Coliziuni ale funcției de dispersie SHA-1 în mecanismul de semnătură electronică

Viorel Malcoci
Școala doctorală Științe Fizice și Inginerești
Institutul de Cercetare și Inovare al USM
Chișinău, Republica Moldova
vioacropolis@gmail.com

Rezumat. Lucrarea reprezentă o sinteză a vulnerabilităților funcției de dispersie SHA-1 și analiza utilizării acestei funcții în mecanismul de semnătură electronică la nivel național. În rezultat sunt înaintate propuneri pentru sporirea nivelului de securitate a funcției de generare a amprentei digitale în mecanismul de semnătură electronică.

Termeni cheie. Coliziuni, funcție de dispersie, amprenta digitală, SHA-1, semnătura electronică.

I. INTRODUCERE

Semnătura electronică oferă un prototip criptografic analogic cu semnătura ologrfă, dar care asigură o securitate mult mai avansată. În fapt, semnătura electronică este un instrument acceptat, din punct de vedere legal, în majoritatea țărilor, pentru semnarea documentelor electronice, certificarea tranzacțiilor electronice, autentificarea deținătorilor și în alte raporturi juridice.

Semnătura electronică permite distribuirea și transmiterea securizată a cheilor publice prin canale publice legalizate, servind astfel ca temelie pentru criptografia cu chei publice.

Semnătura electronică reprezintă o soluție sigură pentru realizarea *autentificării* și garantării *integrității* datelor.

Un alt obiectiv de bază ale securității informației care poate fi realizat prin intermediul semnăturii electronice este *non-repudierea* datelor, ceea ce înseamnă că o entitatea care a semnat și a emis datele respective nu poate nega acest fapt, iar oricare altă entitate poate ușor verifica acest lucru.

În esența sa, *semnătura electronică este o consecutivitate de cifre binare de o lungime fixă, calculată după anumite reguli prin funcția unidirecțională aplicată mesajului M destinat semnării, având ca parametru cheia privată a entității emitente pentru crearea semnăturii electronice și cheia publică pentru verificarea ei.*

Prin urmare, la baza creării semnăturii electronice se află perechea de chei și funcția unidirecțională *H(M),* utilizată pentru *obținerea amprentei digitale de o lungime fixă a unui mesaj de o lungime arbitrară.* Ulterior amprenta digitală obținută este utilizată în calitate de intrare pentru funcția de semnare.

II. SCHEMA DE SEMNĂTURĂ ELECTRONICĂ

Cum a fost menționat mai sus, semnătura electronică este o valoare binară prin care identitatea entității deținătoare se asociază cu un mesaj. O schemă de semnătură electronică constă din trei algoritmi:

- *Algoritmul* de generare a perechii de chei – K_{Pub}, K_{Priv} (cheia publică și cheia privată);
- *Algoritmul* de semnare, care se efectuează cu ajutorul cheii private K_{Priv};
- *Algoritmul* de verificare, care în baza mesajului primit, a semnăturii electronice a acestui mesaj și a cheii publice K_{Pub} validează semnătura electronică [[1], p. 109].

Există mai multe modalități de realizare a algoritmului de semnare/formare a semnăturii electronice. Însă, din punct de vedere al eficienței, cea mai practicată pentru autentificarea și semnarea documentelor este *semnătura electronică cu anexă.* În acest caz, mesajul nu poate fi recuperat din semnătura electronică, el fiind atașat ca anexă la semnătura electronică. Această modalitate presupune utilizarea funcției unidirecționale de tip *hash* pentru obținerea *amprentei digitale* a mesajului, semnătura electronică fiind apoi aplicată doar amprentei digitale a mesajului. În această schemă clasică de semnătură electronică se presupune că *entitatea emitentă cunoaște conținutul documentului care este semnat, iar entitatea receptoare cunoaște cheia publică de verificare și poate verifica corectitudinea aplicării semnăturii electronice* în orice moment, fără a cere permisiunea sau implicarea entității emițătoare.

