Criptografia în Cyberspace

Criptografia computationalã oferã cele mai puternice solutii pentru problemele ce privesc securitatea informaticã a acestui mediu în care ne pregãtim sã trãim în anii urmãtori si care se cheamã Cyberspace. Folositã multã vreme pentru asigurarea confidentialitãtii comunicatiilor în domeniul militar si diplomatic, criptografia a cunoscut în ultimii 20 de ani progrese spectaculoase datorate aplicatiilor sale în securitatea datelor la calculatoare.

Victor-Valeriu Patriciu

Societatea umanã cunoaste în momentul de fatã una din cele mai profunde transformãri din întreaga ei existentã, în care informatica joacã un rol determinant. Dacã deceniul trecut a fost marcat de aparitia si perfectionarea calculatoarelor personale, usor accesibile si la preturi din ce în ce mai scãzute, deceniul anilor '90 este caracterizat de conectivitatea tot mai pronuntatã, adicã fuziunea dintre calculatoare si comunicatii: cele mai multe calculatoare sunt folosite azi în interconectare, în retele locale-LAN si în retele de arie largã-WAN, ceea ce conferã informaticii un rol determinant în asigurarea legãturilor stiintifice, de afaceri, bancare sau de naturã umanã între persoane si institutii. Trãim astãzi o lume în care sute de milioane de calculatoare, deservind utilizatori foarte diversi, sunt interconectate într-o infrastructurã informaticã globalã, numitã de ziaristi si *Cyberspace*(Spatiul Cibernetic). Specialistii cautã si gãsesc, cu o vitezã de-a dreptul incredibilã, solutii tehnice pentru dezvoltarea capacitãtii de comunicatie a calculatoarelor si pentru sporirea calitãtii serviciilor de retea oferite. În acelasi timp societatea se adaptează din mers noilor tehnologii informatice, învãtând sã trãiascã în acestã lume nouã, dominatã de calculatoare si comunicatii între acestea.

Internet, cea mai amplã retea de retele de calculatoare din lume, care se apreciazã cã are câteva zeci de milioane de utilizatori zilnic, interconectând peste 30 de mii de retele de pe tot globul si peste 2.5 milioane de computere, reprezintã embrionul a ceea ce se cheamã *information superhighway* ("autostrada informaticã"). Guvernul federal al SUA investeste în urmãtorii 5 ani 400 milioane dolari pentru dezvoltarea succesorului Internet-ului care se va numi (NREN), despre care se spune cã va fi de 100 de ori mai rapid.

Societatea umanã a început sã transfere pe retele o parte din activitãtiile obisnuite, cãrora comunicatiile aproape instantanee între puncte situate geografic la mii de kilometri le conferã valente superioare. Vorbim astãzi de teleconferinte si grupuri de lucru prin retele de calculatoare, grupuri de discutii, ca niste veritabile cluburi, profilate pe cele mai variate domenii de interes, ziare distribuite prin retele, sisteme electronice de plãti prin retele, sisteme de transfer de fonduri si de comert prin retele, etc. Toate aceste servicii si încã alte sute de acest fel, au început sã fie o realitate a celui mai mare si mai impresionant mediu de comunicatii între oameni care a devenit Internet-ul.

Securitatea informaticã - componentã majorã a Cyberspace

Retelele de calculatoare sunt structuri deschise, la care se pot conecta un numãr mare si uneori necontrolat de calculatoare. Complexitatea arhitecturalã si distributia topologicã a retelelor conduc la o mãrire necontrolatã a multimii utilizatorilor cu acces nemijlocit la resursele retelei- fisiere, baze de date, rutere etc. de aceea putem vorbi de o *vulnerabilitate* a retelelor ce se manifestã pe variate planuri. De aceea un aspect crucial al retelelor de calculatoare, în special al comunicatilor pe Internet, îl constituie *securitatea informatiilor*. Utilizatorii situati la mari distante trebuiesc bine identificati-în mod tipic prin parole. Din nefericire, sistemele de parole au devenit vulnerabile, atât datoritã hacker-ilor care si-au perfectionat metodele cât si datoritã alegerii necorespunzãtoare a parolelor de cãtre utilizatori. Nevoia de *securitate* si de *autenticitate*, apare la toate nivelele

