MD 1872 F1 2002.02.28

REPUBLICA MOLDOVA

(19) Agenţia de Stat
pentru Protecţia Proprietăţii Industriale

(11) 1872 (13) F1
(51) Int. Cl.[7]: H 04 L 9/00;
H 04 K 1/00

(12) BREVET DE INVENŢIE

Hotărârea de acordare a brevetului de invenţie poate fi revocată în termen de 6 luni de la data publicării

(21) Nr. depozit: a 2000 0090
(22) Data depozit: 2000.04.25

(45) Data publicării hotărârii de acordare a brevetului:
2002.02.28, BOPI nr. 2/2002

(71) Solicitant: Compania DEKART, S.R.L., MD
(72) Inventatori: OLEINIK Weaceslaw, MD; ANESTIADI Valerii, MD
(73) Titular: Compania DEKART, S.R.L., MD
(74) Reprezentant: JENICICOVSCAIA Galina, MD

(54) Procedeu şi dispozitiv de asigurare a schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţie

(57) Rezumat:

1

Invenţia se referă la telecomunicaţii şi tehnica de calcul, anume la procedeele criptografice şi dispozitivele pentru cifrarea datelor digitale.

Este propus un procedeu pentru schimbul autentificat cu chei secrete prin canale deschise de telecomunicaţie care foloseşte extinderea algoritmului Diffie şi Hellman prin adăugarea unui protocol nou, care asigură legarea fiabilă a cheii secrete comune cu cheile deschise semnate şi

2

identificatori ai utilizatorilor, şi un dispozitiv care realizează procedeul solicitat.

Rezultatul invenţiei solicitate constă în posibilitatea realizării schimbului autentificat cu chei secrete prin canale deschise şi în majorarea rezistenţei sistemului în întregime.

Revendicări: 2
Figuri: 1

MD 1872 F1 2002 02.28

Descriere:

Invenţia se referă la telecomunicaţii şi tehnica de calcul, şi anume la procedeele criptografice şi dispozitivele pentru cifrarea datelor digitale.

În descrierea invenţiei solicitate se folosesc următorii termeni:

transformare criptografică - transformarea unui volum de informaţie, scopul căreia este ascunderea conţinutului acestei informaţii, prevenirea schimbării ei sau a folosirii ei nelegitime;

funcţie unilaterală - conform definiţiei, ea reprezintă o oarecare funcţie f pentru orice x din domeniul definiţiei acestei funcţii, $f(x)$ se calculează uşor, însă pentru toţi y din domeniul valorilor ei, calcularea valorii x, pentru care $y = f(x)$, practic nu este realizabilă;

cheie - succesiunea simbolurilor, care determină starea unor parametri ai algoritmului transformării criptografice şi care asigură alegerea unei transformări din totalitatea (mulţimea) transformărilor criptografice posibile pentru algoritmul dat al transformării;

cheie deschisă - succesiunea simbolurilor accesibilă pentru toţi conţinând un parametru, care participă în generarea cheii secrete comune, în transformarea criptografică a semnăturii digitale şi care este destinată verificării corespunderii semnăturii digitale a unui utilizator concret;

cheie secretă - succesiunea simbolurilor, conţinând un parametru, care determină generarea cheii secrete comune, îndeplinirea algoritmului criptografic al semnăturii digitale şi care este cunoscută numai unui utilizator împuternicit;

cheie secretă comună - succesiunea simbolurilor, conţinând un parametru, ce determină algoritmul criptografic de cifrare şi de descifrare a mesajului secret, generat cu folosirea cheilor deschise ale participanţilor la schimbul cu mesaje secrete, şi care este cunoscută numai celor doi utilizatori-participanţi la schimbul cu mesaje secrete;

criptoanaliză - calcularea cheii secrete pentru obţinerea accesului nesancţionat la informaţia cifrată sau elaborarea procedeului, care asigură accesul la informaţia cifrată fără calcularea cheii secrete;

criptoanalist - persoana, care îndeplineşte o criptoanaliză;

$\oplus$ - este operaţia "exclusive OR" bit cu bit (sumă după modulul egal cu doi);

$||$ - operaţia de concatenare (aderenţă);

identificatorul utilizatorului concret - succesiunea simbolurilor, care într-un singur sens identifică un utilizator concret al reţelei, sistemului etc.

Este cunoscut procedeul de schimb cu cheile secrete prin canale deschise, care a fost propus de către Diffie şi Hellman [1]. În acest procedeu se foloseşte funcţia unilaterală, care reprezintă o funcţie discretă de ridicare la putere $f(x) = \alpha^x \pmod p$, unde x este un număr întreg de la 1 la p - 1 inclusiv, iar calculele se efectuează după modulul egal cu p, unde p este un număr prim foarte mare; α este un număr întreg din gama $1 \le \alpha \le p$, puterile posibile ale căruia sunt egale cu: $\alpha, \alpha^2, ..., \alpha^{p-1}$ (după modulul egal cu p). (În algebră aşa un α se numeşte element primitiv al câmpului finit Galua GF(p) şi este ştiut că α de acest fel există întotdeauna).

De exemplu, pentru $p=7$ şi $\alpha=3$, $f(x)=\alpha^x \pmod p$ poate avea următorul şir de valori: $x=1$ $f(x)=3$, $x=2$ $f(x)=2$, $x=3$ $f(x)=6$, $x=4$ $f(x)=4$, $x=5$ $f(x)=5$, $x=6$ $f(x)=1$. Funcţia $f(x)$ poate fi uşor calculată cu ajutorul ridicării la pătrat şi înmulţirii (după modulul egal cu p). De exemplu, pentru a calcula $\alpha^{53} = \alpha^{32+16+4+1}$, la început este necesar de găsit α^2, $\alpha^4=(\alpha^2)^2$, $\alpha^8=(\alpha^4)^2$, $\alpha^{14}=(\alpha^8)^2$ şi $\alpha^{32}=(\alpha^{16})^2$; pentru aceasta sunt necesare cinci operaţii de înmulţire. Apoi trebuie de înmulţit α^{32} consecvent la α^{16}, α^4 şi α, ceea ce necesită încă trei operaţii şi astfel rezultatul se obţine cu opt operaţii (după modulul egal cu p). Chiar pentru $p \sim 2^{1000}$ calcularea funcţiei $f(x)$ pentru orice număr întreg x, din gama valorilor posibile ($1 \le x \le p$), necesită mai puţin decât 2000 de operaţii de înmulţire (după modulul egal cu p).