Pentru implementarea acestei scheme de semnătură electronică, pe lângă algoritmii sus menționați de semnare și verificare a semnăturii, mai sunt necesare proceduri de soluționare a contradicțiilor, prin care o entitate emitentă a mesajului semnat să nu poată refuza recunoașterea semnăturii. În practică acest lucru este realizat prin aplicarea mecanismelor de garantare a autenticității de către așa numitele *entități terțe de încredere* sau *centre de certificare*.

Algoritmii utilizați în schema de semnătură electronică au la bază mijloace criptografice, care asigură autenticitatea informației. Prin urmare, entitatea receptoare poate ușor demonstra, că documentul semnat aparține entității emițătoare, iar entitatea emițătoare nu va putea nega acest fapt. Semnătura electronică este foarte greu de falsificat, fapt ce permite încrederea că semnătura aplicată mesajului, poate aparține doar entități care a semnat acest mesaj. Și, deoarece semnătura electronică este parte indispensabilă a documentului semnat, nimeni altcineva nu poate modifica documentul astfel, încât acest fapt să rămână neobservat. În acest sens, orice entitate care deține modelul de semnătura electronică se poate încredința în autenticitatea documentului.

În concluzie, putem menționa că schema de semnătură electronică are la bază mai multe mijloace criptografice, unul din ele fiind funcția unidirecțională *H(M)* (funcția de dispersie).

III. FUNCȚII DE DISPERSIE

Dacă să reprezentăm printr-o relație matematică calculul semnăturii electronice, atunci această relație ar arăta în felul următor:

$$Sign=f(H(M), K_{Priv}) \quad (1)$$

unde, *M* este conținutul mesajul, K_{Priv} cheia privată a entității emițătoare, *H(M)* – funcția de dispersie.

Astfel, se poate observa că mecanismul de semnătură electronică în mare parte se bazează pe funcții unidirecționale, de aici și vine necesitatea studierii acestor funcții.

O funcție unidirecțională poate fi definită astfel:

- fiind *dat x, este ușor de calculat f(x);*
- fiind *dat f(x), este greu/practic imposibil de calculat x.* [[2], p. 226].

Această caracteristica de bază a funcțiilor unidirecționale face imposibilă determinarea datelor inițiale din rezultatul funcției, ceea ce practic semnifică imposibilitatea falsificării semnături electronice.

Funcția de dispersie, numită și funcția *hash*, este o funcție unidirecțională criptografică care produce o valoare de lungimea fixă *n* pentru orice lungime a mesajului de intrare. Funcția hash mai este numită *amprentă digitală a mesajului de intrare*. O funcție hash trebuie să corespundă următoarelor criterii de securitate:

- Rezistența *imaginii* – având *h* o ieșire a funcției de dispersie este practic imposibil de a găsi un mesaj *M* astfel încât *h=H(M)*;
- Rezistența *imaginii secundare* – având un mesaj *M* și rezultatul funcției *H(M)* este practic imposibil de a găsi un alt mesaj *M′* astfel încât rezultatul funcției ambelor mesaje să corespundă *H(M)=H(M′)*;
- Rezistența *la coliziune* – este practic imposibil de a găsi o pereche de mesaje *M* și *M′* astfel, încât rezultatul funcției să coincidă *H(M)=H(M′)*.

O coliziune apare în momentul în care amprenta digitală pentru diferite mesaje este identică. În principiu coliziuni sunt posibile, deoarece mulțimea mesajelor este practic infinită față de mulțimea de valori a amprentei digitale care se limitează la 2^n, unde *n* – este lungimea rezultatului funcției unidirecționale. Este evident, că există mai multe mesaje cu aceiași amprentă digitală, deoarece mulțimea de mesaje posibile este mult mai mare decât mulțimea de valori a amprentei digitale.