arhitecturale ale retelelor. La nivel înalt, utilizatorii vor sã se asigure cã posta electronicã, de exemplu, soseste chiar de la persoana care pretinde a fi expeditorul. Uneori utilizatorii, mai ales când actioneazã în numele unor firme, doresc asigurarea caracterului confidential al mesajelor transmise. În tranzactiile financiare, alãturi de autenticitate si confidentialitate, un loc de mare importantã îl are si *integritatea mesajelor*, ceea ce înseamnã cã mesajul receptionat nu a fost alterat în timpul tranzitiei prin retea. În tranzactiile de afaceri este foarte important ca odatã receptionatã o comandã, aceasta sã fie nu numai autenticã, cu continut nemodificat, dar sã nu existe posibilitatea ca expeditorul sã nu o mai recunoascã, adicã sã se respecte *proprietatea de nerepudiere.* La nivel scãzut, gateway-urile si ruterele trebuie sã discearnã între calculatoarele autorizate sã comunice si cele intruse. De asemenea, este necesar ca, de exemplu, informatia medicalã transmisã prin retele sã fie confidentialã si sã ajungã nealteratã (voit sau nu) la nodurile care retin marile baze de date ale sistemelor de asigurări medicale.

În aceste circumstante, *securitatea informaticã a devenit una din componentele majore ale cea ce numim Cyberspace*. Analistii acestui concept au sesizat o *contradictie aparentã* (*antinomia)* între nevoia de comunicatii si conectivitate, pe de o parte si necesitatea asigurării confidentialitãtii si autentificãrii datelor la calculatoare si retele, pe de alta parte. Domeniul relativ nou al *securitãtii informatice* cautã o serie de solutii tehnice pentru rezolvarea acestei contradictii. Viteza si eficienta pe care o aduc comunicatiile instantanee de documente si mesaje (postã electronicã, mesagerie electronicã, transfer electronic de fonduri, etc) actului decizional al managerilor care actioneazã într-o economie puternic concurentialã, conduc la un fel de euforie a utilizării retelelor, bazatã pe un sentiment fals de securitate a comunicatiilor, care poate transforma potentialele câstiguri generate de accesul la informatii, în pierderi majore cauzate de furtul de date sau de inserarea de date false sau denaturate.

Criptografia computationalã oferã cele mai puternice solutii pentru toate aceste aceste probleme privind securitatea informaticã. Folositã multã

vreme pentru asigurarea confidentialitãtii comunicatiilor în domeniul militar si diplomatic, criptografia a cunoscut în ultimii 20 de ani progrese spectaculoase datorate aplicatiilor sale în securitatea datelor la calculatoare.

Putem spune cã domeniul criptografiei computationale a devenit azi un spatiu legitim de intense cercetãri academice.

Criptografia este stiinta scrierilor secrete. Un cifru se defineste ca transformarea unui *mesaj-clar* sau *text* clar în *mesaj-cifrat* ori *criptogramã*. Procesul de transformare a textului clar în text cifrat se numeste cifrare sau criptare, iar transformarea inversã, a criptogramei în text clar, are denumirea de descifrare sau decriptare. Atît cifrarea cît si descifrarea sunt controlate de cãtre una sau mai multe *chei criptografice*. Criptoanaliza studiazã metodele de spargere a cifrurilor, de obicei pentru determinarea cheii de cifrare din criptogramã si text clar echivalent.

Un *sistem criptografic* (*criptosistem)* are cinci componente:

- spatiul mesajelor în text clar, {M};
- spatiul mesajelor în text cifrat, {C};
- spatiul cheilor, {K};
- familia transformãrilor de cifrare,

E_k: M-> C ;unde K Î{ K}

- familia *transformãrilor de descifrare,* D_k: C -> M, unde KÎ{K}

Fiecare transformare de cifrare, E_k, este definitã de un *algoritm de cifrare*, E, comun tuturor transformãrilor familiei, si o cheie, K, distinctã de la o transformare la alta. În mod similar, fiecare *transformare de descifrare,* D_k, este definitã de un algoritm de descifrare D, si de *cheia K*. Pentru un K dat, D_K reprezintã inversa lui E_K, adicã:

$D_k(E_k((M))=M, ,M_Î{M}.$

Există două mari *categorii de sisteme criptografice folosite azi în securitatea informatică:sisteme simetrice si sisteme cu chei publice.*

Istoria recentă a criptografiei cunoaste numeroase inovatii care au marcat o cotiturã semnificativã în dezvoltarea metodelor criptografice. Acestea sunt legate de dezvoltarea retelelor de calculatoare al cãror stimulent extraordinar s-a manifestat atît prin presiunea exercitatã de tot mai multi utilizatori, a cãror dorintã expresã era pãstrarea secretului si a sigurantei postei electronice private, a transferului electronic de fonduri si a altor aplicatii, cît si prin potentarea gamei de instrumente folosite, pe de o parte pentru executia algoritmilor de cifrare iar pe de altã parte pentru spargerea sistemelor criptografice. *Vom marca câteva din aspectele caracteristice ale utilizării criptografiei în domeniul calculatoarelor si retelelor.*

Algoritmi criptografici cu cheie secretã

Pentru asigurarea confidentialitãtii datelor memorate în calculatoare sau transmise prin retele se folosesc preponderent *algoritmi criptografici cu cheie secretã (simetrici).* Ei se caracterizează prin aceea cã ambii utilizatori ai algoritmului împart aceeasi cheie secretã, folositã atât la cifrare cât si la descifrare (a se vedea schema criptosistemului simetric).

Deoarece algoritmul este valid în ambele directii, utilizatorii trebuie să aibă încredere reciprocă. *Securitatea acestui tip de algoritm depinde de lungimea cheii si posibilitatea de a o pãstra secretã.* Când comunicatiile dintre numerosi utilizatori trebuie să fie criptate, apare o mare problemă a managementului cheilor; pentru n utilizatori sunt posibile n(n-1)/2 legături bidirectionale, fiind necesare tot atîtea chei. Aceasta implica în general probleme dificile în generarea, distributia si memorarea cheilor. Utilizarea calculatoarelor electronice a permis folosirea unor chei de dimensiuni mai mari, sporindu-se astfel rezistenta la atacuri criptoanalitice. Cînd cheia secretă are o dimeniune convenabilă si este suficient de frecvent schimbată, devine practic imposibilă spargerea cifrului, chiar dacă se cunoaste algoritmul de cifrare. Pe această idee

se bazează si standardul american de cifrare a datelor-DES (*Data Encryption Standard*), larg utilizat de guvernul SUA si de diverse companii internationale. Propus initial de IBM sub forma sistemului Lucifer, DES a rezistat evaluării făcute de-a lungul a aproape două decenii nu numai de „spărgătorii de cifruri" de la NSA-National Security Agency din SUA ci si de nenumărati matematicieni de la marile universitãti din lume. DES a fost adoptat ca standard federal în 1977 si a fost folosit intens datoritã performantelor de vitezã atinse la cifrare. Să amintim doar că DES este folosit azi pentru cifrarea datelor de către multe armate din lume sau de către comunitatea bancară internationalã. Din păcate nu există o certitudine absolută că specialistii de la NSA, sau de la vreo altă organizatie, au reusit sau nu să spargă DES. Experienta a arătat însă că orice schemă criptografică are o viatã limitatã si că avansul tehnologic reduce, mai devreme sau mai tîrziu, securitatea furnizatã de ea. Se consideră că perioada DES este aproape încheiatã si că alte sisteme, cum ar fi *IDEA* sau *Clipper* îi vor lua locul.

Algoritmi criptografici cu chei publice

Un alt moment foarte important în evolutia criptografiei computationale l-a constituit adoptarea unui principiu diferit de acela al cifrării clasice, cunoscută de mii de ani. Whitfield Diffie si Martin Hellman, de la Univeritatea Stanford din California, printr-un articol celebru publicat în 1976, au pus bazele *criptografiei cu chei publice*. În locul unei singure chei secrete, criptografia asimetrică foloseste două chei diferite, una pentru cifrare, alta pentru descifrare. Deoarece este imposibilă deducerea unei chei din cealaltă, una din chei este făcută publică fiind pusă la dispozitia oricui doreste să transmită un mesaj cifrat. Doar destinatarul, care detine cea de-a doua cheie, poate descifra si utiliza mesajul. Tehnica cheilor publice poate fi folosită si pentru autentificarea mesajelor, prin asa numita semnătură digitală, fapt care i-a sporit popularitatea. Folosind *algoritmi cu chei publică (asimetrici*), se crează criptosisteme cu două chei, în cadrul cărora doi utilizatori (procese) pot comunica cunoscînd fiecare doar cheia publică a celuilalt.

