Prefaţă

Criptografia este ştiinţa comunicării informaţiei sub o formă securizată. Istoria ei este veche şi fascinantă. Mesaje ascunse sunt descoperite în Biblie; Herodot menţionează o serie de procedee de steganografie folosite de vechii greci; Cezar foloseşte un sistem de criptare care îi poartă numele; decriptarea telegramei Zimmermann a dus la intrarea Statelor Unite în conflictul din 1914-1918. Şi – în fine – cine nu a auzit de celebra maşină de criptat Enigma ?

Societatea actuală, cu un volum de date care se multiplică rapid, a dat noi valenţe şi a creat noi oportunităţi de dezvoltare a criptografiei. Utilizarea Internetului a sporit şi mai mult importanţa asigurării securităţii informaţiei, dar şi a autentificării ei. Acum domeniul şi-a lărgit competenţele şi s-a extins atât de mult încât a fost necesară redefinirea sa. Criptografia a devenit numai un capitol a ceea ce se numeşte astăzi *Securitatea informaţiei*. Alte capitole care merită fi menţionate sunt: protocoale de semnătură electronică, comerţ electronic (Digital Business), infrastructură cu chei publice(PKI), arhitectura de securitate a sistemelor de calcul (hard şi soft), securitatea reţelelor, securitatea fluxului informaţional, securitatea bazelor de date, standarde şi protocoale de gestiune a cheilor, 0 - knowledge, partajarea secretelor, criptografie vizuală, watermarking, criptografie nestandard (cuantum şi moleculară), standarde de testare şi certificare, protocoale criptografice în medii juridice. Şi zona de interes nu este nici pe departe epuizată. Unele subiecte se dezvoltă rapid şi generează la rândul lor domenii noi. De exemplu, reţelele wireless sau smart-cardurile necesită abordări separate, datorită interesului tot mai mare pe care îl ridică în societatea actuală. Deci, aşa cum în anii 60 Knuth avea în vedere o prezentare a artei programării calculatoarelor, aşa ar fi interesant de construit o enciclopedie a *artei securităţii informaţiei*. O enciclopedie care se îmbogăţeşte zilnic.

Lucrarea de bază este un suport de curs predat la Facultatea de Matematică şi Informatică a Universităţii Bucureşti. Mult timp acest curs a fost opţional; după trecerea la sistemul Bologna, s-a luat în considerare importanţa domeniului şi interesul permanent al studenţilor, astfel încât studiul criptografiei a fost trecut în curicula generală. Materia are în vedere atât o prezentare structurată istoric, cât şi o abordare preponderent teoretică, capabilă să asigure baza fundamentală de cunoştinţe absolvenţilor care ulterior vor lucra în domeniul securităţii informaţiei.

După prezentarea sistemelor simple de criptare (monoa-lfabetice, polia-lfabetice, me-

canice, fluide), studiul sistemelor de criptare bloc se încheie cu prezentarea principalelor sisteme utilizate astăzi: *DES* (Data Encryption Standard) şi *AES* (Advanced Encryption Standard). Toate sistemele sunt analizate din trei puncte de vedere: criptare, decriptare, criptanaliză, un rol deosebit de important având acesta din urmă. Nici un sistem de criptare nu este acceptat dacă nu se demonstrează (teoretic) că rezistă la principalele tipuri de atac: criptanaliză liniară, criptanaliză diferenţială, compromis spaţiu - timp, atac meet-in-the middle, atacuri bazate pe frecvenţă. De aceea, discuţiile asupra acestor tipuri de atac sunt detaliate.

O parte importantă a lucrării se referă la criptografia cu chei publice, construită fundamental pe o conjectură: "P versus NP", tema primei probleme a mileniului. Mai exact, sistemele de criptare din această zonă se bazează pe probleme NP - complete (problema factorizării, problema logaritmului discret, problema rucsacului) care asigură construirea de funcţii polinomial neinversabile. Sistemele prezentate aici – RSA, El Gamal, Merkle-Hellman, McElliece – îşi bazează securitatea pe dificultatea acestor probleme. În plus, construirea unei aritmetici pe mulţimea punctelor unei curbe eliptice a dat posibilitatea utilizării acestei baze pentru adaptarea de sisteme criptografice având o serie de avantaje: lungime mică a cheilor, viteză mare de criptare/decriptare, securitate sporită.

Volumul se încheie cu un capitol dedicat generatorilor de numere pseudo-aleatoare, componentă care însoţeşte toate sistemele de criptare cu cheie publică, precum şi unele sisteme simetrice de criptare (*DES* de exemplu).

Acesta este conţinutul primului volum al lucrării – materia predată timp de un semestru. Va urma un al doilea volum, dedicat unor protocoale criptografice cunoscute. Anume, protocoale de semnătură electronică, de gestiune a cheilor, de partajare a secretelor, de comerţ electronic, de vot electronic, de securitate a poştei electronice. Fiecare astfel de subiect poate constitui tema unui curs separat. În plus, vor mai fi prezentate: modalitatea de construcţie a funcţiilor de dispersie criptografică (hash) precum şi probleme NP - complete care stau la baza noilor sisteme – problema reprezentării, problema dualităţii (perechile Weil - Tate din domeniul curbelor eliptice).

Autorul roagă pe cei care s-au lăsat seduşi de domeniul acesta fascinant, au citit cartea de faţă şi au de făcut observaţii, corecturi sau sugestii să i se adreseze direct pe adresa *aadrian@gmail.com*. Orice propunere constructivă este bine venită.