Zoran Constantinescu
Gabriela Moise

Criptarea Informaţiei

Ghid practic

Editura Universităţii Petrol-Gaze din Ploieşti
2013

Autorii poartă întreaga răspundere morală, legală şi materială față de editură şi terțe persoane pentru conținutul lucrării.

Descrierea CIP a Bibliotecii Naționale a României
CONSTANTINESCU, ZORAN
Criptarea informației: ghid practic / Zoran Constantinescu, Gabriela Moise. - Ploieşti : Editura Universității Petrol-Gaze din Ploieşti, 2013
Bibliogr.
ISBN 978-973-719-522-7

I. Moise, Gabriela

003.26
004.056.5

Control ştiințific:
Conf. univ. dr. ing. **Otilia Cangea**
Redactor:
Conf. univ. dr. mat. **Cristian Marinoiu**
Tehnoredactare computerizată:
Şef lucr. dr. ing. **Zoran Constantinescu**
Coperta:
Şef lucr. dr. ing. **Zoran Constantinescu**
Director editură:
Prof. univ. dr. ing. **Şerban Vasilescu**

Adresa:
Editura Universității Petrol-Gaze din Ploieşti
Bd. Bucureşti 39, cod 100680
Ploieşti, România
Tel. 0244-573171, Fax. 0244-575847
http://editura.upg-ploiesti.ro/

Cuprins

1. Introducere

Acest prim capitol incearcă să introducă, intr-un mod cît mai simplu şi uşor de înțeles, noțiuni de bază despre criptare. Vom încerca să răspundem la cîteva întrebări simple, cum ar fi de exemplu: ce este criptarea? de ce avem nevoie de criptare? în ce situații este justificată folosirea criptării? Vom continua cu introducerea unor definiții şi a terminologiei folosite în criptare şi în literatura de specialitate aferentă. De asemenea vom prezenta diferite criterii de clasificare a principalilor algoritmi folosiți în criptare, pentru a avea o vedere de ansamblu asupra acestor algoritmi şi a folosirii acestora. Vom menționa şi criptanaliza, care este acea partea a criptologiei care se ocupă cu analiza şi spargerea cifrurilor pentru a reface textul clar. Vom încheia capitolul cu o alta întrebare: de ce este nevoie de standarde in criptografie? şi cu o scurtă descriere a standardelor din criptografie.

1.1 Problema criptării

Să presupunem că dorim să transmitem un mesaj de la o persoană A la o persoană B, folosind un canal de comunicație. **Mesajul** poate fi orice, de la un simplu cuvînt sau o propoziție, mesajul de pe o carte poştală sau dintr-o scrisoare, toate în format tradițional pe hartie, pînă la un mesaj în format electronic: binar, un text, un şir de numere, diverse fişiere, o imagine, un document, o convorbire telefonică, o transmisiune video live sau orice alt mesaj in format digital. Deasemenea, lungimea mesajului poate varia de la cîțiva bits pîna la zeci de GigaBytes. **Canalul de comunicație** poate fi orice, de la un mesager sau curier, care expediază o scrisoare, sistemul de poştă pe hîrtie, sistemul de telefonie mobilă, pînă la Internet, cu diversele metode de conectare. Vom considera în cele ce urmează că datele primite sînt identice cu cele transmise de-a lungul canalului de comunicație, cu alte cuvinte mediul de transmisie din punct de vedere tehnologic este lipsit de erori. Există un alt domeniu separat denumit *transmisia datelor* care se ocupă cu analiza mediilor de transmisie, sursele de distorsiuni şi zgomote, metodologii de prelucrare şi transmisie a datelor, protocoale de transmitere corectă a datelor şi integritatea lor.

Expeditorul, cel care trimite mesajul, numit şi sursa mesajului, poate fi o persoană, o organizație, un sistem electronic, un telefon mobil, un calculator. La fel si **destinatarul**, cel care primeşte sau recepționează mesajul, numit cîteodată şi receptor. Cea mai simplă analogie este poşta clasică, unde orice scrisoare are două adrese pe ea: expeditorul si destinatarul. În mod similar avem şi cazul poştei electronice, cu adresele de email ale expeditorului şi destinatarului.