În criptosistemele cu chei publice fiecare utilizator A, detine o *transformare de cifrare publicã,* E_A, care poate fi memoratã într-un registru (fisier) public si o transformare de descifrare secretã, DA, ce nu este posibil sã fie obtinutã din E_A. Cheia de descifrare (secretã) este derivatã din cheia de cifrare (publicã) printr-o transformare greu inversabilã (one-way). În sistemele cu chei publice, protectia si autentificarea sunt realizate prin transformãri distincte. Sã presupunem cã utilizatorul (procesul) A doreste sã emitã un mesaj, M, unui alt utilizator (proces) B. Dacã A cunoaste transformarea publicã EB, atunci A poate transmite M la B sub forma C=EB(M), asigurîndu-se astfel functia de confidentialitate.

La receptie, B, va descifra criptograma C utilizînd transformarea secretã DB, cunoscutã doar de el:

$D_B(C)=D_B(E_B(M))=M.$

Schema nu furnizeazã facilitãti de autentificare, deoarece orice utilizator (proces) are acces la transformarea publicã EB a lui B si îi poate trimite mesaje false M' sub forma C'=EB(M').

Pentru *autentificare* se aplicã lui M transformarea secretã DA a lui A. Ignorînd protectia pentru moment, A va emite $C=D_A(M)$ la B, care la receptie va aplica transformarea publicã, E_A a lui A:

$E_A(C)=E_A(D_A(M))=M$ (a se vedea Crearea si Verificarea Semãturii Digitale)

Autentificarea este realizatã deoarece numai A poate aplica transformarea DA. Acest concept poartã numele de *semnãturã digitalã,* fiind folosit pentru recunoasterea sigurã a utilizatorilor sau proceselor. Fie B un receptor de mesaj semnat de A. Semnãtura lui A trebuie sã satisfacã urmãtoarele *proprietãti*:

- B sã fie capabil sã valideze semnãtura lui A;
- sã fie imposibil pentru oricine, inclusiv B, sã falsifice semnãtura lui A;

- în cazul în care A nu recunoaste semnarea unui mesaj M, trebuie sã existe un „judecãtor" care sã poatã rezolva disputa dintre A si B.

Protectia nu este asiguratã, întrucît este posibil ca mesajul M sã fie obtinut de oricine, aplicînd transformarea publicã EA. Pentru a se realiza *simultan protectia si autentificarea* informatiilor spatiului {M} trebuie sã fie echivalent spatiului {C}, asa încît orice pereche (E_A, D_A) sã fie în mãsurã sã opereze atît asupra textului clar, cît si asupra textului cifrat; în plus se cere ca EA si DA sã fie mutual inverse, adicã:

$$E_A(D_A(M))=D_A(E_A(M))=M.$$

Emitãtorul de mesaj A va aplica mai întîi transformarea secretã a sa, D_A, mesajului M, semnându-l. Apoi A va cifra rezultatul - utilizînd transformarea publicã a lui B, EB si va emite cãtre receptor criptograma:

$$C=E_B(D_A(M)).$$

Receptorul B îl obtine pe M aplicînd la început propria-i functie de descifrare, D_B, iar apoi transformare publicã a lui A, E_A, cea care furnizeazã autentificarea :

$$E_A(D_B(C))=E_A(D_B(E_B(D_A(M))))$$
$$=E_A(D_A(M))$$
$$=M.$$

Cel mai cunoscut sistem cu chei publice este RSA al cãrui nume provine de la de cei trei cercetãtori de la Massachusetts Institute of Technology care l-au creat- Rivest, Shamir si Adleman. El este un adevãrat standard „de facto" în domeniul semnãturilor digitale si al confidentialitãtii cu chei publice. Se bucurã de o foarte mare apreciere atît în mediul guvernamental cît si în cel comercial, fiind sustinut prin lucrãri si studii de comunitatea academicã. Sub diferite forme de implementare, prin programe sau dispozitive hardware speciale, RSA este astãzi recunoscutã ca cea mai sigurã metodã de cifrare si autentificare disponibilã comercial. O serie de firme producãtoare de

sisteme de programe si echipamente ca DEC, Lotus, Novell, Motorola precum si o serie de institutii importante (Departamentul Apãrãrii din SUA, National Aeronautics-SUA, Boeing, reteaua bancarã internationalã SWIFT, guvernul Belgiei etc), folosesc acest algoritm pentru protejarea si autentificarea datelor, parolelor, fisierelor, documentelor memorate sau transmise prin retele.

