Ecaterina GARABAJII, UCCM

EVOLUȚIA SISTEMELOR CRIPTOGRAFICE ŞI ROLUL LOR ÎN ASIGURAREA PROTECȚIEI RESURSELOR INFORMAȚIONALE

Abstract: *Secure transactions across the Internet have some goals like as protect the data transfer from neauthorized access. Today 's data encryption methods rely on a technique called public-key cryptography.*

Pentru societatea contemporană informația a devenit o materie primă, fiind prezentă peste tot şi astfel evoluând în resurs strategic.

În prezent, se folosesc informații referitoare la construirea calculatoarelor, la elaborarea programelor în sensul degrevării de activități prea dificile, care necesită un timp mai mult de muncă sau care au un caracter repetitiv.

Dar a apărut o problemă ce ține de împiedicarea acceselor neautorizate la informații, confidențialitatea comunicării fiind o cerință a tuturor timpurilor. Deci, a fost necesară inventarea unui mod de protecție a datelor cît mai sigur, ceea ce şi s-a făcut datorită *criptografiei* sau așa-numitei *ştiinței codificării informației.*

Cunoştințele actuale referitoare la începuturile criptografiei sunt furnizate de diferite lucrări despre ştiințele, religiile, războaiele de pe vremea unor civilizații de mult apuse. Invenția şi aplicarea criptografiei au avut loc în mod independent în mai multe părți ale lumii, la mai multe popoare. Dezvoltarea şi continua perfecționare a criptografiei se datorează, în primul rând, războaielor şi activităților diplomatice.

Se cunosc aşa varietăți de bază ale evoluției criptografiei, cum sunt: criptografia antică, criptografia clasică şi criptografia modernă, fiecare din ele dispunând de specificul său, de anumite priorități şi neajunsuri caracteristice pentru epoca invenției, elaborării şi funcționării lor.

Dezvoltarea sistemelor criptografice cunoaşte o cotitură semnificativă în epoca modernă, datorită următoarelor patru factori:

1. Utilizarea calculatorului electronic a permis potențarea gamei de instrumente folosite efectiv în execuția algoritmilor de cifrare, folosirea unor chei de dimensiuni mai mari (sporindu-se rezistența la atacurile criptoanalitice) datorită puterii de calcul mereu sporite. Criptografia clasică asigură secretul mesajelor în principal prin nedivulgarea algoritmilor (metodei) de criptare şi complicarea lui, combinând substituții şi transpoziții. Criptografia modernă asigură secretul mesajelor prin folosirea unor chei de cifrare de dimensiuni mari frecvent schimbate, chiar dacă se cunoaşte algoritmul de cifrare. Pe această idee se bazează

standardul american de cifrare a datelor DES (Data Encryption Standard), adoptat în 1977 şi bazat pe criptografia simetrică;

2. Dezvoltarea rețelelor de calculatoare şi a Internetului au impus dorința utilizatorilor (persoane, organizații economice şi comerciale) de a păstra secretul şi siguranța poştei electronice, a transferului electronic de fonduri, a comunicațiilor şi altor aplicații, ceea ce a dus la perfecționarea metodelor şi algoritmilor de criptare;
3. Criptografia asimetrică (cu chei publice);
4. Criptografia cu chei în custodie (Key escrow Systems).

În continuare sunt elucidate sistemele criptografice simetrice, asimetrice (cu chei publice) în domeniul sistemelor electronice de plăți JAVA. Este efectuată analiza acestor sisteme şi sunt formulate concluziile respective.

Bibliografie:

1. www.ase.md
2. www.ac.upg-ploiesti.ro
3. www.biblioteca.ase.ro
4. www.referatele.ro
5. www.rasolssariu.blogpost.com
6. www.einformatica.ro
7. www.byte.ro