Pentru simplificarea prezentării diverselor sisteme, în criptografie şi în literatura de specialitate, pentru părțile implicate în comunicare se folosesc nume de persoane: pentru expeditor se foloseşte numele **Alice** (persoana A), iar pentru destinatar se foloseşte numele **Bob** (persoana B). Este mult mai simplu să spunem: "Alice trimite un mesaj lui Bob folosind un algoritm de criptare X", decît sa spunem: "O persoana sau un sistem A trimite un mesaj unei alte persoane sau sistem B folosind un algoritm X".

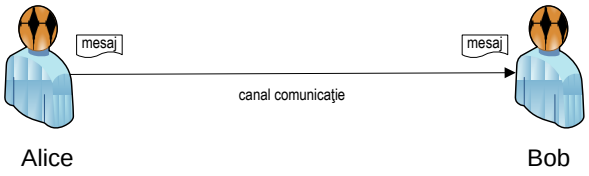

Figura 1.1 Alice şi Bob

Ce se intimplă daca cineva ascultă mesajul transmis de Alice lui Bob? Un exemplu simplu este situația în care mesagerul, sau o altă persoană sau sistem, citeşte mesajul care este transmis. Sînt situații în care acest lucru nu se doreşte, şi se preferă ca acesta să nu cunoască deloc conținutul mesajului. Persoana care doar ascultă mesajele, dar fără a interveni asupra lor, este denumită în literatură **Eve**, de la cuvîntul englez *eavesdrop*, care înseamnă a asculta în secret convorbiri particulare, a trage cu urechea.

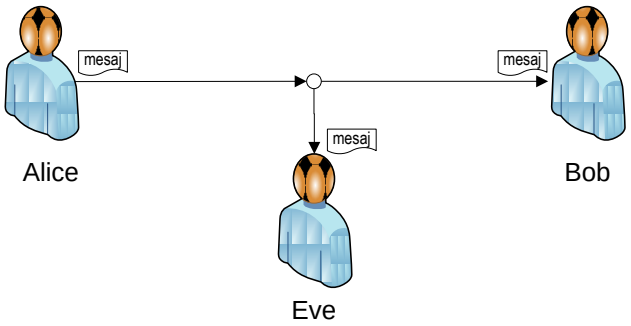

Figura 1.2 Alice, Bob şi Eve

Aici intervine **criptografia** (*cryptography*), ştiința care oferă diferite metode de a ascunde mesajul original. Mesajul nu mai este trimis în clar, ci este transformat sau codificat astfel încît oricine l-ar asculta nu ar putea să-l înțeleagă. Este ca şi cum mesajul ar fi scris într-o altă limbă, dar pe care nu o înțeleg decît Alice şi Bob, necunoscută pentru Eve sau pentru oricine altcineva, limbă pe care nimeni nu ar putea s-o învețe. Deşi pare simplu la prima vedere, nu este deloc uşor acest lucru. De-a lungul istoriei au fost folosite diferite metode de a ascunde informația trimisă, de la simple substituții de litere din mesajul clar (acum mii de ani), pînă la mecanisme sau sisteme foarte complexe pentru codificarea mesajelor (în timpul celor două războaie mondiale), şi pînă la sisteme informatice de toate dimensiunile şi toate complexitățile, omniprezente în zilele noastre.

Scenariul descris mai sus este de fapt primul şi cel mai important obiectiv urmărit de criptografie, şi anume **confidențialitatea datelor** (*data confidentiality, privacy, secrecy*), cu alte cuvinte proprietatea de a putea păstra secretul informației pentru a fi siguri că doar persoanele autorizate au aces la aceste informații. Confidențialitatea datelor ne poate garanta de exemplu că parola de login trimisă pentru conectarea la un server sau website nu poate fi aflată de nimeni care ascultă fluxul de date din rețea, sau că nimeni neautorizat nu poate afla numărul cardului de credit folosit într-o tranzacție online.