La baza schemei de semnătură electronică se situează utilizarea mijloacelor de criptografie asimetrică. Astfel, în urma criptării mesajului *M* cu cheia publică obținem rezultatul *C(M)*. Iar în rezultatul decriptării criptogramei *C(M)* cu ajutorul cheii private obținem *D(C(M))*. Așa dar, pentru ca metoda asimetrică de criptare să fie posibil de utilizat în mecanismul de semnătură electronică, este necesar să aibă loc următoarea relație:

$$C(M) = D(C(M)) = M. \quad (2)$$

Algoritmul de semnare a unui mesaj care utilizează mijloace de criptografie asimetrică poate fi reprezentat astfel:

$$Sign(M)=(H(M), K_{Priv}) \quad (3)$$

unde *H(M)* este amprenta digitală a mesajului, obținută ca rezultat a funcției unidirecționale asupra mesajului *M*, în baza cheii private K_{Priv} (Fig. 1.).

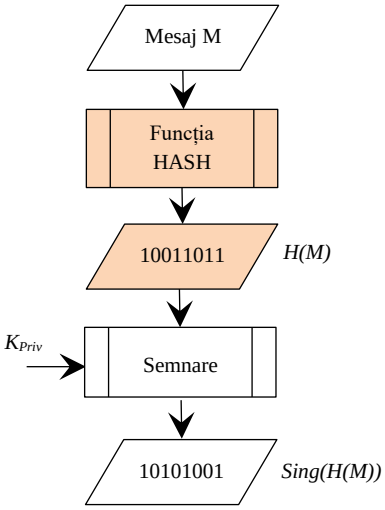

Fig. 1. Algoritmul de semnare

Verificarea semnăturii presupune 2 faze *(Fig.2).*

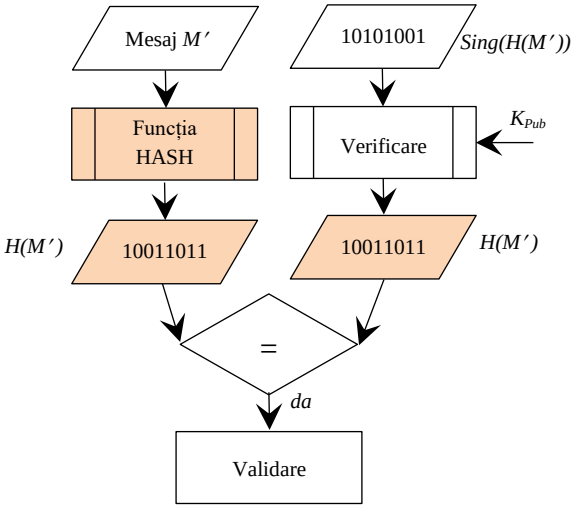

Fig. 2. Algoritmul de verificare a semnăturii electronice

Prima fază constă în aplicarea funcției unidirecționale asupra mesajului recepționat *M′* și obținerea unei amprente digitale *H(M′)*. A doua fază constă în aplicarea mijloacelor de criptografie asimetrică asupra semnăturii electronice atașate la mesaj *Sign(M′)* cu scopul obținerii amprentei digitale *H(M′)* în baza cheii publice. Se compară amprentele digitale obținute la faza întâi și la faza doi, dacă coincid semnătura electronică este validată *(Fig.2)*. În așa mod, semnătura electronică asigură integritatea mesajelor și certifică identitatea entității deținătoare, prin urmare, adevărește proveniența mesajului și asigură non-repudierea lui.

Funcția de dispersie este utilizată și în mecanismul de garantare a autenticității de către centrele de certificare, cunoscut sub denumirea de *infrastructura PKI (public key infrastructure) pentru certificarea cheii publice.*

După generarea perechii de chei, pentru asocierea acestora cu o entitate concretă, cheia publică se supune certificării. Astfel, structura de date care constă din cheia publică și datele de identificare ale entității deținătoare, este supusă aplicării funcției de dispersie, iar amprenta digitală obținută este semnată cu cheia privată a entității care certifică.

Algoritmii de creare și verificare a certificatelor cheii publice sunt identici cu cei prezentați în figura 1 și în figura 2, însă în calitate de mesaj de intrare se ia structura de date a entității deținătoare, iar cheia publică și cheia privată sunt ale entității care certifică.