De exemplu firma Lotus a dezvoltat Notes, un nou concept de lucru în comun (groupware) într-o retea. La o astfel de legãturã în comun a numeroase programe si persoane se cere însã o mare încredere în informatie cît si o mare confidentialitate; ca urmare Lotus foloseste semnãtura digitalã si secretizarea cu ajutorul criptosistemelor RSA.

În sistemul de operare NetWare, pentru retele locale, al firmei Novell, se foloseste curent RSA în mecanismele de autentificare care permit utilizatorilor sã acceadã la orice server al retelei.

Motorola comercializeazã telefoane sigure care încorporeazã o serie de metode de confidentialitate si autentificare a utilizatorilor cît si a partenerilor de dialog.Toate acestea se bazeazã pe algoritmul RSA si se regãsesc atît în variante de uz general cît si în variante pentru comunicatii militare, fiind destinate atît transmisiilor de voce cît si de FAX.

Un alt exemplu semnificativ de utilizare a sistemului RSA este reteaua de postã electronicã a guvernului belgian.Toate protocoalele de asigurare a confidentialitãtii si de autentificare prin semnãturã digitalã folosesc acest algoritm.

Publicat în 1978, RSA *este bazat pe imposibilitatea practicã, la nivelul performantelor calculatoarelor de azi, de a factoriza numere prime mari. În acelasi timp gãsirea unor numere prime mari este usoarã. Fuctiile de criptare / decriptare sunt exponentiale, unde exponentul este cheia si calculele se fac în inelul claselor de resturi modulo n.*

Dacã p si q sunt numere prime foarte mari (100-200 de cifre zecimale), cifrarea si descifrarea se fac astfel:

$C=E(M)=M^e \bmod (p*q)$;
$M=D(C)=C^d \bmod (p*q)$;

Numerele e si d sunt cheile, publicã si secretã. Valorile p si q sunt tinute secrete iar n=p*q este fãcut public.

Cifrarea si descifrarea sunt bazate pe *generalizarea lui Euler a teoremei lui Fermat*, care afirmã cã pentru orice M relativ prim cu n,

$M^{j(n)} \pmod n = 1,$

unde j(n) este indicatorul lui Euler. Aceastã proprietate implicã faptul cã e si d sã satisfacã proprietatea:

$e*d \pmod{j(n)} = 1,$

Rezultã:

$M^{ed} = M \pmod n.$

Criptosistemele cu chei publice au urmãtoarele aplicatii mai importante în serviciile specifice retelelor de azi:

-*autentificarea* continutului mesajelor si al emitãtorului, prin semnãturã digitalã;

-*distributia cheilor de cifrare simetricã*, prin anvelopare cu ajutorul sistemelor cu chei publice;

-*autentificarea utilizatorilor* si a cheilor publice prin asa numitele certificate digitale.

Datã fiind importanta pentru securitatea informaticã a criptosistemelor cu chei publice guvernul SUA a initiat adoptarea unui standard de semnaturã digitalã bazat pe conceptul de cheie publicã. Acest demers a generat controverse, soldate chiar cu acuze între organizatiile implicate. Pînã în decembrie 1990, Institutul National de Standarde si Tehnologie al SUA (NIST) recomanda pentru adoptare ca standard metoda RSA, prezentã deja în industrie. Dar nouã luni mai tîrziu, în august 1991, NIST a avansat un cu totul

alt algoritm, bazat pe o metodã cu chei publice publicatã de *El Gamal* în 1985. Noua propunere, denumitã DSS (*Digital Signature Standard),* a fost dezvoltatã de Agentia de Securitate Nationalã a SUA (NSA). Ea a stârnit controverse, nu datoritã performantelor sale, ci mai degrabã ca urmare a suspiciunilor asupra autorului(NSA), care este si spãrgãtor de cifruri.