Există deasemenea situații in care nu se doreşte doar ascunderea mesajului trimis pentru a nu putea fi citit, ci se doreşte în plus asigurarea faptului că mesajul transmis de Alice este identic cu cel primit de Bob şi nu a fost modificat în mod intenționat de către altcineva, oricare ar fi intențiile acestuia.

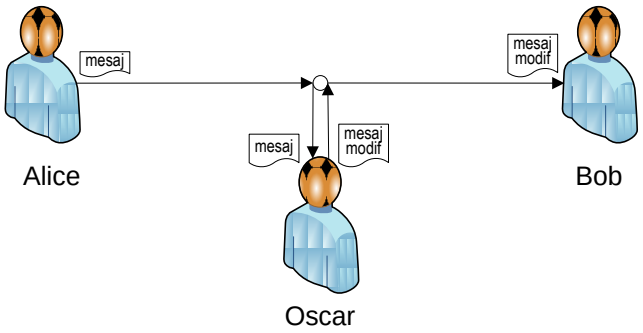

Figura 1.3 Alice, Bob şi Oscar

Un astfel de personaj care modifică în mod intenționat şi cu scop răuvoitor mesajele trimise de la Alice către Bob este numit în literatura **Oscar**, de la cuvîntul englez *opponent*, sau **Mallory** (sau **Mallet, Marvin, Moriarty**), de la cuvîntul englez *malicious*, care înseamnă răuvoitor. Acesta poate nu doar să intercepteze mesajele, dar poate să le şi modifile, să le ştearga de tot, să le scurteze, să le substituie cu propriile sale mesaje, să folosească mesaje mai vechi pe care le-a interceptat mai demult în locul lor şamd. Dificultatea asigurării unui sistem împotriva unor astfel de atacuri devine mult mai dificilă, şi stă la baza întregului domeniu al criptanalizei. Diferența între Oscar şi Mallory este că cel din urmă are întotdeauna intenții răuvoitoare, în timp ce Oscar poate face acest lucru şi cu alte scopuri, nu neaparat rele.

Aici am identificat al doilea obiectiv important al criptologiei: **integritatea datelor** (*data integrity*). Aceasta este proprietatea de a putea evita orice modificare neautorizată a informației, cum ar fi inserare, substituție, ştergere şi sînt folosite diverse metode pentru a putea detecta sau împiedica astfel de schimbări.

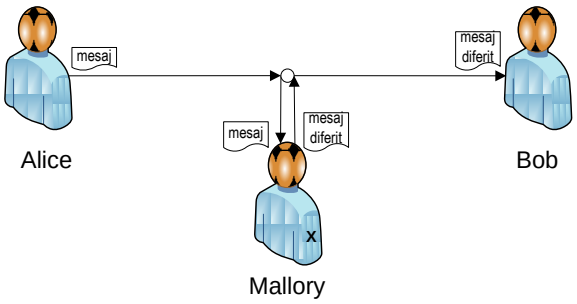

Figura 1.4 Alice, Bob şi Mallory

O altă situație care este pe larg analizată de către criptologie este situația în care vrem sa fim siguri că mesajul trimis de către Alice este intr-adevăr trimis de Alice şi nu de altcineva, iar acesta este primit doar de către Bob. Acesta este de fapt al treilea obiectiv al criptografiei, denumit **autentificare** (*authentication*) şi reprezintă proprietatea de a putea identifica că o anumită entitate este conform anumitor criterii, că este autentică, conform cu adevărul. Poate cuprinde atît autentificarea sursei sau a destinației, dar şi autentificarea mesajului, respectiv a informației transmise sau a unei semnături electronice. Autentificarea poate fi considerat ca un proces care verifică dacă "*cineva (ceva) este cine (ceea ce) spune că este*".

Un alt termen asemănător întîlnit este cel de **autorizare** (*authorization*), care se referă la procesul de descriere, verificare a accesului la resurse, cu alte cuvinte dacă "*cineva (ceva) are dreptul să facă un anumit lucru*".

