(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) RO 132697 A2
(51) Int.Cl.
H03M 7/00 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2016 01062**

(22) Data de depozit: **30/12/2016**

(41) Data publicării cererii:
29/06/2018 BOPI nr. **6/2018**

(71) Solicitant:
• **NICULESCU IONEL GABRIEL**,
ŞOS.ALEXANDRIEI NR.94, BL.PC 11, SC.A, ET.4, AP.17, SECTOR 5, BUCUREŞTI, B, RO

(72) Inventatori:
• **NICULESCU IONEL GABRIEL**,
ŞOS. ALEXANDRIEI NR. 94, BL. PC11, SC. A, ET. 4, AP. 17, SECTOR 5, BUCUREŞTI, B, RO

(54) # METODĂ PENTRU PROTEJAREA CONFIDENŢIALITĂŢII DATELOR DIGITALE

(57) **Rezumat:**

Invenţia se referă la o metodă pentru protejarea confidenţialităţii datelor digitale. Metoda conform invenţiei utilizează pentru codificarea datelor un tabel de corespondenţe dezordonat aleatoriu, care cuprinde: o coloană cu înregistrări, cu texte ordonate în logica normală a conţinutului de informaţii şi date ale acestora, o coloană cu numerotarea ordonată crescător, consecutiv, a înregistrărilor cu texte, şi o coloană cu numere dezordonate aleatoriu. Datele codificate pot fi salvate pe un HDD intern sau într-o memorie amovibilă, pot fi transmise unor aplicaţii software care rulează pe staţia de lucru, sau pot fi transmise în reţea, iar pentru a citi textele codificate, utilizatorul/primitorul datelor trebuie să deţină o copie a tabelului de corespondenţe dezordonate aleatoriu, care va fi folosit de o aplicaţie informatică pentru restabilirea ordinii corecte a înregistrărilor din tabel.

Revendicări: 1
Figuri: 1

METODĂ PENTRU PROTEJAREA CONFIDENŢIALITĂŢII DATELOR DIGITALE

Tabel de corespondenţă dezordonat aleator

coloană cu numere în format zecimal ordonate crescător consecutiv începând cu un număr de start	coloană cu numere în format zecimal dezordonate aleator începând cu un număr de start	etapele procedeului confidenţial pentru "producerea sucului pe bază de cofeină"
1000	7497	text-etapa1
1001	7510	text-etapa2
1002	7501	text-etapa3
1003	7493	text-etapa4
1004	7513	text-etapa5
1005	458	text-etapa6
1006	7511	text-etapa7
1007	7509	text-etapa8
1008	7492	text-etapa9
1009	7520	text-etapa10
1010	7502	text-etapa11
1011	4262	text-etapa12
1012	4271	text-etapa13
1013	4258	text-etapa14
1014	4273	text-etapa15
1015	1236	text-etapa16
1016	4250	text-etapa17
1017	4270	text-etapa18
1018	4257	text-etapa19
1019	4259	text-etapa20
1020	4261	text-etapa21
1021	4248	text-etapa22
1022	4269	text-etapa23
1023	4272	text-etapa24
1024	10238	text-etapa25
1025	4253	text-etapa26
1026	4276	text-etapa27
1027	4260	text-etapa28
1028	4252	text-etapa29
1029	4268	text-etapa30
1030	4254	text-etapa31

RO 132697 A2

METODĂ PENTRU PROTEJAREA CONFIDENŢIALITĂŢII DATELOR DIGITALE

DESCRIERE

Invenţia se referă la o metodă pe care o numim "protejare prin ordine aleatoare" pentru protejarea datelor digitale utilizând într-un mod inovativ metoda descrisă în cererea de brevet de invenţie "PROCEDEU ŞI SISTEM ELECTRONIC PENTRU CODIFICAREA ŞI DECODIFICAREA DIGITALĂ A DATELOR ÎN ECHIPAMENTE INFORMATICE, DE AUTOMATIZARE ŞI DE COMUNICAŢII" publicată in BOPI nr.7 din 2016 pag. 41, metodă utilizată cu scopul protejării datelor digitale confidenţiale fară utilizarea de parole sau a tehnicilor de criptare ci prin metoda care face obiectul acestei invenţii.

Este cunoscut procedeul si echipamentul descrise in cererea de brevet cu nr. OSIM a2014 01000 şi nr. PCT/RO2015/050014 şi publicată internaţional cu nr. WO 2016/130037, a căror titular suntem, care fololseşte un algoritm simplu pentru codificare/decodificare în cadrul căruia are loc o operaţie simplă de înlocuire a unui număr binar cu mulţi biţi cu unul cu mai puţini biţi, şirurile (numerele) cu biţi, cel de înlocuit şi înlocuitorul său, utilizate în procedeul de codificare fiind plasate într-un tabel de corespondenţă.