În cazul în care $y=\alpha^x \pmod p$, calcularea lui x se realizează cu ajutorul funcţiei $x=\log_\alpha(y) \pmod p$, iar problema inversiunii funcţiei $f(x)$ se numeşte problema găsirii logaritmilor discreţi. Fiindcă funcţia discretă de ridicare la putere este unilaterală, calcularea funcţiei $\log_\alpha(y) \pmod p$ este practic irealizabilă pentru toţi y din gama valorilor posibile ($1 \le y \le p$).

Folosind acest fapt Diffie şi Hellman au propus următorul procedeu, foarte simplu, de folosire a logaritmilor discreţi pentru schimbul cu chei secrete între utilizatorii reţelei cu folosirea mesajelor deschise. Se va presupune că tuturor utilizatorilor le sunt cunoscute α şi p. Fiecare utilizator, de exemplu utilizatorul i, în mod aleatoriu alege un număr întreg R_i, din gama valorilor posibile de la 1 la p-1, ţinându-l în secret. Acest număr este cheia lui secretă. Apoi el calculează cheia lui deschisă $W_i=\alpha^{Ri} \pmod p$.

Utilizatorul i publică valoarea W_i într-un ghid deschis, accesibil pentru toţi utilizatorii. În viitor, dacă utilizatorii i şi j vor dori să stabilească o legătură secretă, utilizatorul i va folosi din ghid cheia deschisă a utilizatorului j - W_j şi cu ajutorul cheii sale secrete R_i va calcula cheia secretă comună pentru utilizatorii i şi j - Z_{ij}:

$Z_{ij} = (W_j)^{R_i} = (\alpha^{R_j})^{R_i} = \alpha^{R_j R_i}$ (mod p).

În mod similar şi utilizatorul j va calcula cheia sa secretă comună

$Z_{ji} = (W_i)^{Rj} = (\alpha^{R_i})^{Rj} = \alpha^{RiRj}$ (mod p). Fiindcă $Z_{ij} = Z_{ji}$, utilizatorii i şi j din acest moment pot să folosească Z_{ij} şi, corespunzător, Z_{ji} ca cheie secretă comună, care le aparţine în exclusivitate şi există într-un sistem criptografic clasic. Dacă un criptoanalist ar putea să rezolve problema calculării logaritmilor discreţi, el ar putea, folosind din ghid W_i şi W_j, să rezolve ecuaţia $R_i = \log_\alpha W_i (\text{mod } p)$ şi să calculeze Z_{ij} asemănător utilizatorului i.

Schema descrisă se numeşte sistem de răspândire deschisă a cheilor Diffie şi Hellman. Acest sistem, care permite a se renunţa la transmiterea cheilor secrete, este unul din cele mai rezistente şi comode sisteme cu chei deschise.

Însă sistemul răspândirii deschise a cheilor Diffie şi Hellman, deşi permit de a exclude folosirea unui canal protejat pentru transmiterea cheilor secrete, nu înlătură necesitatea autentificării cheilor deschise ale utilizatorilor. Deţinătorul ghidului public accesibil trebuie să fie sigur că cheia deschisă W_i este introdusă în ghid chiar de către utilizatorul i, iar utilizatorul i trebuie să fie sigur că cheia deschisă W_j este trimisă lui chiar de către deţinătorul ghidului.

Cel mai apropiat după esenţă şi rezultatul obţinut este procedeul de generare a cheii secrete comune între emiţător şi receptor [2] care foloseşte un generator al cheii secrete comune şi constă în generarea cheii secrete comune $K_{ij} = Y_i^{X_j} (\text{mod } q) = K_{ji} = Y_j^{X_i} (\text{mod } q)$ pentru transmiţătorul i şi receptorul j cu ajutorul funcţiei discrete de ridicare la putere $f(x) = \alpha^x (\text{mod } q)$, calcularea şi schimbul cu cheile deschise $Y_i = a^{X_i} (\text{mod} q)$, $Y_j = a^{X_j} (\text{mod } q)$, incluzând următorii paşi:

1. Generarea şi transformarea în mod ireversibil a semnalului unu, care este cheia secretă a emiţătorului, pentru primirea semnalului unu transformat, care prezintă cheia deschisă a emiţătorului, totodată transformarea semnalului unu menţionat se îndeplineşte prin ridicarea primului număr la putere, care este prezentată de către semnalul unu menţionat, după modulul egal cu numărul al doilea.
2. Generarea şi transformarea în mod ireversibil a semnalului doi, care este cheia secretă a receptorului, pentru a primi semnalul doi transformat, care prezintă cheia deschisă a receptorului, totodată transformarea semnalului doi menţionat se îndeplineşte prin ridicarea primului număr la putere, care este prezentată de către semnalul doi menţionat, după modulul egal cu numărul al doilea.
3. Transmiterea semnalului unu transformat menţionat de la emiţător la receptor.
4. Transmiterea semnalului doi transformat menţionat de la receptor la emiţător.
5. Transformarea semnalului doi transformat menţionat împreună cu semnalul unu menţionat în emiţător pentru generarea semnalului trei, care prezintă cheia secretă comună a emiţătorului, care nu poate fi generată numai cu semnalul unu transformat menţionat şi semnalul doi transformat menţionat, totodată transformarea semnalului doi transformat menţionat împreună cu semnalul unu menţionat se îndeplineşte prin ridicarea numărului prezentat de către semnalul doi transformat menţionat, la puterea prezentată de către semnalul unu menţionat, după modulul egal cu numărul al doilea, şi
6. Transformarea semnalului unu transformat menţionat împreună cu semnalul doi menţionat în receptor pentru generarea semnalului patru, care este identic cu semnalul trei şi prezintă cheia secretă comună menţionată a receptorului care nu poate fi generată numai cu semnalul unu transformat menţionat şi semnalul doi transformat menţionat, totodată transformarea semnalului unu transformat menţionat cu semnalul doi menţionat se îndeplineşte prin ridicarea numărului prezentat de către semnalul unu transformat menţionat, la puterea prezentată de către semnalul doi menţionat, după modulul egal cu numărul al doilea.