Un aspect important studiat de criptologie este situația în care Alice neagă că anumite mesaje trimise de ea în trecut îi aparțin. Deşi ea le-a trimis, ulterior ea neagă acest lucru. În acest caz sînt dezvoltate anumite protocoale care să o oblige pe Alice să îşi recunoască propriile mesaje, fără a le putea nega după bunul plac. Pentru această situație se foloseşte termenul de **non-repudiere** ***(****non-repudiation****)***, care este un alt obiectiv important al criptologiei. Termenul provine din cuvîntul *a repudia* care înseamnă a respinge, a nu mai recunoaşte pe cineva sau ceva, a alunga. Una din metodele folosite în criptografie pentru asigurarea non-repudierii este **semnătura digitală**, prin care se poate *semna* de exemplu un document sau un mesaj de către expeditor. Această semnătură trebuie să îndeplinească mai multe criterii: să nu poată fi falsificată (doar expeditorul poate semna), să fie autentică (destinatarul poate verifica faptul că expeditorul a semnat şi nu altcineva), să nu poată fi reutilizată pentru alt document sau mesaj (să nu poată fi copiată pe alt document), documentul să nu poată fi modificat ulterior semnării şi să fie non-repudiabilă (să nu poată fi negată de cel care a semnat).

În tabelul 1.1 am descris pe scurt cele patru obiective fundamentale ale criptologiei.

1	**confidentialitatea datelor**	secretul informatiei
2	**integritatea datelor**	evitarea modificarii informatiei
3	**autentificarea**	identificarea entitatilor
4	**non-repudierea**	prevenirea negarii evenimentelor

Tabelul 1.1 – Obiectivele principale ale criptologiei

Lista obiectivelor criptologiei este însă mult mai lungă, citeva din ele fiind prezentate succint in tabelul 1.2. Toate acestea insă pot fi descrise folosind doar cele patru obiective fundamentale de mai sus.

De cele mai multe ori mecanismul de protecție folosit de un sistem pentru a transmite mesaje depinde de o multitudine de factori: de complexitatea sistemului, de resursele disponibile, de ceea ce se doreşte a fi protejat, de celelalte sistemele cu care interacționează şamd. Nu există un algoritm care să fie bun în orice situație.

confidentialitatea datelor	secretul informatiei
integritatea datelor	evitarea modificarii informatiei
autentificarea entitatilor	identificarea entitatilor
autentificarea mesajelor	identificarea mesajelor, a sursei
semnatura	asocierea de informatii unei entitati
autorizare	imputernicire sau obtinerea unui drept
validare	recunoasterea valabilitatii
controlul accesului	accesul selectiv la resurse
certificare	dovedirea autenticitatii
datare, timestamping	stabilirea datei exacte a unui eveniment
anonimitate	lipsa identificarii unei entitati sau mesaj
non-repudierea	prevenirea negarii evenimentelor
revocare	retragerea unui drept

Tabelul 1.2 – Cîteva obiective ale criptologiei

Criptografia este folosită în zilele noastre aproape în orice sistem de comunicație, rețea de calculatoare sau sistem informatic. Exemple de zi cu zi care folosesc criptarea: cardul bancar cu chip folosit în automatele bancare sau la plata într-un magazin, cardul SIM dintr-un telefon mobil, banala telecomanda pentru activarea alarmei de la maşină, autentificarea la serverul de email, tranzacțiile online pentru cumpărături (eBay, PayPal), comunicația de tip wireless WiFi, televiziunea digitală.

1.2 Definiții. Terminologie

Criptarea (în engleză *encryption*) reprezintă transformarea unui mesaj clar într-un format care nu poate fi uşor interpretat de către o persoană neautorizată. La modul general, criptarea reprezintă conversia datelor dintr-un format uşor interpretabil de către oricine, într-un format dificil, sau chiar imposibil de interpretat de către o persoană (sau un sistem), dar uşor de interpretat de către persoanele autorizate. Operațiunea inversă de transformare a mesajului codificat în mesajul clar, original, pentru a putea fi interpretat se numeşte **decriptare** (în engleză *decryption*).

