Considerations on data encryption and decryption

Prof.dr. Manole VELICANU, asist. Simona IONESCU
Catedra de Informatică Economică, A.S.E. Bucureşti

In informatics field, storing and managing data must be done by ensuring protection under both aspects: security and integrity. One of the data security methods is encrypting, meaning a codification of these data, so that the access should be allowed only for authorized persons. The encrypting process rules with the opposite one, the decrypting process, in a cryptographic system. This contains cryptographic algorithms and encrypting/decrypting keys. In the paper work some cryptographic algorithms with symmetric keys and some with asymmetric keys are exemplified. It is also made a comparative analysis of both cryptographic algorithm categories and a suggestion for their usage combined. After the data security insurance, the integrity, meaning their correctness is necessary to be ensured. In this way, a serial of dyspepsia algorithms are used. The presented algorithms, for the data security as well as for their integrity are the one used in Database Management Systems (ie. Oracle 9i), but also in Internet.

Key words*: database, cryptography, encryption, data security, Internet, data integrity, encryption algorithms, encryption keys, cryptosystems.*

Introducere

Datele sunt „materia primă" informațională pentru orice calculator, fie că funcționează ca stație de lucru individuală, fie că lucrează ca un nod într-o rețea. Datele sunt încărcate, stocate, transmise şi prelucrate pe calculatoare. Pe parcursul realizării acestor operații asupra datelor trebuie avută în vedere *protecția* datelor. Acest lucru este valabil atât pentru organizarea datelor în fişiere, cât şi în baza de date. Protecția datelor cuprinde două aspecte: securitatea şi integritatea datelor.

Securitatea datelor se referă la interzicerea accesului la date pentru utilizatorii neautorizați. Cele mai utilizate metode pentru asigurarea securității datelor sunt: autorizarea şi controlul accesului la date, viziunile (partiții logice) asupra datelor, procedurile (rutinele) speciale, criptarea. Această ultimă metodă va fi prezentată în articolul de față.

Integritatea datelor se referă la păstrarea corectitudinii lor pe parcursul stocării şi manipulării. Cele mai utilizate metode pentru asigurarea integrității datelor sunt: controlul concurenței la date, salvarea/restaurarea, integritatea semantică. Această ultimă metodă va fi abordată în lucrarea de față.

Ne vom ocupa, mai întâi, de câteva aspecte legate de criptare, ca metodă pentru asigurarea securității datelor.

Pentru a defini criptografia putem porni de la etimologia cuvântului: *cripto* vine din grecescul *kryptos*, care înseamnă ascuns, obscur, secret, iar *grafie* de la *graphia*, adică scriere. Cu alte cuvinte putem defini criptografia ca arta scrierii secrete. O definiție concisă este dată Yaman Akdeniz, în articolul său "Cryptography and Encryption": "*Criptografia, definită ca <<ştiința care se ocupă cu studiul scrierii secrete>>, se ocupă cu mijloacele prin care comunicațiile şi datele pot fi codificate pentru a preveni descoperirea lor prin interceptare, folosind coduri, cifruri şi alte metode, astfel încât numai anumite persoane să poată vizualiza mesajul inițial.*"

În cadrul sistemelor criptografice se identifică două procese complementare:

1. Criptarea – procesul prin care mesajul este transformat în mesaj cifrat/criptat, utilizând un algoritm de criptare şi o cheie de criptare specifică.
2. Decriptarea – procesul invers criptării, prin care mesajul cifrat/criptat este transformat în mesajul inițial, original, utilizând o funcție de decriptare şi o cheie de decriptare.

Algoritmi criptografici cu chei simetrice

Atât pentru criptare, cât şi pentru decriptare

este utilizată aceeaşi cheie (cheia de criptare = cheia de decriptare). Algoritmii criptografici cu chei simetrice se utilizează în special în cazul transferului unei cantităţi mari de date. În cadrul acestui tip de algoritmi se pot folosi cifruri secvenţiale sau cifruri bloc.

Cifrurile secvenţiale criptează mesajul la nivel de octet, pe rând, unul câte unul. Se utilizează un generator de numere pseudo-aleatoare care este iniţializat cu o cheie şi generează ca rezultat o secvenţă de biţi denumită cheie secvenţială. Cifrarea poate fi cu sincronizare (în cazul în care cheia secvenţială depinde de textul în clar), respectiv fără sincronizare. Cele mai utilizate sunt cifrurile fără sincronizare. Pentru fiecare octet al textului în clar şi cheia secvenţială se aplică operaţia XOR (sau exclusiv). Fiind un algoritm simetric, la decriptare se utilizează operaţia XOR între biţii textului cifrat şi cheia secvenţială, astfel obţinându-se textul în clar.