În practică, cele mai răspândite funcții de dispersie sunt MD5, SHA-1 și familia de funcții SHA-2.

MD5 (Message Digest) produce o valoare binară cu lungimea 128 biți. Este implementată într-un număr larg de produse, deși s-au demonstrat mai multe deficiențe ale acestui algoritm.

SHA-1 (Secure Hash Algorithm), produce o amprentă digitală binară cu lungimea 160 biți. Din 1995 a servit în calitate de standard, iar din 2013 a fost depreciat de Institutul National de Standarde și Tehnologii (NIST, S.U.A), deși este utilizată în continuare pe scară largă.

SHA-2 (Secure Hash Algorithm), la moment este utilizată în calitate de standard de către NIST și este descris în FIPS PUB 180-4. Constă din 5 algoritmi: Pentru mesaje cu lungimea de până la 2^{64} se utilizează SHA-1, SHA-224, SHA-256, iar pentru mesaje cu lungimea de până la 2^{128} se utilizează SHA-384, SHA-512(SHA-512/224, SHA-512/256). Produce o amprentă digitală în diapazonul de la 160 biți până la 512 biți în dependență de algoritm [[7], p. iv]. Preponderent, este utilizată în protocoale de securitate a informațiilor și de autentificare. Este utilizată în DSS (Digital Signature Standard) în combinație cu DSA (Digital Signature Algorithm).

Dat fiind faptul că la nivel mondial, inclusiv în Republica Moldova sunt multe sisteme care utilizează funcția SHA-1, în continuare ne vom referi anume la această funcție. Funcția de dispersie SHA-1, garantează autenticitatea datelor și integritatea acestor în sistemele în care este utilizată, însă nu este lipsită și de vulnerabilități sau coliziuni.

IV. VULNERABILITĂȚILE FUNCȚIILOR HASH

Funcția de dispersie are un rol crucial în realizarea mecanismului de semnătură electronică. Pentru asigurarea securității semnăturii electronice funcția de dispersie trebuie să satisfacă celor trei criterii de securitate descrise mai sus: *rezistența imaginii, rezistența imaginii secundare și rezistența la coliziune*. În acest sens „rezistența" înseamnă absența unor tehnici specifice care ar permite găsirea imaginii, a imaginii secundare sau a coliziunii mai rapid decât un algoritm generic. Această „rezistență" depinde de lungimea amprentei digitale. Dacă valoarea amprentei digitale este de lungimea *n* biți, atunci algoritmul generic are nevoie de $2^{n/2}$ iterații de calcul pentru a găsi o coliziune în conformitate cu „paradoxul zilei de naștere", iar în cazul rezistenței imaginii și rezistenței imaginii secundare 2^n iterații de calcul [[5]].

Teoretic, un atac aspra rezistenți imaginii (*First pre-image attack*) sau a imagini secundare (*Second pre-image attack*) a funcției SHA-1 este un atac de tip „*brute force*" care ar genera 2^{160} combinații de calcul, ce reprezintă practic un număr foarte mare de posibile colizii.

Un atac asupra rezistenței la coliziuni (*Collision attack*), care presupune identificarea a două mesaje diferite dar cu același hash teoretic stabilit ar consuma mai puțin de 2^{80} iterații de calcul.

Chiar și în cazul existenței probabilității de obținere a două mesaje care au conținut diferit și care au, în genere un sens logic practic este imposibilă, însă obținerea teoretică a acestora este realizabilă. Ca urmare, două documente cu același hash pot să aibă semnătura electronică identică, fapt care poate duce la falsificarea semnăturilor electronice și a documentelor semnate.