Mesajul original se mai numeşte şi **mesaj clar** (în engleză *plaintext*), iar cel care se obține în urma criptării se numeşte **mesaj criptat** (în engleză *ciphertext*).

Criptologia (*cryptology*), constituită ca o ramură interdisciplinară este domeniul ştiinţific care se ocupă cu studiul codurilor secrete. Termenul vine din cuvintele greceşti *kryptos*=ascuns,secret şi *logia*=studiu,teorie. Cuprinde două mari componente: **criptografia** (*cryptography*) (din cuvintele greceşti *kryptos* si *graphia*=scriere) este partea care se ocupă cu studiul tehnicilor, algoritmilor, metodelor matematice referitoare la diverse aspectele ale securităţii informaţiei, incluzînd proiectare, construirea şi analiza diverselor protocoale, şi **criptanaliza** (*cryptanalysis*) (din cuvintele greceşti *kryptos* si *analyein*) este ştiinţa şi arta care se ocupă cu analiza sistemelor informatice din punct de vedere al securităţii, îndeosebi a aspectelor ascunse ale acestora. Pe lîngă analiza matematică a algoritmilor criptografici, include şi studiul diverselor alte căi de atac ale sistemelor, nu neapărat ale algoritmilor, ci ale diverselor puncte slabe ale sistemelor, ale implementărilor acestora, cu decodificarea mesajelor criptate fără a se cunoaşte cheile de criptare. Criptografia ar putea fi privită ca latura defensivă a criptologiei, în timp ce criptanaliza ca latura ofensivă a acesteia. Specialiştii din criptografie se numesc **criptografi**, iar cei din domeniul criptanaliză se numesc **criptanalişti**. Scopul final al criptanalizei este cumva similar cu cel al decriptării şi anume aflarea textului clar al mesajlui. Diferenţa constă în faptul ca la decriptare se cunoaşte cheia, în tip ce criptanaliza încearcă acest lucru fără a cunoaşte cheia.

Din punct de vedere istoric, criptologia a fost asociată exclusiv cu criptarea si decriptarea mesajelor, cu scopul de a ascunde informaţia. Abia dupa apariţia sistemelor de calcul in sec. XIX-XX, domeniul s-a dezvoltat foarte mult, au apărut noi metode bazate pe teorii matematice complexe şi necesitatea folosirii calculatoarelor din ce în ce mai performante, precum şi noi cerinţe pentru sistemele informatice.

Un **algoritm criptografic** (*cryptographic algorithm*), sau **cifru** (*cipher*) pe scurt, este o funcţie matematică folosită în procesul de criptare şi de decriptare. Un astfel de algoritm de criptare este folosit de obicei în combinaţie cu o **cheie** (*key*), care poate fi de exemplu un cuvînt, o frază, un text mai lung sau un numar. Aceasta cheie este folosită pentru criptarea unui text clar. Folosind acelaşi algoritm pentru un text clar, dar chei diferite de criptare, se obţine texte codificate diferite. De obicei securitatea (confidenţialitatea) mesajului criptat este dependentă atît de puterea algoritmului (in engleză *strength*), cît si de confidenţialitatea cheii de criptare.

Există foarte mulți termeni folosiți în criptografie, noi am prezentat doar o mică parte din ei. Pentru o listă completă cu definițiile termenilor folosiți în criptografie şi în special în securitatea Internetului se poate consulta [3].

1.3 Clasificarea algoritmilor de criptare

Exista mai multe criterii după care se pot clasifica algoritmii de criptare. Cel mai important criteriu este după felul în care se foloseşte cheia la criptarea, respectiv decriptarea mesajului. Algoritmii se împart în două mari clase: cu **chei simetrice** (sau chei private) şi cu **chei publice** (sau chei asimetrice).

