a comutatorului care permite introducerea cheii;
- introducere incorectă a cheii de la tastatură;
- execuţie incorectă a algoritmului de generare a şirurilor pseudoaleatoare de caractere;
- defecţiune de alimentare a memoriei de salvare.

Integrarea funcţiei de secretizare în sistemele care realizează transmiterea şi prelucrarea la distanţă a datelor se obţine cu ajutorul protocoalelor de securizare adoptate diferitelor proceduri de transmitere, diferitelor viteze de lucru şi diferitelor tipuri de terminale între care se realizează

transferul la distanță a datelor prin intermediul canalelor de transmisiuni. Pentru a realiza compatibilizarea cu întreaga gamă de terminale utilizate în rețelele de transmitere a datelor prin țara noastră, aparatul conform invenției este prevăzut cu patru tipuri de protocoale de secretizare care vor fi prezentate în continuare.

Protocolul de secretizare în mod paralel asigură livrarea către transmițătorul de date deservit a câte unui caracter aleator de 7 biți plus un bit de paritate la fiecare cerere prezentată de transmițător. Livrarea se efectuează pe principiul semnalelor de întrerupere generate de către un port de ieşire. În cadrul acestui protocol, aparatul se rezumă a fi un simplu generator de şiruri pseudoaleatoare de caractere ce nu intervine în procesul propriu-zis de transmitere a datelor, din care cauză mixarea caracterelor livrate cu textul clar, măsurile de securitate a secretizării, precum şi rezolvarea eventualelor incidente de transmitere sunt sarcini care revin în totalitate procedurii de teletransmitere utilizate.

Protocolul de secretizare în mod caracter este destinat criptării informațiilor vehiculate în transmisiile de date semiduplex în mod caracter, seriale, asincrone (stop-start) pe 7 biți plus un bit de paritate. La recepționarea, prin intermediul interfației standard 14 din linie sau de la terminalul deservit a unui caracter definitiv anterior, unitatea de transmisie emite un semnal de întrerupere care provoacă lansarea în execuție a unei rutine de tratare a acestui tip de întrerupere. În cadrul acestei rutine, caracterul recepționat este mixat cu caracterul curent din şirul pseudoaleator generat conform algoritmului şi emis de către unitatea de transmisie, prin intermediul interfeței standard către terminalul deservit sau către linie. Caracterul BREAK ("Zero lung"), fiind singurul tratat special cu scopul de a fi recunoscut şi emis fără implicații asupra procesului de criptare, care ține cont automat de viteza de transmitere.

Protocolul de securizare în mod mesaj sincron asigură recepția şi emisia atât a blocurilor informaționale de lungime variabilă sau de lungime fixă cât şi a secvențelor de răspuns a receptorului constând în acceptarea sau neacceptarea blocului informațional recepționat. Principiul de funcționare se bazează tot pe semnalele de întrerupere emise de către unitatea de transmisie către microprocesor la recepția fiecărui caracter din linie sau de la terminalul deservit iar rutina de tratare a acestui tip de întreruperi respectă o procedură complexă ținând cont de poziția şi tipul fiecărui caracter în cadrul blocului de date. Când terminalul deservit prezintă o cerere de emisie către aparatul de secretizare, acesta prelucrează cererea şi transmite această comandă modemului. La recepția fiecărui caracter din linie sau de la terminalul, rutina de întrerupere analizează structura acestuia şi dacă este caracter STX (cod ASCII), îl emite în clar. Dacă este ETX (cod ASCII) intră în execuția unei subrutine pentru tratarea sfârşitului de bloc, subrutină care permite sincronizarea automată a şirurilor pseudoaleatoare de caractere generate de către cele două aparate de secretizare aflate în corespondență. Operațiuni similare se execută şi în rutinele de tratare a recepției, secvențelor de răaspuns ACK, NAK şi EOT. Subrutina de tratare a sfârşitului de bloc se execută şi în cazul lucrului pe blocuri fixe de 32 caractere informaționale după recepția celui de al 32-lea caracter informațional. Operațiunea de sincronizare automată se efectueazăprin compararea de către aparatul de secretizare receptor a numărului de bloc propriu al şirului pseudoaleator de caractere cu numărul de bloc recepționat de la aparatul de secretizare emițător, numărul de bloc înseriat la sfârşitul fiecărei secvențe de date emise. În cadrul acestui protocol unitatea de

transmisie lucrează full-duplex în mod asincron, permiţând protocolului de secretizare, ce include şi sincronizarea automată a paşilor de secretizare, să lase neschimbată procedura de teletransmisie utilizată.

Protocolul de secretizare în mod mesaj sincron execută operaţiuni din cea mai mare parte similare operaţiunilor descrise la protocolul anterior, deosebirile principale provenind din faptul că unitatea de transmisie lucrează în full-duplex mod sincron cu sincronizare exterioară, că se lucrează numai pe blocuri informaţionale variabile încadrate între caracterele de serviciu STX şi ETX cu lungimea maximă declarată la cele două transmiţătoare de date aflate în corespondenţă şi că sincronizarea caracterelor transmise nu se realizează cu ajutorul biţilor START-STOP ci se realizează o sincronizare la nivelul de bloc cu ajutorul caracterelor de sincronizare. De asemenea, timpii de răspuns şi de aşteptare se tratează în mod diferit în special datorită restricţiilor suplimentare impuse de lucrul cu calculatorul.

Totodată, datorită faptului că tactul de transmitere a datelor pentru unitatea de transmisie este preluat în acest caz de la modem, schimbarea vitezelor de transmitere nu mai implică nici o comandă pentru aparatul de securizare.