În februarie 2005, Wang Xiaoyun, Lisa Yin, și Yu Hongbo Itsyun în lucrarea sa [[6]] au prezentat un atac asupra rezistenței la coliziuni a funcție SHA-1 cu o complexitate de calcul mai puțin de 2^{69} operații, care reduce considerabil timpul necesar găsirii unei coliziuni. Autorii au introdus un set de strategii și tehnici corespunzătoare, ce pot fi utilizate pentru înlăturarea obstacolelor majore în căutarea coliziunii pentru SHA-1. În rezultat, a fost obținut primul atac asupra funcției SHA-1 cu o complexitate de calcul mai mică decât valoarea teoretică stabilită anterior de 2^{80}, iar în august 2005, la Conferința internațională de criptologie, CRYPTO 2005, aceiași experți au prezentat o versiune îmbunătățită a atacului asupra SHA-1, cu o complexitate de calcul în 2^{63} operații.

Mai târziu, la conferința internațională Eurocrypt 2009, Cameron McDonald, Philip Hawkes and Josef Pieprzyk au introdus o versiune și mai bună atacului asupra SHA-1, care a redus complexitatea operațională la 2^{52} [[3]].

O altă lucrare a fost publicată în acest sens de către Mark Stevens, Elie Bursztein ș.a. în care se arată că atacurile de tip rezistență la coliziuni au devenit practice prin furnizarea primului exemplu cunoscut de coliziune. Astfel, ei au reușit să creeze condiții în care un atacator poate genera pentru două fișiere diferite de tip .pdf unul și același hash al funcției SHA- 1 și au obținut o complexitate operațională de 2^{35} [[4]].

Într-un alt articol, Mark Stevens arată că crearea de semnături false bazate pe SHA-1 poate fi realizată cu cheltuieli în valoare de aproximativ 100 de mii de dolari. Astfel, sistemele care utilizează funcția hash SHA-1 în aplicarea semnăturii electronice au devenit vulnerabile.

Existenta posibilității de efectuare a atacurilor asupra funcției de dispersie, a dus la faptul constatării, de către organizațiile de standardizare și de prestatori de servicii electronice, a existenței vulnerabilităților funcției unidirecționale SHA-1. În acest context, NIST s-a expus în privința utilizării funcției SHA-1, ca idee principală fiind *încetarea utilizării funcției de dispersie SHA-1 pentru crearea semnăturilor electronice, generarea timbrelor și alte servicii electronice* și altele. Funcția SHA-1 poate fi folosită în continuare doar pentru verificarea semnăturilor electronice

vechi și a timbrelor, generarea și verificarea codurilor de autentificare a mesajelor bazate pe hash (HMAC), generarea aleatorie de biți.

Utilizarea unei funcției criptografice unidirecționale mai complicate ca exemplu SHA-2, poate servi drept soluție pentru minimizarea riscurilor și a vulnerabilităților în mecanismul de semnătura electronică.

V.UTILIZAREA SHA-1 ÎN INFRASTRUCTURA NAȚIONALĂ DE SEMNĂTURĂ ELECTRONICĂ

În anul 2004 în Republica Moldova a fost aprobată reglementarea, la acel moment, a domeniului semnăturii digitale, care prevedea că funcția de dispersie utilizată să corespundă următoarelor condiții: este o funcție unidirecțională și posedă complexitate algoritmică înaltă de depistare a coliziunilor. Totodată, cerințele tehnice pentru funcția unidirecțională utilizată pentru crearea semnăturilor digitale erau stabilite în conformitate cu standardele internaționale în domeniu.

Implementarea cadrului normativ aprobat, a practicii și standardelor internaționale a creat premise necesare pentru crearea infrastructurii cheilor publice la nivel național. Ca urmare, pentru crearea semnăturii digitale a fost prestabilită funcția unidirecțională SHA-1, utilizată până în prezent.

Scopul arhitecturii tuturor infrastructurilor cheilor publice este determinarea și executarea cerințelor necesare pentru sporirea gradului de rezistența semnăturilor electronice, cheilor și funcțiilor criptografice la vulnerabilitățile și riscurile menite de a obține și/sau falsifica date importante.