Sisteme cu chei în custodie

Un alt concept este pe cale a fi implementat în SUA de cãtre NSA (National Security Agency). El este numit sistem cu chei în custodie (Escrowed Key System) si promoveazã pentru SUA o nouã tehnologie criptograficã sub numele de Clipper. El este destinat sã permitã, sub control (legal se sustine), interceptarea si decriptarea, de cãtre institutiile abilitate ale statului, a unor informatii transmise prin telefon, fax sau Internet. Decriptarea se face cu ajutorul unor fragmente de chei obtinute prin aprobãri legale de la asa numite *agentii de custodie a cheilor*.

Cipul Clipper, care va fi integrat atât în telefoane, fax-uri cât si în interfata de retea a calculatoarelor, contine un algoritm de criptare simetricã, pe 64 biti, numit „Skipjack". Acesta foloseste o cheie de 80 biti (în comparatie cu 56 de biti la DES) si are 32 de runde de iteratii (fatã de numai 16 la DES), suportînd toate cele 4 moduri DES de operatii.

Fiecare cip include urmãtoarele componente :

- *algoritmul de criptare „Skipjack"(secret si studiat sub jurãmânt de câtiva mari specialisti);*
- *F- cheie de familie pe 80 biti comunã tuturor chip-urilor ;*
- *N - numãr serial al chip-ului, de 30 biti;*
- *U- cheie secretã pe 80 biti, care va fi lãsatã, sub forma unor fragmente în custodie.*

Cipurile sunt programate de Mykotronx Inc., care le denumeste MYK-78. Suportul fizic este asigurat de VLSI Tehnology Inc., în

tehnologia de 0.8 microni, costînd aproximativ 30 dolari bucata, pentru cantitãti mai mari de 10.000 bucãti.

Majoritatea firmelor din SUA ca si societatea civilã rejecteazã conceptia NSA, obiectând în principal urmãtoarele:

- Clipper a fost dezvoltat în secret, fãrã informarea si colaborarea producãtorilor în domeniu ;
- Algoritmii nu sunt documentati si disponibili;
- Existã teama existentei unor trape care pot permite FBI/CIA sã spargã cifrul ;
- Controlul sever exercitat de guvernul SUA asupra productiei si exportului vor restrictiona afacerile;
- Existã teamã în fata posibilitãtiilor FBI/CIA de a intercepta comunicatiile dintre calculatoare pe scarã mare, fãrã aprobãrile legale.

Sisteme electronice de plãti

Dezvoltarea retelei globale de comunicatii între calculatoare, în ceea ce unii numesc *Global Village* (*Satul Global),* a permis introducerea si folosirea pe scarã tot mai largã a sistemelor electronice de plãti. Acest gen de aplicatii pot fi vãzute ca o laturã a utilizãrii calculatoarelor si retelelor în activitãti financiare si comerciale la mare distantã. *Dintre numeroasele utilizãri ale metodelor criptografice în aplicatiile cu caracter financiar-bancar putem aminti:*

- confidentialitatea (secretizarea) datelor din fisiere, baze de date sau documente me-morate pe suportii externi;
- confidentialitatea datelor din fisiere/documente/postã electronicã transmise prin re-tele de calculatoare sau prin legãturi fax;
- protectia continutului fisierelor/mesajelor/documentelor, autentificarea originii acestora precum si confirmarea receptiei lor autorizate prin servicii de securitate cum ar fi: semnãturã digitalã, sigiliu digital, anvelopã digitalã, certificat digital sau notar digital;

- sigilarea digitalã (criptograficã) a software-ului utilizat, ceea ce împiedicã orice încercãri de modificare a programelor autorizate (protectia software-lui);
- protocoale sigure (criptografice) care sã permitã utilizarea eficientã si robustã a sistemelor de tip POS (Point of Sale)
- asigurarea unor metode de semnãturã digitalã si autentificare pentru cartele magnetice si cartele inteligente (smart-cards);
- asigurarea unor protocoale criptografice sigure pentru utilizarea cecurilor electronice în aplicatiile de EFT (Electronic Founds Transfer).