În procedeul descris termenii emiţător şi receptor sunt identici cu termenii utilizatorul i şi utilizatorul j, în mod corespunzător.

De asemenea este cunoscut dispozitivul pentru generarea cheii secrete comune, care conţine:

- generatorul primei chei secrete comune, a cărui intrare unu, pentru recepţia semnalului lansat unu, este conectată cu ieşirea blocului de introducere a cheii secrete, şi intrarea doi, pentru recepţia semnalului doi, este conectată la ieşirea unu a blocului de realizare a funcţiilor, având mijloace pentru generarea semnalului trei la ieşirea unu, conectată la intrarea doi a blocului de realizare a funcţiilor, totodată semnalul trei menţionat Y_i se descrie prin expresia $Y_i = a^{X_i} (\text{mod} q)$, unde q este un număr prim mare, a – un număr aleatoriu, care se află în gama valorilor $1 \le a \le q-1$, iar X_i este semnalul unu, care este un număr aleatoriu şi care se află în gama valorilor $1 \le X_i \le q-1$, totodată transformarea semnalului unu menţionat este ireversibilă, şi mijloace pentru generarea semnalului patru la ieşirea doi conectată la intrarea blocului pentru păstrarea cheii secrete comune,

totodată semnalul patru menţionat K_{ij} se descrie prin expresia $K_{ij} = Y_j^{X_i} (\mathrm{mod}\, q)$, unde Y_j corespunde semnalului doi, rezultatul transformării semnalului doi menţionat împreună cu semnalul unu menţionat prezintă cheia secretă comună;

- generatorul celei de-a doua chei secrete comune, a cărui intrare unu, pentru recepţia semnalului cinci, este conectată la ieşirea blocului de introducere a cheii secrete, intrarea doi, pentru recepţia semnalului trei, este conectată la ieşirea unu a blocului primei chei secrete, având mijloace pentru generarea semnalului doi la ieşirea unu conectată la intrarea doi a blocului primei chei secrete, totodată semnalul doi menţionat Y_j se descrie prin expresia $Y_j = a^{X_j} (\mathrm{mod}\, q)$, unde X_j este semnalul cinci, care prezintă un număr aleatoriu, care se află în gama valorilor $1 \le X_j \le q-1$, transformarea semnalului cinci menţionat fiind ireversibilă, şi mijloace pentru generarea semnalului şase la ieşirea doi conectată la intrarea blocului pentru păstrarea cheii secrete comune, totodată semnalul şase menţionat K_{ji} se descrie prin expresia $K_{ji} = Y_i^{X_j} (\mathrm{mod} q)$, rezultatul transformării semnalului trei împreună cu semnalul cinci menţionat prezentând cheia secretă comună.

Procedeul şi dispozitivul descrise asigură schimbul cu cheile secrete K_{ij} şi K_{ji} prin canale deschise la transmiterea exclusivă a parametrilor nesecreţi q, a şi a cheilor deschise (nesecrete) Y_i, Y_j. Acest procedeu funcţionează bine în multe aplicaţii. Însă deficienţa lui este aceea că în el lipseşte autentificarea cheilor deschise ale utilizatorilor, adică, de exemplu, un utilizator i nu va putea fi sigur că cheia Y_j este realmente cheia deschisă a utilizatorului j. Această problemă devine actuală în mod deosebit atunci, când condiţiile schimbului cu mesaje secrete necesită folosirea de fiecare dată a unor chei secrete noi (pentru o şedinţă de legătură). Metoda clasică de autentificare a cheilor deschise în acest caz nu se potriveşte, fiindcă ea într-o măsură semnificativă reduce viteza schimbului.

Problema pe care o rezolvă invenţia este elaborarea unui procedeu şi, respectiv, a unui dispozitiv, care ar permite asigurarea schimbului autentificat cu chei secrete prin canale deschise şi schimbului operativ al cheii secrete pentru o şedinţă de legătură fără certificarea suplimentară a cheii deschise pentru o şedinţă de legătură.

Problema invenţiei se rezolvă prin aceea că în procedeul de asigurare a schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţii, care constă în generarea cheii secrete comune $K_{ij} = Y_i^{X_j} (\mathrm{mod}\ q) = K_{ji} = Y_j^{X_i} (\mathrm{mod}\ q)$ pentru transmiţătorul i şi receptorul j cu ajutorul funcţiei discrete de ridicare la putere $f(x) = \alpha^x (\mathrm{mod}\ q)$, calcularea şi schimbul cu cheile deschise $Y_i = a^{X_i} (\mathrm{mod} q)$, $Y_j = a^{X_j} (\mathrm{mod}\ q)$, nou este aceea că în timpul schimbului cu cheile deschise între transmiţătorul i şi receptorul j se folosesc suplimentar identificatorii lor I_i şi I_j, se creează succesiuni aleatorii de biţi C_i şi C_j, se calculează valorile $Z_i = K_{ij} \oplus C_i$, $Z_j = K_{ji} \oplus C_j$ şi semnăturile digitale $S_i = DSA\,(HASH\ (I_i \| Y_i \| I_j \| Y_j \| C_i))$, $S_j = DSA\,(HASH\ (I_i \| Y_i \| I_j \| Y_j \| C_j))$, transmiţătorul i şi receptorul j se schimbă cu valorile I_i, Z_i, S_i şi I_j, Z_j, S_j, folosind cheia secretă comună K_{ij} se calculează $C_{ir} = K_{ij} \oplus Z_i$, $C_{jr} = K_{ij} \oplus Z_j$, se verifică semnătura digitală a parametrilor I_i, Y_i, I_j, Y_j, C_i şi I_i, Y_i, I_j, Y_j, C_j.

Procedeul conform invenţiei conţine următorii parametri suplimentari: identificatorul utilizatorului I_i; succesiunea aleatorie de biţi C_i; algoritmii suplimentari: DSA - algoritmul, care realizează semnătura digitală; HASH - algoritmul, care realizează funcţia HASH şi include următorii paşi suplimentari:

1. Utilizatorul i creează cheia secretă aleatorie X_i şi calculează cheia deschisă corespunzătoare ei $Y_i = a^{X_i} (\mathrm{mod}\, q)$ pe care el împreună cu identificatorul său I_i le transmite utilizatorului j.