*Cifrurile bl**oc*** criptează mesajul în blocuri de 64 sau 128 de biţi. Se aplică o funcţie matematică între un bloc de biţi ai mesajului în clar şi cheie (care poate varia ca mărime), rezultând acelaşi număr de biţi pentru mesajul criptat. Funcţia de criptare este realizată astfel încât să îndeplinească următoarele cerinţe:

- ştiind un bloc de biţi ai textului în clar şi cheia de criptare, sistemul să poată genera rapid un bloc al textului criptat;
- ştiind un bloc de biţi ai textului criptat şi cheia de criptare/decriptare, sistemul să poată genera rapid un bloc al textului în clar;
- ştiind blocurile textului în clar şi ale textului criptat, sistemului să-i fie dificil să genereze cheia.

Avantaj: utilizarea cifrurilor în bloc este mai sigură decât utilizarea cifrurilor secvenţiale, deoarece fiecare bloc este procesat în parte.

Dezavantaj: algoritmii care folosesc cifruri bloc sunt mai lenţi decât algoritmii care folosesc cifruri secvenţiale.

Exemple de algoritmi criptografici simetrici mai utilizaţi sunt:

- **DES** (Data Encryption Standard) – dezvoltat iniţial de IBM la cererea Agenţiei Naţionale de Securitate (NSA), devenind din 1977 metoda general acceptată pentru protejarea datelor confidenţiale. În 1993 National Institute of Standards and Technology a emis un document în care se preciza: "Algoritmul criptografic DES transformă o valoare de 64 de biţi într-o valoare binară unică de 64 de biţi, folosind o variabilă de 56 de biţi. Dacă se foloseşte întregul bloc de 64 de biţi (adică, nici unul dintre biţii de intrare nu poate fi dedus de la un bloc la altul), iar variabila de 56 de biţi este aleasă aleator, cheia aleasă nu poate fi dedusă decât prin încercarea tuturor cheilor posibile, cunoscând intrarea şi ieşirea DES. Deoarece există peste $7X10^{16}$ de chei posibile de 56 de biţi, este extrem de puţin probabil să se descopere o anumită cheie folosind această metodă, în mediile expuse în mod obişnuit pericolului."

Totuşi *cracker*-ii nu folosesc acest mod de decriptare. Chiar dacă informaţia nu poate fi decodificată, se poate utiliza un proces comparativ. Astfel se poate lua un dicţionar de cuvinte (al limbii în care se presupune că a fost transmis mesajul), care reprezintă date de intrare pentru un program care le criptează folosind standardul DES (acest standard este public, inclusiv programul de generare a textului criptat). Prin compararea cuvintelor rezultate cu textul criptat, în caz de coincidenţă, există o probabilitate mare ca textul iniţial să fie descoperit. În acest proces de *cracking* se pot adăuga suplimentar îmbunătăţiri, prin inserarea în dicţionarul de cuvinte şi a altor combinaţii generate conform unei liste de reguli.

- **Triple DES** (3DES) **-** criptează datele aplicând de trei ori algoritmul DES. Creşte securitatea datelor, dar implică şi mărirea timpului de criptare.
- **RC4** (Ron's code # 4) – a fost dezvoltat de RSA Security Inc., în 1987 de către Ronald Rivest, fiind standardul internaţional de criptarea simetrică a datelor la viteză mare. Este un algoritm ce utilizează cifruri secvenţiale de lungime variabilă. Operează de câteva ori mai rapid decât algoritmul DES.

Oracle Advanced Security Release 9.0.1 permite utilizarea criptării datelor, folosind în mod aleatoriu oricare dintre aceşti algoritmi de criptare, cu lungimi a cheilor de criptare variabile, în funcţie de setările celor două calculatoare care transmit, respectiv recepţi-

onează mesaje. Astfel algoritmii de criptare valizi în cadrul sistemului Oracle sunt: DES cu o cheie pe 56 sau 40 de biți, 3DES utilizând două sau trei chei, RC4 cu o cheie pe 256, 128, 56 sau 40 de biți.