Algoritmii de criptare cu chei simetrice au proprietatea că folosesc aceeaşi cheie atît pentru criptarea textului clar, cît şi pentru decriptare textului codificat. Din acest motiv este folosit termenul de *simetric*. Cheile pot fi identice, sau una din ele să poată fi obținută din cealaltă folosind transformări simple. Cheile reprezintă de fapt un secret care este partajat doar de părțile implicate (de exemplu Alice şi Bob) şi care permite schimbul ulterior de mesaje în mod secret intre acestea. Unul din marile dezavantaje ale acestor tipuri de algoritmi este faptul că aceste chei trebuie partajate, acest lucru nefiind întotdeauna posibil, existînd situații în care această cheie nu poate fi transmisă în mod sigur.

Algoritmii de criptare cu chei asimetrice, sau cu chei publice folosesc două chei diferite pentru criptare şi decriptare, una din ele fiind secretă (privată) iar cealalta publică. Deşi cheile sînt diferite, există o legătură între ele din punct de vedere matematic. Una din chei este folosită pentru criptarea mesajului clar, iar cealaltă pentru decriptarea mesajului codat. Niciuna dintre aceste chei nu poate fi folosită doar ea atît pentru criptare cît şi pentru decriptare. Cheia publică poate fi publicată fără nici un risc în a compromite securitatea, în timp ce cheia privată nu trebuie să o ştie decît cei care au acces la informație. Algoritmii folosiți în criptarea asimetrică au la bază probleme matematice care nu au soluții eficiente (factorizarea numereler întregi foarte mari, problema logaritmului discret, etc.).

Deşi este uşor să se genereze cele două chei împreună, avînd doar cheia publică este extrem de dificil, practic aproape imposibil să se găsească cheia privată asociată. Din acest motiv algoritmii de criptare

asimetrici nu necesită un canal de comunicație sigur între parteneri pentru schimbul inițial de chei secrete, spre deosebire de algoritmii simetrici, unde acest lucru este necesar. Criptarea este realizată de Alice folosind cheia publică a lui Bob, în timp ce Bob este singurul care poate decripta mesajul folosind cheia sa privată. O altă utilizare a acestor algoritmi este verificarea autenticității unui mesaj utilizînd semnătura digitală. Această semnătură poate fi efectuată folosind cheia privată, iar verificarea semnăturii poate fi efectuată ulterior de către oricine, folosind doar cheia publică.

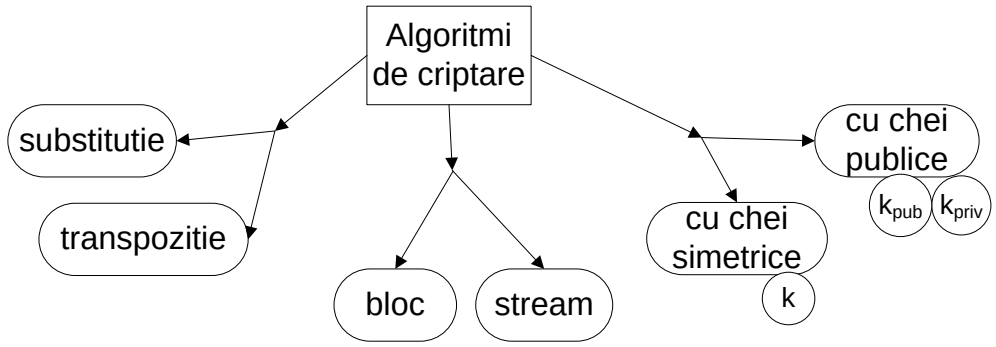

Figura 1.5 Clasificarea algoritmilor de criptare

Clasificarea algoritmilor de criptare se poate face şi după felul în care se procesează textul clar/criptat la criptare/decriptare. O primă metodă este procesarea pe blocuri, iar algoritmii se numesc de obicei **cifruri bloc**. Textul clar este împărțit în blocuri cu lungime fixă de caractere, după care fiecare bloc este criptat rînd pe rînd. În cazul în care lungimea textului clar nu este multiplu întreg de lungimea blocului, se foloseşte un algoritm de completare a acestuia cu caractere pînă la lungimea blocului folosită. Acest lucru se numeşte **padding** (din cuvîntul englez *to pad*=a căptuşi), iar cea mai simplă variantă este completarea cu caractere zero sau spații.