2. Utilizatorul j creează cheia secretă aleatorie X_j şi calculează cheia deschisă corespunzătoare ei $Y_j = a^{X_j} (\mathrm{mod}\ q)$. În plus, el calculează cheia secretă comună $K_{ji} = Y_i^{X_j} (\mathrm{mod}\, q)$. Ulterior el creează succesiunea aleatorie a biţilor C_j şi calculează $Z_j = K_{ji} \oplus C_j$, iar apoi utilizatorul j calculează semnătura digitală $S_j = DSA\,(HASH\ (I_i \| Y_i \| I_j \| Y_j \| C_j))$. Valorile I_j, Y_j, Z_j şi S_j utilizatorul j le transmite utilizatorului i.

3. Utilizatorul i calculează cheia secretă comună K_{ij}, folosind pentru aceasta Y_j şi cheia sa secretă X_i în felul următor: $K_{ij} = Y_j^{X_i} (\mathrm{mod}\, q)$, ulterior el calculează succesiunea restaurată a biţilor $C_{jr} = K_{ij} \oplus Z_j$, şi verifică semnătura digitală a parametrilor I_i, Y_i, I_j, Y_j şi C_j, îndeplinită de utilizatorul j. Apoi el creează succesiunea aleatorie a biţilor C_i, calculează $Z_i = K_{ij} \oplus C_i$ şi $S_i = DSA\,(HASH\ (I_i \| Y_i \| I_j \| Y_j \| C_i))$ şi transmite valorile Z_i, S_i utilizatorului j.

4. Utilizatorul j, folosind cheia sa secretă comună K_{ji} calculează succesiunea restaurată a biţilor $C_{ir}=K_{ji} \oplus Z_i$ şi verifică semnătura digitală a parametrilor I_i, Y_i, I_j, Y_j şi C_i, îndeplinită de utilizatorul *i*.

Problema dată se rezolvă de asemenea cu ajutorul dispozitivului pentru asigurarea schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţie, care conţine:

- generatorul (2) al primei chei secrete comune, a cărui intrare unu, pentru recepţia semnalului lansat unu, este conectată cu ieşirea blocului (1) de introducere a cheii secrete, şi intrarea doi, pentru recepţia semnalului doi, este conectată la ieşirea unu a blocului (6) de realizare a funcţiilor, având mijloace pentru generarea semnalului trei la ieşirea unu, conectată la intrarea doi a blocului (6), totodată semnalul trei menţionat Y_i se descrie prin expresia $Y_i = a^{X_i} (\mathrm{mod} q)$, unde q este un număr prim mare, a – un număr aleatoriu, care se află în gama valorilor $1 \le a \le q-1$, iar X_i este semnalul unu, care este un număr aleatoriu şi care se află în gama valorilor $1 \le X_i \le q-1$, totodată transformarea semnalului unu menţionat este ireversibilă, şi mijloace pentru generarea semnalului patru la ieşirea doi conectată la intrarea blocului (3) pentru păstrarea cheii secrete comune, totodată semnalul patru menţionat K_{ij} se descrie prin expresia $K_{ij} = Y_j^{X_i} (\mathrm{mod} q)$, unde Y_j corespunde semnalului doi, rezultatul transformării semnalului doi menţionat împreună cu semnalul unu menţionat prezintă cheia secretă comună;
- generatorul (6) al celei de-a doua chei secrete comune, a cărui intrare unu, pentru recepţia semnalului cinci, este conectată la ieşirea blocului (7) de introducere a cheii secrete, intrarea doi, pentru recepţia semnalului trei, este conectată la ieşirea unu a blocului (2), având mijloace pentru generarea semnalului doi la ieşirea unu conectată la intrarea doi a blocului (2), totodată semnalul doi menţionat Y_j se descrie prin expresia $Y_j = a^{X_j} (\mathrm{mod}\, q)$, unde X_j este semnalul cinci, care prezintă un număr aleatoriu, care se află în gama valorilor $1 \le X_j \le q-1$, transformarea semnalului cinci menţionat fiind ireversibilă, şi mijloace pentru generarea semnalului şase la ieşirea doi conectată la intrarea blocului (5) pentru păstrarea cheii secrete comune, totodată semnalul şase menţionat K_{ji} se descrie prin expresia $K_{ji} = Y_i^{X_j} (\mathrm{mod} q)$, rezultatul transformării semnalului trei împreună cu semnalul cinci menţionat prezentând cheia secretă comună, dispozitivul conţinând suplimentar:
- generatorul (9) de realizare a funcţiei Z_i, a cărui intrare unu, pentru recepţia semnalului şapte, este conectată la ieşirea blocului (8) de recepţionare a succesiunilor aleatorii de biţi C_i, intrarea doi, pentru recepţia semnalului patru, este conectată la ieşirea doi a blocului (2), având mijloace pentru generarea semnalului opt la ieşire, totodată semnalul opt menţionat Z_i se descrie prin expresia $Z_i = K_{ij} \oplus C_i$, unde C_i este semnalul şapte, care prezintă o succesiune aleatorie de biţi;
- generatorul (12) al semnalului C_{jr}, a cărui intrare unu, pentru recepţia semnalului patru, este conectată la intrarea doi a blocului (9), intrarea doi, pentru recepţia semnalului zece, este conectată la ieşirea blocului (10) pentru realizarea funcţiei, având mijloace pentru generarea semnalului C_{jr} la ieşirea conectată la intrarea unu a blocului (18) de verificare a semnăturii digitale şi prezintă o succesiune aleatorie a biţilor C_j restabilită, totodată $C_{jr} = K_{ij} \oplus Z_j$;
- generatorul (15) de realizare a primei semnături digitale S_i, a cărui intrare unu, pentru recepţia semnalului unsprezece, este conectată la ieşirea blocului (14) de introducere şi păstrare a identificatorului I_i, intrarea doi, pentru recepţia semnalului doisprezece, este conectată la ieşirea blocului (17) de introducere şi păstrare a identificatorului I_j, intrarea trei, pentru recepţia semnalului trei - la ieşirea unu a blocului (2), intrarea patru, pentru recepţia semnalului doi - la ieşirea unu a blocului (6), intrarea cinci, pentru recepţia semnalului şapte - la ieşirea blocului (8), şi mijloace pentru generarea semnalului treisprezece la ieşirea, care este conectată la intrarea doi a blocului (19) de verificare a semnăturii digitale, totodată semnalul treisprezece menţionat S_i se descrie prin expresia $S_i = DSA(HASH(I_i \| Y_i \| I_j \| Y_j \| C_i))$, unde I_i este semnalul unsprezece, care prezintă identificatorul utilizatorului *i*, I_j este semnalul doisprezece, care prezintă identificatorul utilizatorului *j*;
- generatorul (10) de realizare a funcţiei Z_j, a cărui intrare unu, pentru recepţia semnalului nouă, este conectată la ieşirea blocului (11) de recepţionare a succesiunilor aleatorii de biţi C_j, intrarea doi, pentru recepţia semnalului şase, este conectată la ieşirea doi a blocului (6), conţinând mijloace pentru generarea semnalului