Transferarea comodã, rapidã si sigurã a banilor a devenit una din cerintele fundamentale de viabilitate a noului concept de sisteme electronice de platã. De asemenea, înlocuirea formelor traditionale de numerar prin intermediul *banilor electronici* (*digibani)* oferã o mai bunã flexibilitate sistemelor de plãti, în conditiile ridicãrii gradului de securitate al tuturor participantilor la sistem. Se diminueazã mult, în aceste conditii, costurile implicate de emiterea si mentinerea în circulatie a numerarului. În sistemele de plãti electronice, cele mai multe lucrând on-line, plãtitorul si plãtitul comunicã cu bãncile în decursul tranzactiilor de platã. Acest lucru implicã necesitatea asigurãrii unui nivel înalt de securitate al sistemului de plãti în ansamblu. Folosirea monedelor electronice, a cecurilor electronice si desfãsurarea unor repetate schimburi de date prin retele, fac necesarã asigurarea confidentialitãtii tranzactiilor, a autentificãrii sigure a entitãtiilor comunicante prin semnãturã si certificate digitale. Folosirea unor smart-carduri pe post de portmoneu electronic fac necesarã desfãsurarea unor protocoale criptografice sigure între aceste mici calculatoare si dispozitivele care joacã rol de registru de casã. Smart-cardurile contin în spatele stratului magnetic un microprocesor pe 8 biti si o memorie de dimensiuni mici. Memoria este divizatã în 3 zone:

- 8 kb de (EP)ROM continînd „inteligenta" (programele);
- 256 b de RAM;

- 8 kb de EEPROM care contine informatiile de identificare a utilizatorului si cheile de cifrare. Partea care contine cheia nu poate fi cititã din afara cartelei.

Dispozitivele de acces si smart-card-urile trebuie sã continã hard si soft securizate la deschidere-"temper proof resistant"- pentru a nu se putea opera modificări în vederea falsificărilor.

În implementarea sistemelor bazate pe digibani, se folosesc pentru cifrare si autentificare algoritmi criptografice cu chei publice. Multe solutii actuale se bazeazã pe schema de identificare/semnãturã a lui Schnorr, a cãrei tãrie porneste de la intractabilitatea problemei logaritmilor discreti, problemã cu o complexitate echivalentã factorizãrii de la schema RSA. Alte implementãri cunoscute în sistemele de plãti electronice folosesc o schemã de autentificare criptograficã propusã de Fiat&Shamir sau cea propusã pentru standardizare de cãtre ISO si publicatã de Guillou&Quisquater .

În momentul de fatã sunt demarate mai multe proiecte de bani electronici si portofel electronic, dintre care amintim: VISA-MASTERCARD-EUROPAY, Banksys în tãrile Beneluxului, Mondex al Bãncii Centrale a Marii Britanii, precum si proiectul ESPRIT-CAFE (Conditional Access for Europe), dezvoltat prin finantarea Comunitãtii Europene, care încearcã sã impunã un limbaj financiar comun bazat pe ECU între tãrile comunitare, în domeniul sistemelor de plãti electronice.

We are at risk

Desigur, cele prezentate în cadrul acestui articol nu sunt decât câteva dintre aplicatiile criptografiei în asigurarea securitãtii informatice a acestui mediu în care ne pregãtim sã trãim în anii urmãtori si care se cheamã Cyberspace. In lucrarea Computer at Risks, dedicatã securitãtii calculatoarelor si retelelor, National Research Council din SUA deschide primul capitol cu acest semnal de alarmã: "We are at risk". Este o afirmatie perfect acoperitã de realitatea în care evoluează majoritatea retelelor din diferite tãri ale lumii, pe care se executã,

concurent, un mare numãr de programe, insuficient protejate împotriva unor atacuri privind integritatea si autenticitatea informatiilor procesate. Tehnologii pentru ameliorarea acestui enorm risc al anilor urmãtori nu pot veni decât din comunitatea cercetãtorilor iar numitorul lor comun va fi acela cã vor utiliza diferite tehnici si protocoale criptografice. Pentru *cã se poate aprecia cu certitudine cã mãsurile legislative care sunt preconizate pentru asigurarea securitãtii Cyberspace-ului trebuiesc dublate de solutii tehnice de protectie, indisolubil legate de noua tinerete a criptografiei computationale*.