Algoritmi criptografici cu chei asimetrice

Cheia utilizată pentru criptare este diferită de cheia utilizată pentru decriptare, între ele existând o relație matematică. Cheia de criptare se mai numeşte şi cheie publică, deoarece este cunoscută, disponibilă, fără a compromite mesajul criptat sau cheia de decriptare. Cheia de decriptare se mai numeşte şi cheie privată, fiind cunoscută doar de proprietar şi stocată pe calculatorul său. Datele criptate cu cheia publică pot fi decriptate doar prin utilizarea cheii private. Datele criptate cu cheia privată pot fi decriptate doar având şi cheia publică.

Utilizarea cheii publice se poate realiza doar de entitățile autorizate de către o Autoritate de Certificare, care depozitează şi administrează cheile publice, fiind responsabilă de emiterea şi revocarea certificatelor digitale.

Expeditorul unui mesaj utilizează cheia publică a destinatarului pentru a cripta mesajul. Destinatarul este singurul care posedă cheia privată, utilizată pentru decriptarea mesajului.

Analiza comparativă a algoritmilor criptografici simetrici şi asimetrici

Deoarece în cadrul criptografiei simetrice este utilizată aceeaşi cheie atât pentru criptare, cât şi pentru decriptare, securitatea acestei criptări este redusă, depinzând în mod evident de împiedicarea obținerii cheii secrete de către o terță parte. De cele mai multe ori este necesară securizarea schimbului de chei înainte de începerea propriu-zisă a interschimbului de date criptate.

În cazul algoritmilor asimetrici securitatea este asigurată prin folosirea cheii private şi utilizarea certificatelor digitale. Algoritmii asimetrici sunt ecuații matematice complexe care operează cu numere foarte mari, ceea ce implică o relativă încetineală a procesului.

Algoritmii simetrici sunt de obicei mult mai rapizi, având însă problema partajării cheii de criptare. Un astfel de algoritm este cu atât mai sigur, cu cât lungimea cheii este mai mare (numărul cheilor care ar putea fi testate de o persoană neautorizată creşte). În practică se preferă combinarea celor două forme de criptografie, pentru optimizarea performanțelor.

Combinarea algoritmilor simetrici cu algoritmii asimetrici

Se utilizează criptarea asimetrică (cu chei publice) ca metodă eficientă pentru transmiterea cheii secrete. Utilizând această cheie secretă se începe procesul de criptare / decriptare folosind algoritmi simetrici. Acest proces se realizează în următorii paşi:

1. expeditorul obține cheia publică a destinatarului;
2. expeditorul îşi creează o cheie de criptare aleatoare (cheia unică utilizată în algoritmii de criptare cu chei simetrice) - *cheia1*. Pentru platforma Windows se utilizează aplicația CryptoAPI pentru generarea cheii;
3. expeditorul criptează datele folosind un algoritm simetric şi cheia generată (*cheia1*);
4. expeditorul utilizează cheia publică a destinatarului pentru a cripta *cheia1* întru-un text cifrat (*cheia2*);
5. expeditorul trimite datele criptate şi cheia cifrată destinatarului (*cheia2*);
6. destinatarul, utilizând cheia sa privată, decriptează textul cifrat al cheii (*cheia2*), rezultând astfel *cheia1*;
7. destinatarul decriptează textul utilizând cheia secretă a expeditorului, decriptată la pasul anterior (*cheia1*).

Asigurarea integrității datelor în procesul de criptare

Pentru a se asigura securitatea datelor criptate, adică eliminarea unei posibile intervenții a unei persoane neautorizate se folosesc algoritmi bazați pe funcții de dispersie.

Criptarea datelor asigură caracterul privat al acestora (securitatea), în sensul că terțe persoane nu pot vizualiza informațiile interschimbate. Acest lucru nu este suficient, deoarece poate fi afectată integritatea (corectitudinea) datelor criptate deja. De exemplu, o persoană neautorizată poate modifica datele criptate transmise, proces denumit atac de modificare a datelor (într-un sistem informatic bancar pot fi transmise depuneri de sume