zece la ieşirea, conectată la intrarea doi a blocului (12), totodată semnalul zece Z_j se descrie prin expresia $Z_j = K_{ij} \oplus C_j$, unde C_j este semnalul nouă, care prezintă o succesiune aleatorie de biţi;

- generatorul (13) al semnalului C_{ir}, a cărui intrare unu, pentru recepţia semnalului şase, este conectată la ieşirea doi a blocului (6), intrarea doi, pentru recepţia semnalului opt, este conectată la ieşirea blocului (9), conţinând mijloace pentru generarea semnalului C_{ir} la ieşirea conectată la intrarea unu a blocului (19), care prezintă o succesiune aleatorie de biţi C_i restabilită, totodată $C_{ir} = K_{ji} \oplus Z_i$;

- generatorul (16) de realizare a celei de-a doua semnături digitale S_j, a cărui intrare unu, pentru recepţia semnalului unsprezece, este conectată la ieşirea blocului (14), intrarea doi, pentru recepţia semnalului doisprezece - la ieşirea blocului (17), intrarea trei, pentru recepţia semnalului doi - la ieşirea unu a blocului (6), intrarea patru, pentru recepţia semnalului trei - la ieşirea unu a blocului (2), intrarea cinci, pentru recepţia semnalului nouă - la ieşirea blocului (11), având mijloace pentru generarea semnalului paisprezece la ieşirea care este conectată la intrarea doi a blocului (18), totodată semnalul paisprezece S_j se descrie prin expresia $S_j = DSA(HASH(I_i \| Y_i \| I_j \| Y_j \| C_j))$.

Rezultatul invenţiei solicitate este realizarea schimbului autentificat cu chei secrete prin canale deschise şi mărirea rezistenţei sistemului în întregime.

Astfel se rezolvă problema schimbului autentificat cu chei secrete prin canalul deschis şi majorării rezistenţei sistemului în întregime, întrucât parametrii C_i şi C_j sunt succesiuni aleatorii de biţi unice, iar operaţiunile $K_{ij} \oplus C_i$, $K_{ji} \oplus C_j$ prezintă "cifrul Vernam", care după cum se ştie, este absolut rezistent. Mai precis, în acest caz rezistenţa depinde de volumul de informaţie despre C_i şi C_j care poate fi "căpătată" din semnăturile S_i şi S_j. Însă, fiindcă în semnăturile S_i şi S_j în esenţă sunt prezente nu C_i şi C_j ca atare, dar "urmele" lor, obţinute cu ajutorul funcţiei unilaterale HASH şi algoritmului semnăturii digitale DSA, restaurarea cu ajutorul lor a succesiunilor C_i şi C_j practic nu este posibilă.

Esenţa invenţiei solicitate se explică cu ajutorul exemplelor de realizare a ei cu referinţe la desenul prezentat în fig.1. În fig. 1 este prezentată schema-bloc generalizată a dispozitivului pentru asigurarea schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţie.

Procedeul solicitat poate fi realizat cu ajutorul programelor de calculator sau dispozitivului de calcul, prezentat în schema-bloc din fig. 1, unde blocurile 1 şi 7 sunt dispozitive de introducere a cheii secrete; blocurile 2 şi 6 - dispozitive, care realizează funcţiile $Y_i = \alpha^{X_i} (\mathrm{mod}\ q)$, $K_{ij} = Y_j^{X_i} (\mathrm{mod}\ q)$ şi $Y_j = \alpha^{X_j} (\mathrm{mod}\ q)$, $K_{ji} = Y_i^{X_j} (\mathrm{mod}\ q)$, în mod corespunzător; blocurile 3 şi 5 - dispozitive pentru păstrarea cheii secrete comune, după schimbul cu datele nesecrete prin canalul de legătură deschis 4; blocurile 8 şi 11 - dispozitive pentru crearea succesiunilor aleatorii de biţi C_i şi C_j; blocurile 9 şi 10 - dispozitive care realizează funcţiile $Z_i=K_{ij}\oplus C_i$ şi $Z_j=K_{ji}\oplus C_j$ în mod corespunzător; blocurile 12 şi 13 - dispozitive care realizează funcţiile $C_{jr}=K_{ij}\oplus Z_j$ şi $C_{ir}=K_{ji}\oplus Z_i$ în mod corespunzător; blocurile 14 şi 17 - dispozitive pentru introducerea şi păstrarea identificatorilor I_i şi I_j; blocurile 15 şi 16 - dispozitive care realizează funcţiile $S_i=DSA(HASH(I_i\|Y_i\|I_j\|Y_j\|C_i))$ şi $S_j=DSA(HASH(I_i\|Y_i\|I_j\|Y_j\|C_j))$, respectiv; blocurile 18 şi 19 execută verificarea semnăturii digitale, iar semnalele la ieşirile lor Q_i, Q_j reprezintă rezultatul acestei verificări.

În fig. 1 blocurile sunt prezentate în felul următor: intrările şi ieşirile blocurilor sunt arătate cu săgeţi orientate spre bloc sau, corespunzător, de la el, iar marcarea intrărilor şi ieşirilor S1…S14 corespunde numerelor semnalelor, care se lansează la intrările blocurilor sau se generează de ele.