Sunt cunoscute de asemeni metode de protejare a datelor confidenţiale fie folosind doar parole fie utilizând parole şi metode de criptare simetrică sau asimetrică bazate pe utilizarea unor algoritmi de criptare. Aceste metode au dezavantaje astfel:

- Parolele utilizate singure protejează doar accesul la fişiere şi directori nu şi conţinutul acestora şi pot fi sparte utilizând

diverse tehnici şi mijloace informatice, parolele foarte performante fiind dificil de memorat. În plus conţinutul fişierului parolat poate fi aflat cu mijloace adecvate relativ simple şi la îndemână chiar şi pentru nespecialişti.

- Metodele de criptare simetrică şi asimetrică utilzează şi ele parole cu neajunsurile menţionate la punctul anterior. De asemeni fişierele criptate sunt expuse posibilităţii de a fi decriptate prin mijloace informatice care folosesc o putere de calcul adecvată (aplicaţii informatice care folosesc un mare număr de calculatoare pentru decriptare frauduloasă). Aceasta este posibil deoarece un element al metodei de securizare este public şi anume algoritmul de criptare.

Scopul invenţiei este de a oferii o alternativă care să fie utilizată în domeniul protejării datelor digitale confidenţiale care să elimine neajunsurile prezentate.

Metoda "protejare prin ordine aleatoare" pentru protejarea confidenţialităţii datelor digitale utilizează "procedeul şi sistemul electronic pentru codificarea şi decodificarea digitală a datelor în echipamente informatice, de automatizare şi de comunicaţii" care va fi folosit în modul inovativ propus de invenţie prin utilizarea unui "tabel de corespondenţe dezordonat aleator". Astfel dacă tabelul de corespondenţă conţine articolele, paragrafele şi aliniatele unei legi din sistemul legislativ, de exemplu, ordonate prin numerotarea acestora în mod crescător consecutiv uzual, pentru asigurarea confidenţialităţii apariţiei acestor articole, paragrafe şi aliniate într-un text transmis sau depozitat electronic digital pentru care există raţiunea confidenţialităţii, se va utiliza un "tabel de corespondenţe dezordonat aleator" care va conţine paragrafele şi aliniatele legii respective ordonate aleator sau ordonate dupe alte reguli. Astfel "tabelul de corespondenţe dezordonat aleator" va conţine:

- o coloană cu articolele, paragrafele şi aliniatele legii ordonate crescător consecutiv uzual, aşa cum a fost publicată legea,
- o coloană cu numere binare pentru "codificarea generalizată

1număr=1şir_de_numere" cu ordonare crescătoare consecutivă (n+1, n+2, n+3 etc., unde n este un număr de start) a acestora (conform documentaţiei din cererea de brevet a2014 01000) şi

- o coloană destinată codurilor (numerelor binare) pentru înlocuire (codificare) protejată cu metoda "protejare prin ordine aleatoare" unde se vor afla numere binare începând cu un număr de start ales convenabil, numere binare ordonate fie într-o ordine stabilită pe baza unei reguli sau formule de ordonare alta decât cea crescător consecutivă fie ordonate aleator, adică o ordine întâmplătoare generată informatic.

Pentru codificarea protejată a datelor cu metoda "protejare prin ordine aleatoare" se va utiliza un "tabel de corespondenţe dezordonat aleator" care va fi încărcat în RAM sau într-o memorie cache, dedicată sau nu, a microprocesorului, în vederea codificării protejate cu această metodă, de pe un dispozitiv de memorie digitală portabil cu regim de utilizare de cheie de protecţie digitală, gen token, cum ar fi o memorie USB, un miniCD etc. Datele codificate protejat cu metoda "protejare prin ordine aleatoare" vor fi salvate pe un HDD intern sau pe o memorie amovibilă, vor fi transmise la alte aplicaţii SW care rulează pe staţia de lucru sau vor fi transmise în reţea, pe Internet sau prin e-mail sau altă formă de mesagerie digitală. Pentru a putea citi textele codificate protejat cu metoda "protejare prin ordine aleatoare" este nevoie ca utilizatorul/primitorul să deţină o copie a "tabelului de corespondenţe dezordonat aleator" care va fi folosit de o aplicaţie informatică pentru restabilirea ordinii corecte a înregistrărilor din tabel.