Aparatul de securizare , conform invenţiei, prezintă avantajul că oferă utilizatorilor posibilitatea realizării de sisteme informaţionale conţinând date alfanumerice cu caracter secret şi strict secret în cadrul reţelelor de teleprelucrare, asigurând protecţia la scurgerea de informaţii prin intermediul secretizării automate cu ajutorul unei metode de mare rezistenţă criptanalitică.

Revendicare

Aparat pentru secretizare automată a datelor, ce utilizează un algoritm de generare a şirurilor pseudoaleatoare de caractere şi integrează funcţia de secretizare, în cadrul procedurilor de teletransmitere, prin intermediul unor protocoale de secretizare, multifuncţionale, cu compatibilitate faţă de terminalele reţelei de teletransmisie, **caracterizat prin aceea că**, este alcătuit dintr-o unitate centrală cuprinzând un microprocesor (**1**), un generator (**2**) al impulsurilor de tact, un amplificator (**3**) al magistralei de date (**4**), un amplificator (**5**) al magistralei de adrese (**6**) şi un formator (**7**) al semnalelor de control, unitatea centrală fiind cuplată la porturile de intrare-ieşire (**8**), la un decodificator (**9**) furnizor de semnale de selecţie a unei memorii fixe (**10**), la o memorie de lucru (**11**) şi la o memorie de salvare (**12**), destinată depozitării informaţiilor necesare reluării funcţionării aparatului consecutiv întreruperilor tensiunii de alimentare.

(56) **Referinţe bibliografice:**
Brevet US nr. 4310720
Brevet, FR nr. 2497617

PREŞEDINTELE COMISIEI DE INVENŢII: **ing. Erhan Valeriu**
EXAMINATOR: **ing. Sergiu Balaban**

RO 84795

(51) Int.Cl.[7]: H 04 L 9/00;

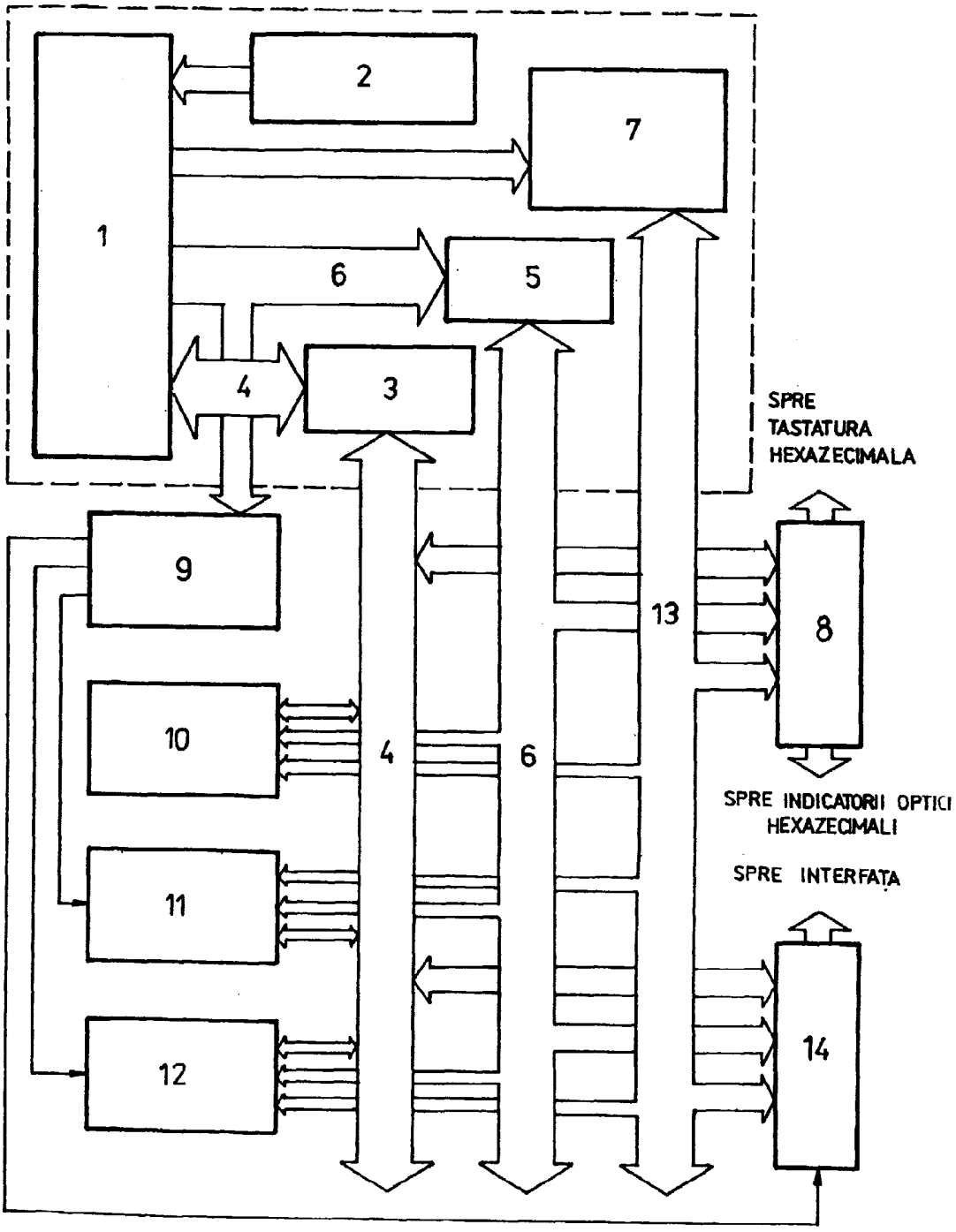

Fig. 1

Editare şi tehnoredactare computerizată - OSIM
Tipărit la: Oficiul de Stat pentru Invenţii şi Mărci