PREFAȚĂ

Proiectarea și întreținerea unor sisteme informatice trebuie să satisfacă condiții importante legate de protecția informațiilor memorate în diverse puncte sau transmise pe liniile de comunicații. Aceasta presupune realizarea unui ansamblu de mijloace, metode și măsuri, ce au ca scop prevenirea distrugerii, modificării sau folosirii neautorizate a informației.

Unul din cele mai importante obiective constă în eliminarea posibilităților de distrugere accidentală (utilizându-se cu precădere rezultate din teoria codurilor) sau voită a informațiilor și de acces neautorizat la acestea (având în vedere acoperirea criptografică a informației). Ne propunem abordarea în această lucrare a celei de-a doua direcții.

O primă perioadă de menționare a criptografiei o reprezintă cea cuprinsă din antichitate și până în 1949, cu identificarea [Mas 91] și a câtorva nume semnificative: Julius Cezar, G.S.Vernan, A Turing, etc.

În 1949, de formație inginer și matematician, C. E . Shannon [Sha 49] publică lucrarea *Communication Theory of Secrecy Systems* și deschide o eră ce identifică criptologia ca știință. Sunt avute în vedere comunicațiile cu chei secrete (sisteme criptografice simetrice).

Când în 1976 W. Diffie și M.E. Hellman [DH 76] publică lucrarea *New Directions in Cryptography*, este pentru prima dată enunțată posibilitatea existenței unor comunicații secrete, fără a fi necesar și un transfer al cheii secrete, între emițător și receptor. Este deschisă epoca *criptografiei cu chei publice* (sisteme criptografice asimetrice). Principalele criptosisteme cu chei publice, proiectate și analizate în lucrări bine fundamentate matematic, sunt cele *de tip rucsac, exponențiale, bazate pe coduri corectoare de erori*, dezvoltate *ca aplicații ale teoriei limbajelor și automatelor finite.*

Criptografia a fost folosită mult timp numai pentru secretizarea comunicațiilor diplomatice și militare. În prezent, o dezvoltare fără precedent a mijloacelor și tehnicilor de comunicație, orientate în principal pe transmisiile digitale cu aplicații practic în orice domeniu (economic, social, diplomatic, militar) a impus o dezvoltare permanentă a criptografiei.

În ***Capitolul 1*** sunt prezentați principalii termeni legați de sistemele criptografice, alături de o clasificare a acestora. Nivelele de integrare a metodelor,

procedurilor şi protocoalelor criptografice sunt strâns legate de modelul **OSI**, definit ca standard de comunicaţie, pentru reţelele de comunicaţii digitale.

Elementele de teorie a transmiterii în secret a informaţiei conturează complexitatea descrierii matematice a sistemelor criptografice.

Metodele criptografice simetrice sunt abordate în ***Capitolul 2***. După prezentarea metodei transpoziţiei şi metodei substituţiei, accentul este pus pe descrierea succintă a standardelor de criptare **DES**, **PES**, **FEAL**, precum şi a celui de autentificare **DAA**, elaborat pe baza standardului **DES**.

În ***Capitolul 3*** sunt aprofundate principalele criptosisteme cu chei publice: de tip rucsac, bazate pe problema logaritmilor discreţi, şi cele exponenţiale. Sunt analizate îndeaproape tehnicile de implementare ale metodei **RSA** într-un sistem de autentificare pe bază de cartele inteligente, şi sunt prezentate metode noi de alegere a elementelor de încărcare a procesorului auxiliar. Alte subiecte pe care le-am abordat sunt: generarea şi distribuirea cheilor criptografice (cu autentificarea directă şi indirectă a acestora), funcţii de dispersie, semnătura digitală. Pentru standardul **SHA-1** şi **SHA-1M** (modificat) sunt construite procedurile de obţinere a mesajului rezumat **POMRSHA-1** şi **POMRSHA-1M**.