Este necesar de remarcat că, în esenţă, dispozitivul constă din două părţi identice, distribuite în sens diferit al canalului de legătură. Cu alte cuvinte, în timpul funcţionării participă ambele părţi, adică utilizatorul *i* şi utilizatorul *j*.

În conformitate cu schema-bloc, prezentată în fig. 1 dispozitivul funcţionează în felul următor:

- utilizatorul *i* creează cheia secretă aleatorie X_i, care prezintă semnalul unu şi o introduce în blocul 1; cu ajutorul generatorului 2 el calculează cheia deschisă $Y_i = \alpha^{X_i} (\mathrm{mod}\ q)$, care corespunde cheii secrete şi care prezintă semnalul trei; cheia deschisă împreună cu identificatorul său I_i, care prezintă semnalul unsprezece din blocul 14 utilizatorul *i* o transmite utilizatorului *j*;

- utilizatorul *j* creează cheia sa secretă aleatore X_j, care este semnalul cinci, o introduce în blocul 7 şi cu ajutorul generatorului 6 calculează cheia deschisă $Y_j = \alpha^{X_j} (\mathrm{mod}\ q)$, care corespunde cheii secrete şi este semnalul doi. În afară de aceasta, el cu ajutorul generatorului 6, calculează cheia sa secretă comună $K_{ji} = Y_i^{X_j} (\mathrm{mod}\ q)$, pe care o introduce în blocul 5. Apoi în blocul 11 el creează succesiunea aleatorie de biţi C_j, care este semnalul nouă şi calculează cu ajutorul blocului 10 valoarea $Z_j=K_{ji}\oplus C_j$, care este semnalul zece, şi după aceasta utilizatorul *j* calculează cu ajutorul generatorului 16 semnătura digitală

S_j=*DSA*(*HASH*(I_i||Y_i||I_j||Y_j||C_j)), care este semnalul paisprezece. I_j care se alimentează din blocul 17 şi care este semnalul doisprezece, Y_j, Z_j şi S_j utilizatorul *j* le transmite utilizatorului *i* prin canalul deschis de legătură 4;

- utilizatorul *i* calculează cu ajutorul blocului 2 cheia sa secretă comună K_{ij}, care este semnalul patru, folosind pentru aceasta Y_j şi cheia sa secretă X_i în conformitate cu expresia $K_{ij} = Y_j^{X_i} \pmod q$, o introduce în blocul 3, după care el obţine cu ajutorul blocului 12 valoarea C_{jr}=K_{ij}⊕Z_j şi verifică semnătura digitală a parametrilor I_i, Y_i, I_j, Y_j şi C_j în blocul 18. Apoi în blocul 8 el creează succesiunea aleatorie de biţi C_i, care este semnalul şapte, cu ajutorul blocului 9 calculează Z_i=K_{ij}⊕C_i, care este semnalul opt, iar cu ajutorul generatorului 15 calculează semnătura digitală S_i=*DSA*(*HASH*(I_i||Y_i||I_j||Y_j||C_i)), care este semnalul treisprezece, şi transmite valorile Z_i, S_i prin canalul deschis 4 utilizatorului *j*;

- utilizatorul *j*, folosind cheia sa secretă comună K_{ji} din blocul 5 calculează cu ajutorul blocului 13 valoarea C_{ir}=K_{ji}⊕Z_i=C_i şi în blocul 19 verifică semnătura digitală a parametrilor I_i, Y_i, I_j, Y_j şi C_i, îndeplinită de utilizatorul *i*.

Ca rezultat al îndeplinirii acestor paşi în blocurile 3 şi 5, care se află la utilizatorii *i* şi *j* corespunzător, se obţine cheia secretă comună K_{ij}(K_{ji}). Dacă ambele semnale, lansate la ieşirile blocurilor 18 şi 19 au valoarea TRUE, schimbul autentificat cu cheia secretă K_{ij} prin canalul deschis 4 s-a efectuat cu succes. În caz contrar, chiar dacă unul din semnalele de ieşire ale blocurilor 18 sau 19 are valoarea FALSE, schimbul cu cheia secretă comună nu a fost realizat.

(57) Revendicări:

1. Procedeu de asigurare a schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţie, care constă în generarea cheii secrete comune $K_{ij} = Y_i^{X_j} \pmod q = K_{ji} = Y_j^{X_i} \pmod q$ pentru transmiţătorul *i* şi receptorul *j* cu ajutorul funcţiei discrete de ridicare la putere $f(x) = \alpha^x \pmod q$, calcularea şi schimbul cu cheile deschise $Y_i = a^{X_i} \pmod q$, $Y_j = a^{X_j} \pmod q$, **caracterizat prin aceea că** în timpul schimbului cu cheile deschise între transmiţătorul i şi receptorul j se folosesc suplimentar identificatorii lor I_i şi I_j, se creează succesiuni aleatorii de biţi C_i şi C_j, se calculează valorile $Z_i = K_{ij} \oplus C_i$, $Z_j = K_{ji} \oplus C_j$ şi semnăturile digitale $S_i = DSA(HASH(I_i \| Y_i \| I_j \| Y_j \| C_i))$, $S_j = DSA(HASH(I_i \| Y_i \| I_j \| Y_j \| C_j))$, transmiţătorul i şi receptorul j se schimbă cu valorile I_i, Z_i, S_i şi I_j, Z_j, S_j, folosind cheia secretă comună K_{ij} se calculează $C_{ir} = K_{ij} \oplus Z_i$, $C_{jr} = K_{ij} \oplus Z_j$, se verifică semnătura digitală a parametrilor I_i, Y_i, I_j, Y_j, C_i şi I_i, Y_i, I_j, Y_j, C_j.