Avantajele invenţiei constau în:

- simplitatea implementării care este la îndemâna oricui fără a necesita cunoştinţe de specialitate,
- oferă grad superior de protecţie a datelor digitale şi un sentiment superior de protecţie deoarece absolut toate elementele utilizate pentru protecţie sunt ştiute numai şi

numai de proprietar sau de persoanele eligibile să folosească "tabelul de corespondenţe dezordonat aleator".

- grad superior de protecţie a datelor digitale deoarece metoda permite implementări care să nu poată fi compromise decât print furt sau trădare. Descifrarea unui text este imposibilă în implementări foarte performante şi înalt disciplinate, indiferent câtă putere de calcul ar exista şi indiferent cât de mare ar fi aceasta.

Nivelul de protecţie poate creşte combinând metoda "protejare prin ordine aleatoare" cu tehnici de protecţie tradiţionale cum ar fi parolele sau criptarea pentru protejarea "tabelul de corespondenţe dezordonat aleator" sau prin protejarea accesului la memoria portabilă care păstrează acest tabel dar şi cu metode noi de protecţie.

Se dă în continuare un exemplu de implementare a invenţiei în legătură cu Fig.1.

Pentru protejarea textului cu conţinutul procedeului confidenţial pentru "producerea sucului pe bază de cofeină" ce urmează a fi transmis pe cale electronică la un destinatar, procedeu care se realizează în 31 de etape, se utilizează o implementare a metodei din cererea de brevet a2014 01000 în care se utilizează ca tabel de corespondenţă, în cadrul realizării algoritmului "codificarea generalizată 1număr=1şir_de_numere", "tabelul de corespondenţe dezordonat aleator" din Fig.1.

METODĂ PENTRU PROTEJAREA CONFIDENŢIALITĂŢII DATELOR DIGITALE

REVENDICĂRI

1. Metodă pentru protejarea confidenţialităţii datelor digitale care utilizează "PROCEDEUL ŞI SISTEMUL ELECTRONIC PENTRU CODIFICAREA ŞI DECODIFICAREA DIGITALĂ A DATELOR ÎN ECHIPAMENTE INFORMATICE, DE AUTOMATIZARE ŞI DE COMUNICAŢII" descrisă în cererea de brevet de invenţie a2014 01000 şi în cererea de brevet internaţional PCT/RO2015/050014 publicată internaţional cu nr. WO 2016/130037, a căror titular suntem, **caracterizată prin aceea că** foloseşte ca tabel de corespondenţă un "tabel de corespondenţe dezordonat aleator" care conţine:
   - o coloană cu înregistrări cu texte ordonate în logica normală a conţinutului de informaţii şi date a acestora,
   - o coloană cu numere binare pentru "codificarea generalizată 1număr=1şir_de_numere" cu ordonare crescătoare consecutivă (n+1, n+2, n+3 etc., unde n este un număr de start) şi
   - o coloană destinată codurilor (numerelor binare) pentru înlocuire (codificare generalizată 1număr=1şir_de_numere) protejată cu metoda propusă unde se vor afla numere binare începând cu un număr de start ales convenabil, numere binare ordonate, fie într-o ordine stabilită pe baza unei reguli sau formule de ordonare alta decât cea crescător consecutivă fie ordonate aleator, adică o ordine întâmplătoare generată informatic.

METODĂ PENTRU PROTEJAREA CONFIDENŢIALITĂŢII DATELOR DIGITALE

DESENE

Tabel de corespondenţă dezordonat aleator		
coloană cu numere în format zecimal ordonate crescător consecutiv începând cu un număr de start	**coloană cu numere în format zecimal dezordonate aleator începând cu un număr de start**	**etapele procedeului confidenţial pentru "producerea sucului pe bază de cofeină"**
1000	7497	text-etapa1
1001	7510	text-etapa2
1002	7501	text-etapa3
1003	7493	text-etapa4
1004	7513	text-etapa5
1005	458	text-etapa6
1006	7511	text-etapa7
1007	7509	text-etapa8
1008	7492	text-etapa9
1009	7520	text-etapa10
1010	7502	text-etapa11
1011	4262	text-etapa12
1012	4271	text-etapa13
1013	4258	text-etapa14
1014	4273	text-etapa15
1015	1236	text-etapa16
1016	4250	text-etapa17
1017	4270	text-etapa18
1018	4257	text-etapa19
1019	4259	text-etapa20
1020	4261	text-etapa21
1021	4248	text-etapa22
1022	4269	text-etapa23
1023	4272	text-etapa24
1024	10238	text-etapa25
1025	4253	text-etapa26
1026	4276	text-etapa27
1027	4260	text-etapa28
1028	4252	text-etapa29
1029	4268	text-etapa30
1030	4254	text-etapa31

Fig. 1