Capitolul 4 precizează principalele elemente specifice curbelor eliptice: structura de grup pe o curbă eliptică, calculul ordinului acestuia, curbe eliptice peste câmpuri de caracteristică *2* (supersingulare şi nesupersingulare). Sunt aprofundate aspectele matematice legate de clasele şi numărul de izomorfisme, şi sunt analizaţi algoritmi folosiţi pentru calculul numărului de puncte de pe o curbă eliptică.

Proceduri şi tehnici de implementare a operaţiilor descrise pe curbe eliptice, sunt prezentate în ***Capitolul 5***. Implementarea soft şi hard a criptosistemelor cu chei publice, în general, şi a celor construite pe curbe eliptice, în particular, impun abordarea unor metode de optimizare. Sunt studiate îndeosebi bazele normal optimale de tip I şi II, şi este dezvoltată o *bibliotecă criptografică*, specifică criptosistemelor cu chei publice construite pe curbe eliptice. Este prezentată o analiză asupra unor circuite de multiplicare de referinţă, citate în literatură [AMV 93] ca fiind utile aplicaţiilor criptografice şi sunt abordaţi noi algoritmi de calcul în câmpuri finite.

În ***Capitolul 6*** este proiectat un set de protocoale ce acoperă o arie largă a serviciilor criptografice. Noutatea acestora o constituie tocmai dezvoltarea integrală pentru criptosisteme construite pe curbe eliptice. Sunt abordate o serie de aspecte legate de generarea şi distribuirea cheilor criptografice: folosirea funcţiilor greu inversabile (**OWF**), dezvoltarea de protocoale de *tip token* (specifice reţelelor de calculatoare). Secretizarea şi autentificarea mesajului transmis sunt servicii de bază ce sunt asigurate de protocoalele proiectate. Funcţiile de dispersie universale (**UHF**) permit personalizarea serviciilor de criptare şi decriptare, având şansă de a se defini şi ca un standard pentru reţelele de comunicaţie. Algoritmul de generare în *n* paşi a cheii comune de comunicaţie între doi utilizatori, pentru un sistem distribuit, sesizează un mare avantaj al folosirii curbelor eliptice: un simplu număr

întreg constituie cheia secretă. Aceasta este uşor de memorat şi mult mai *mică* decât orice cheie secretă corespunzătoare unui alt criptosistem cu chei publice.

Prin procedurile şi tehnicile prezentate sunt generate curbe eliptice reprezentative, caracterizate printr-o mai eficientă implementare, prin folosirea cărora să se asigure o mai bună acoperire criptografică a mesajului transmis.

Prin investigaţiile realizate, lucrarea poate provoca deschideri ştiinţifice în două direcţii:

1. proiectarea unor sisteme criptografice construite pe curbe eliptice peste câmpuri de caracteristică ≥ 2.
2. proiectarea de coduri de geometrie algebrică, folosite eventual în construirea unor noi sisteme criptografice.

Doresc să mulţumesc pentru îndrumările ce mi-au fost acordate, cu tact şi în mod constant, încă din perioada studenţiei, de către domnul prof. univ. dr. ing. *Valeriu MUNTEANU.*

Pentru lectura manuscrisului şi observaţiile utile făcute, pentru deschiderea ştiinţifică oferită, autorii aduc mulţumiri doamnei prof. univ. dr. mat. *Mirela ŞTEFĂNESCU.*

Climatul de lucru favorabil din cadrul Catedrei de Radioelectronică Navală, Facultatea de Marină Militară, Academia Navală "Mircea cel Bătrân", Constanţa, şi sprijinul acordat de întreg colectivul de-alungul timpului, au fost benefice.

Cursurile ţinute în cadrul Facultăţii de Matematică – Informatică, Universitatea "Ovidius", Constanţa, baza materială pusă la dispoziţie şi colaborările avute cu colectivul de cadre didactice, au fost rodnice.

Înţelegerea şi susţinerea din partea familiei au fost constant îndreptate spre finalizarea acestei lucrări.

Mulţumirile mele se îndreaptă către toţi cei ce, direct sau indirect, m-au stimulat şi ajutat pentru ca această lucrare să poată apare. Colectivul editurii Matrix Rom se numără printre aceştia.

Eugen PETAC