2. Dispozitiv pentru asigurarea schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţie, care conţine:

- generatorul (2) al primei chei secrete comune, a cărui intrare unu, pentru recepţia semnalului lansat unu, este conectată cu ieşirea blocului (1) de introducere a cheii secrete, şi intrarea doi, pentru recepţia semnalului doi, este conectată la ieşirea unu a blocului (6) de realizare a funcţiilor, având mijloace pentru generarea semnalului trei la ieşirea unu, conectată la intrarea doi a blocului (6), totodată semnalul trei menţionat Y_i se descrie prin expresia $Y_i = a^{X_i} \pmod q$, unde q este un număr prim mare, a – un număr aleatoriu, care se află în gama valorilor $1 \le a \le q-1$, iar X_i este semnalul unu, care este un număr aleatoriu şi care se află în gama valorilor $1 \le X_i \le q-1$, totodată transformarea semnalului unu menţionat este ireversibilă, şi mijloace pentru generarea semnalului patru la ieşirea doi conectată la intrarea blocului (3) pentru păstrarea cheii secrete comune, totodată semnalul patru menţionat K_{ij} se descrie prin expresia $K_{ij} = Y_j^{X_i} \pmod q$, unde Y_j corespunde semnalului doi, rezultatul transformării semnalului doi menţionat împreună cu semnalul unu menţionat prezintă cheia secretă comună;

- generatorul (6) al celei de-a doua chei secrete comune, a cărui intrare unu, pentru recepţia semnalului cinci, este conectată la ieşirea blocului (7) de introducere a cheii secrete, intrarea doi, pentru recepţia semnalului trei, este conectată la ieşirea unu a blocului (2), având mijloace pentru generarea semnalului doi la ieşirea unu conectată la intrarea doi a blocului (2), totodată semnalul doi menţionat Y_j se descrie prin expresia $Y_j = a^{X_j} \pmod q$, unde X_j este semnalul cinci, care prezintă un număr aleatoriu, care se află în gama

valorilor $1 \le X_j \le q-1$, transformarea semnalului cinci menţionat fiind ireversibilă, şi mijloace pentru generarea semnalului şase la ieşirea doi conectată la intrarea blocului (5) pentru păstrarea cheii secrete comune, totodată semnalul şase menţionat K_{ji} se descrie prin expresia $K_{ji} = Y_i^{X_j} (\mathrm{mod} q)$, rezultatul transformării semnalului trei împreună cu semnalul cinci menţionat prezentând cheia secretă comună, **caracterizat prin aceea că** dispozitivul conţine suplimentar:

- generatorul (9) de realizare a funcţiei Z_i, a cărui intrare unu, pentru recepţia semnalului şapte, este conectată la ieşirea blocului (8) de recepţionare a succesiunilor aleatorii de biţi C_i, intrarea doi, pentru recepţia semnalului patru, este conectată la ieşirea doi a blocului (2), având mijloace pentru generarea semnalului opt la ieşire, totodată semnalul opt menţionat Z_i se descrie prin expresia $Z_i = K_{ij} \oplus C_i$, unde C_i este semnalul şapte, care prezintă o succesiune aleatorie de biţi;

- generatorul (12) al semnalului C_{jr}, a cărui intrare unu, pentru recepţia semnalului patru, este conectată la intrarea doi a blocului (9), intrarea doi, pentru recepţia semnalului zece, este conectată la ieşirea blocului (10) pentru realizarea funcţiei, având mijloace pentru generarea semnalului C_{jr} la ieşirea conectată la intrarea unu a blocului (18) de verificare a semnăturii digitale şi prezintă o succesiune aleatorie a biţilor C_j restabilită, totodată $C_{jr} = K_{ij} \oplus Z_j$;

- generatorul (15) de realizare a primei semnături digitale S_i, a cărui intrare unu, pentru recepţia semnalului unsprezece, este conectată la ieşirea blocului (14) de introducere şi păstrare a identificatorului I_i, intrarea doi, pentru recepţia semnalului doisprezece, este conectată la ieşirea blocului (17) de introducere şi păstrare a identificatorului I_j, intrarea trei, pentru recepţia semnalului trei - la ieşirea unu a blocului (2), intrarea patru, pentru recepţia semnalului doi - la ieşirea unu a blocului (6), intrarea cinci, pentru recepţia semnalului şapte - la ieşirea blocului (8), şi mijloace pentru generarea semnalului treisprezece la ieşirea, care este conectată la intrarea doi a blocului (19) de verificare a semnăturii digitale, totodată semnalul treisprezece menţionat S_i se descrie prin expresia $S_i = DSA(HASH(I_i \| Y_i \| I_j \| Y_j \| C_i))$, unde I_i este semnalul unsprezece, care prezintă identificatorul utilizatorului i, I_j este semnalul doisprezece, care prezintă identificatorul utilizatorului j;

- generatorul (10) de realizare a funcţiei Z_j, a cărui intrare unu, pentru recepţia semnalului nouă, este conectată la ieşirea blocului (11) de recepţionare a succesiunilor aleatorii de biţi C_j, intrarea doi, pentru recepţia semnalului şase, este conectată la ieşirea doi a blocului (6), conţinând mijloace pentru generarea semnalului zece la ieşirea, conectată la intrarea doi a blocului (12), totodată semnalul zece Z_j se descrie prin expresia $Z_j = K_{ij} \oplus C_j$, unde C_j este semnalul nouă, care prezintă o succesiune aleatorie de biţi;

- generatorul (13) al semnalului C_{ir}, a cărui intrare unu, pentru recepţia semnalului şase, este conectată la ieşirea doi a blocului (6), intrarea doi, pentru recepţia semnalului opt, este conectată la ieşirea blocului (9), conţinând mijloace pentru generarea semnalului C_{ir} la ieşirea conectată la intrarea unu a blocului (19), care prezintă o succesiune aleatorie de biţi C_i restabilită, totodată $C_{ir} = K_{ji} \oplus Z_i$;

- generatorul (16) de realizare a celei de-a doua semnături digitale S_j, a cărui intrare unu, pentru recepţia semnalului unsprezece, este conectată la ieşirea blocului (14), intrarea doi, pentru recepţia semnalului doisprezece - la ieşirea blocului (17), intrarea trei, pentru recepţia semnalului doi - la ieşirea unu a blocului (6), intrarea patru, pentru recepţia semnalului trei - la ieşirea unu a blocului (2), intrarea cinci, pentru recepţia semnalului nouă - la ieşirea blocului (11), având mijloace pentru generarea semnalului paisprezece la ieşirea care este conectată la intrarea doi a blocului (18), totodată semnalul paisprezece S_j se descrie prin expresia $S_j = DSA(HASH(I_i \| Y_i \| I_j \| Y_j \| C_j))$.

