REZUMATUL TEZEI DE DOCTORAT

„Securitatea algoritmilor criptografici”

Autor: ing. Florin Medeleanu

Email: florinmed@yahoo.com, tel: 0723 606 176

Conducător de doctorat: prof.univ.dr.ing. Ciprian Răcuciu

În cadrul **Capitolului 1**, sunt prezentate elemente introductive ale tezei, noţiuni de bază utilizate în domeniul criptografiei, aspecte generale referitoare la algoritmii criptografici, funcţiile rezumat şi codurile de autentificare a mesajelor. De asemenea, este precizat obiectivul principal al lucrării şi metodele de lucru utilizate pentru atingerea acestui deziderat. Detalierea metodelor de lucru şi de analiză folosite sunt detaliate în conţinutul tezei, pe parcursul capitolelor din cadrul lucrării.

Capitolul 2 prezintă o analiză a mecanismelor criptografice cu cheie simetrică utilizate în procesul de asigurare a securităţii informaţiilor, precum şi principalele metode de atac criptanalitic. În prima parte a capitolului sunt prezentate principalele criterii care stau la baza proiectării şi realizării sistemelor criptografice. Sunt prezentate caracteristicile algoritmilor de criptare simetrici, tipurile de atacuri criptanalitice împotriva acestora, precum şi rezultatele care se pot obţine. Sunt prezentate atacurile de criptanaliză liniară, diferenţială, MITM (meet-in-the-middle) şi atacul prin interpolare, aceste atacuri fiind considerate atacuri criptanalitice de bază. De asemenea, este analizată rezistenţa criptografică a schemelor de criptare obţinute prin înlănţuirea algoritmilor criptografici.

Capitolul 3 face o analiză a algoritmilor criptografici de tip bloc, fiind descrisă funcţionarea celor mai importanţi algoritmi simetrici, DES şi AES. Sunt analizate criteriile de proiectare a elementelor din compunerea acestora algoritmi, arhitectura reţelelor de substituţie-permutare şi a reţelelor Feistel. Ulterior, sunt determinate şi propuse noi elemente care să îmbunătăţească rezistenţa acestor algoritmi la atacurile de criptanaliză liniară şi diferenţială. În partea a doua a capitolului sunt prezentate noţiunile matematice care stau la baza algoritmilor asimetrici şi este descris sistemul criptografic cu chei publice RSA.

Capitolul 4 face o analiză a rezistenţei algoritmilor criptografici de tip bloc la atacurile criptanalitice. Este analizată rezistenţa la atacurile criptanalitice de bază (atacul de criptanaliză liniară, diferenţială, “meet-in-the-middle” şi interpolare), atacul de forţă brută, atacul de potrivire a textului cifrat şi atacul asupra algoritmului de expandare a cheii. Sunt detaliate două tipuri de atac care fac parte din metodele de atac criptanalitic diferenţial asupra algoritmilor bloc, şi anume: metoda caracteristicii diferenţiale şi metoda elementelor active şi pasive. Cele două metode analizate sunt utilizate în desfăşurarea atacului criptanalitic diferenţial şi a atacului square. Metodele de atac sunt analizate în amănunt şi complet exemplificate, fiind utilizate în acest sens două modele reduse de algoritmi bloc, astfel: un algoritm SPN simplificat şi algoritmul mini-AES. Modelarea celor două atacuri studiate pe cei doi algoritmi au rolul de a permite înţelegerea în amănunt a principiilor de desfăşurare a acestor atacuri şi constituie punctul de plecare pentru desfăşurarea unor atacuri similare asupra versiunilor reale de algoritmi bloc, de exemplu AES sau DES.

Capitolul 5 descrie noţiuni de bază şi elemente de teoria câmpurilor Galois, precum şi etapele de dezvoltare şi verificare a unor programe de calcul şi unelte necesare efectuării de calcule în câmpuri Galois. Aceste unelte şi programe sunt folosite ulterior pentru determinarea unor elemente noi din compunerea algoritmilor criptografici analizaţi anterior, DES şi AES. Noile elemente determinate, cutiile de substituţie neliniară (S-box), conduc la construirea unor algoritmi criptografici personalizaţi, cu proprietăţi similare algoritmilor standard (în privinţa rezistenţei la atacurile de criptanaliză) sau chiar cu proprietăţi îmbunătăţite. La finalul acestui capitol, pentru demonstrarea performanţelor criptografice obţinute, sunt efectuate testările statistice ale celor doi algoritmi criptografici propuşi, IAES (AES Îmbunătăţit) şi IDES (DES Îmbunătăţit).

În **capitolul 6** sunt prezentate noţiuni şi definiţii referitoare la anonimitatea în mediul electronic. De asemenea, sunt prezentate principiile teoretice şi câteva scheme de semnare anonimă. În continuare sunt descrise principalele metode de atac asupra schemelor de semnare anonimă. În partea a doua a capitolului este descrisă o aplicaţie a schemelor de semnare anonimă, respectiv analiza anonimă a lucrărilor, şi sunt propuse două noi posibile aplicaţii ale acestor scheme, respectiv loteria electronică cu semnătură anonimă şi votul electronic cu semnătură anonimă. Cele două aplicaţii propuse au fost proiectate de către autor, acesta realizând şi simularea implementării unor părţi din aceste aplicaţii, simulările dovedind viabilitatea şi eficienţa soluţiilor propuse. Pe baza rezultatelor obţinute la aceste simulări, sistemul propus de loterie electronică cu semnături anonime, spre exemplu, ar putea face obiectul unei implementări experimentale, ca fază intermediară spre realizarea unui sistem de loterie electronică complet funcţional.

În **capitolul 7** sunt prezentate principalele concluzii, o sinteză a principalelor contribuţii originale ale autorului precum şi direcţiile viitoare de cercetare.