de 1000 milioane lei, în loc de 1 milion lei).
Un alt mod de reducere a integrității datelor este atacul de tip retransmitere (replay attack), prin care un întreg set de date valide este retransmis (de exemplu, în acelaşi sistem bancar, o tranzacție de 1 milion lei poate fi retransmisă de 200 de ori).
Pentru eliminarea acestor forme de atac se utilizează o sumă de control (checksum), care se calculează utilizând o funcție de dispersie. Funcția realizează conversia datelor de orice lungime într-un număr de lungime fixă (această lungime trebuie să fie suficient de mare pentru a face improbabilă găsirea a două şiruri de date cu aceeaşi valoare rezultat).
În momentul transmiterii datelor, în primă fază se generează suma de control, apoi se criptează datele şi se transmit împreună cu valoarea de control. Destinatarul mesajului decriptează atât mesajul, cât şi suma de control şi generează la rândul său o sumă de control pentru mesajul primit. Dacă cele două sume de control (primită, respectiv generată) sunt identice, există o probabilitate foarte mare ca mesajul să fi fost transmis intact.
Cei mai utilizați algoritmi de dispersie sunt **MD5** – Message Digest 5 (care generează sume de control cu o lungime de 128 biți) şi **SHA-1** – Secure Hash Algorithm-1 (care generează sume de control cu o lungime de 160 biți).
Oracle Advanced Security Release 9.0.1 permite utilizarea ambilor algoritmi de asigurare a integrității datelor, aleşi în mod variabil în funcție de setările celor două calculatoare care comunică.

Utilizarea algoritmilor în sisteme de criptare disponibile în Internet

În Internet, sistemele criptografice pot fi grupate în două categorii: protocoale de rețea şi programe/protocoale folosite pentru criptarea mesajelor trimise prin poşta electronică (tabelul 1).

Tabelul 1. Utilizarea algoritmilor în sisteme de criptare disponibile în Internet

Nr. crt.	Sistem	Caracteristici	Principalii algoritmi
1	PCT (Private Communications Technology)	Protocol criptare transmisii TCP/IP	RSA(algoritm de criptare pentru chei publice dezvoltat de Rivest, Shamin, Aldemann) RC4 MD5
2	SSL (Secure Socket Layer)	Protocol criptare transmisii TCP/IP	RSA RC4 MD5
3	S-HTTP – Secure-HyperText Transfer Protocol	Protocol pentru criptarea cererilor şi răspunsurilot HTML	RSA DES
4	SET (Secure Electronic Transaction)	Protocol criptare transmisii de instrucțiuni de plată prin Internet	RSA MD5 RC2
5	CyberCash	Protocol criptare transmisii de instrucțiuni de plată prin Internet	RSA MD5 RC2
6	Ipsec, Ipv5	Protocol de nivel scăzut pentru criptarea pachetelor IP	Diffie-Hellman
7	DNSSEC (Domain Name System Security)	Sistem pentru securizarea DNS	RSA MD5
8	Kerberos	Securitate în rețea pentru aplicațiile de nivel înalt	DES
9	SSH (Secure Shell)	Protecție pentru Telnet la transferul de fişiere	RSA Diffie-Hellman Des Triple DES
10	S/MIME – Secure Multipurpose Inter-	Format pentru criptarea poştei electronice	Specificații utilizator

	net Mail Extension		
11	PGP (Pretty Good Privacy)	Aplicație pentru criptarea poș-tei electronice	MD5 IDEA (International Data Encryption Algorithm) RSA

Bibliografie

1. Securitatea în Internet. Ghidul hacker-ului pentru rețelele conectate on-line şi siteuri Web, Editura Teora, 2001
2. E. Biham, A.Shamir - Differential Cryptanalysis of DES-like Cryptosystems, 1990
3. F.Nastase - Arhitectura rețelelor de calcu-latoare, Editura Economică, 1999
4. R.Shimonski -Your Quick Guide to Common Attacks, 2000
5. M.Velicanu, I.Lungu, M.Muntean, S.Ionescu – Sisteme de baze de date – teorie şi practică, Editura Petrion, 2003
6. M.Velicanu, I.Lungu, M.Muntean, M.Iorga, S.Ionescu – Oracle – platformă pen-tru baze de date, Editura Petrion, 2002

**** Oracle Advanced Security Administra-tor's Guide, Oracle Company
**** CISCO Networking Academy Program
**** http://csrc.nist.gov
**** http://www.oracle.com
**** http://www.pgpi.org
**** http://www.microsoft.com/windows2000/techinfo/cryptpki.asp
**** http://wikipedia.org-wiki/symetric_key_algorithm