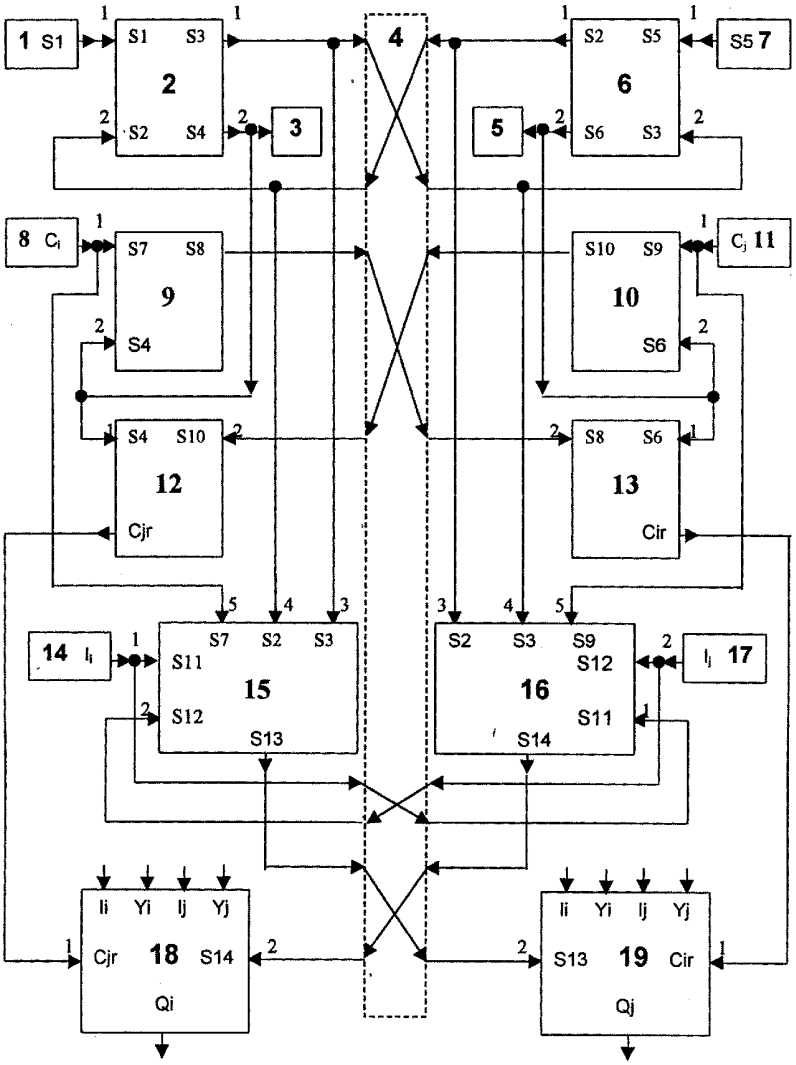
(56) Referinţe bibliografice:

1. W. Diffie and M.E. Hellman, "New Direction in Cryptography ", IEEE Trans. On Info. Theory, Vol. IT-22,pag. 644-654, Nov. , 1976
2. US 4200770 B

Şef Secţie: COZMA Valeriu

Examinator: NASTAS Xenia

Redactor: ANDRIUŢĂ Victoria


1 S1
S1 S3
2
S2 S4
3
4
S2 S5
S5 7
6
5
S6 S3
8 Ci
S7 S8
9
S4
S10 S9
10
S6
Cj 11
S4 S10
12
Cjr
S8 S6
13
Cir
14 Ii
S7 S2 S3
S11
15
S12
S13
S2 S3 S9
S12
16
S11
S14
Ij 17
Ii Yi Ij Yj
Cjr
18
S14
Qi
Ii Yi Ij Yj
S13
19
Cir
Qj

RAPORT DE DOCUMENTARE

(21) Nr. depozit: a 2000 0090 (22) Data depozit: 2000.04.25	(85) Data fazei naţionale PCT: (86) Cerere internaţională PCT:

Prioritatea invocată :
(31) nr.: 32) data : 33) ţara :
(51) Int. Cl. (7) : H 04 L 9/00; H 04 K 1/00
Alţi indici de clasificare:
(54) **Titlul** : Procedeu şi dispozitiv de asigurare a schimbului autentificat cu chei secrete prin canale deschise de telecomunicaţie
(71) Solicitantul : Compania DEKART, S.R.L., MD
Termeni caracteristici : procedeu şi dispozitiv

I. Minimul de documente consultate (sistema clasificării şi indicii de clasificare)

C.I.B. 7:
MD 1994-2000
EA 1996-2000

II. Documente considerate ca relevante

Categoria*	Date de identificare ale documentelor citate si indicarea pasajelor pertinente	Numărul revendicării vizate
-	-	-

☐ **Documentele următoare sunt indicate în continuare a rubricii II**	☐ **Informaţia referitoare la brevete paralele se anexează**
*** categoriile speciale ale documentelor consultate:**	**P** - document publicat inainte de data depozitului naţional reglementat dar după data priorităţii invocate
A - document care defineşte statutul general al tehnicii	**T -** document publicat după data depozitului sau a priorităţii invocate, care nu aparţine stadiului pertinent al tehnicii, dar care este citat pentru a pune în evidenţa principiul sau teoria care conţine baza invenţiei
E - document anterior dar publicat la data de depozit naţional reglementar sau după aceasta data	**X** - document de relevanţă deosebită: invenţia revendicată nu poate fu considerată nouă sau implicând activitate inventivă
L - document care poate pune în discuţie data priorităţii invocate, poate contribui la data publicării altor divulgări sau pentru un motiv expres (se va indica motivul)	**Y** - document de relevanţă deosebită: invenţia revendicată nu poate fu considerată ca implicând activitate inventivă când documentul este asociat cu unul sau mai multe alte documente de aceiaşi natură, aceasta combinaţie fiind evidentă pentru o persoană de specialitate
O - document referitor la o divulgare orală, un act de folosire, la o expunere sau orice altă	**&** - document care face parte din aceiaşi familie de documente

Data efectuării documentării 2000.08. 01

Examinatorul Xenia Nastas

itoare la brevete paralele		(21) Nr. depozit:	
Date de identificare ale documentelor citate in raport	Data publicării	**Brevete paralele**	Data publicării
1	2	3	4