La momentul actual, în Republica Moldova este creat lanțul național de certificate a cheilor publice în baza certificatului cheii publice a centrului de certificare de nivel superior (*rootcasis2*) care a fost generat în baza funcției de dispersie SHA-1[[10]]. Totodată, certificatele centrelor de certificare de nivelul 2, eliberate de către CRIS Registru (Agenția de servicii publice Registru CA) [[11]], Fiscservinform (Fiscservinform QCA) [[11]2], și Centrul de telecomunicații speciale (Moldsign MID3) [[13]], de asemenea sunt eliberate în baza funcției de dispersie SHA-1.

Necesitatea sporirii gradului de protecție a semnăturilor electronice și a infrastructurii cheilor publice în complex, în legătura cu riscurile și vulnerabilitățile apărute a dus la modificarea cadrului normativ în domeniul semnăturii electronice. În această ordine de idei, recent au fost aprobate norme tehnice în domeniul semnăturii electronice avansate calificate în care pentru crearea și verificarea semnăturii electronice prestatorii trebuie să utilizeze funcția hash SHA-256 [[9]].

Trecerea prestatorilor de servicii de certificare a cheilor publice la o funcție criptografică mai complicată este actuală și în contextul extinderii termenului de valabilitate a certificatului cheii publice de la 1 an la 5 ani.

CONCLUZII

Analizând utilizarea semnăturii electronice la nivel național, s-a constat că la moment infrastructura PKI națională utilizează funcția hash de tip SHA-1. Acest fapt este determinat de existența sau funcționarea sistemelor informaționale a prestatorilor de servicii de certificare, precum și adaptarea acestora la funcția SHA-1 în baza normelor tehnice stabilite anterior. Utilizarea funcției SHA-1 pentru semnătura electronica creează vulnerabilitățile. Trecerea treptată a prestatorilor de servicii de certificare și altor servicii electronice, la o funcție hash mai complicată, și anume SHA-256 stipulată în Normele tehnice [[9]], poate servi drept soluție pentru minimizarea riscurilor de atac asupra rezistenței la coliziuni pentru semnătura electronică.

BIBLIOGRAFIE

[1] Bogdan Groza, Introducere în criptografie. Funcții criptografice, fundamente matematice și computaționale. Editura politehnice, Timișoara, 2012.

[2] Emil Simion, Securitatea criptografică, suport de curs, 2011-2012.

[3] Cameron McDonald, Philip Hawkes and Josef Pieprzyk, SHA-1 collisions now 2^{52}, 2009. Macquarie University and Qualcomm, Australia. Sursa: http://eurocrypt2009rump.cr.yp.to/837a0a8086fa6ca714249409ddfae43d.pdf

[4] Marc Stevens, Elie Bursztein și alții, The first collision for full SHA-1, 2017. Sursa: https://shattered.io/static/shattered.pdf

[5] Simon Knellwolf, Dmitry Khovratovich, New Preimage Attacks Against Reduced SHA-1. Sursa https://eprint.iacr.org/2012/440.pdf

[6] Xiaoyun Wang, Yiqun Lisa Yin and Hongbo Yu, Finding Collisions in the Full SHA-1, 2005. Sursa: https://tayloredge.com/~taylore1/reference/Mathematics/sha1-crypto-auth-new-2-yao.pdf

[7] FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology, 2012.

[8] Legea Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic, publicată 04.07.2014 în Monitorul Oficial Nr. 174-177.

[9] Normele tehnice în domeniul semnăturii electronice avansate calificate, aprobat prin ordinul Directorului SIS nr.69 din 15.07.2016, Publicat 19.07.2016 în Monitorul Oficial Nr. 215-216.

[10] Certificatul cheii publice a Prestatorului de servicii de certificare de nivel superior. Sursa: http://pki.sis.md/cert/MoldovaCA

[11] Сертификаты центра сертификации Государственного предприятия «ЦГИР «Registru». Sursa: https://www.pki.registru.md/ru/repository/сертификаты-i-го уровня.html

[12] Certificatele cheilor publice ale Centrului de certificare al Î.S. "Fiscservinform". Sursa: https://pki.fsi.md/page/public-key-certificates

[13] Certificatele cheilor publice ale Centrului de certificare. Sursa: https://pki.cts.md/registru/certificatele-cheilor-publice.html