Cele mai cunoscute moduri de operare ale cifrurilor bloc sînt: **ECB** (*electronic code block)* şi **CBC** (*chiper block chaining*). Modul ECB este cel mai simplu şi cel mai uzual şi presupune codificarea independentă a fiecărui bloc B_i al mesajului clar într-un bloc cifrat C_i de aceeaşi mărime, folosind chei diferite K_i pentru fiecare pas. Modul CBC foloseşte un mecanism de feedback în care rezultatul cifrării unui bloc anterior C_{i-1} este folosit pentru cifrarea blocului curent B_i, textul cifrat nemaifiind dependent doar de textul clar ci şi de textul cifrat.

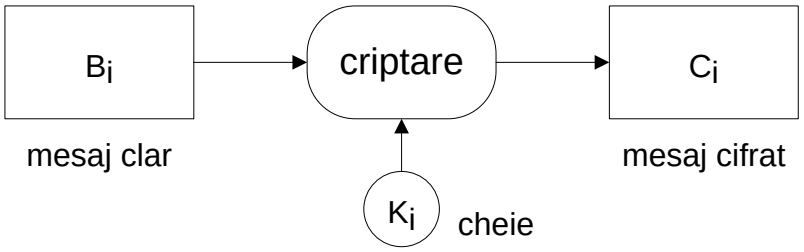

Figura 1.6 – Codificare pe blocuri de tip ECB

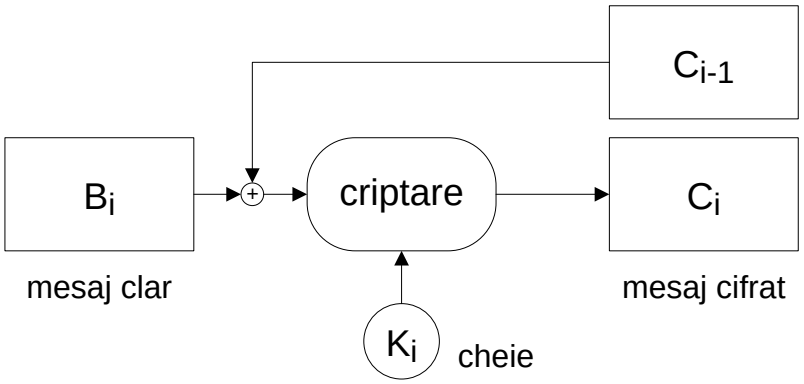

Figura 1.7 – Codificare pe blocuri de tip CBC

Pentru decriptare se foloseşte în mod similar împărțirea în blocuri de aceeaşi lungime. Lungimea blocurilor este relativ mare, şi poate avea valori tipice de 64, 128 sau 256 bits. Spre deosebire de cifrurile de tip bloc, **cifrurile stream** codifică mesajele folosind blocuri foarte mici, de un character (sau o literă din alfabet) sau chiar şi de 1 bit lungime.

1.4 Metode de criptanaliză

Criptanaliza se ocupă cu determinarea unei chei folosite de un algoritm de criptare, doar pe baza mesajelor criptate şi eventual a altor informații secundare. Criptanalistul poate folosi diferite strategii pentru aflarea cheii, în funcție de algoritm şi de situația în care se află. El poate de exemplu să cunoască doar textul criptat şi eventual alte detalii despre textul clar (limba în care este scris mesajul, frecvența literelor unui alfabet şamd). Deasemenea, este posibil să cunoască una sau mai multe perechi de caractere sau blocuri (*text clar, text criptat*), ori poate să aibă acces la algoritm şi să poată cripta anumite texte clare selectate de el.

Criptanaliza prin forță brută (*brute force attack*) constă în parcurgerea tuturor cheilor posibile. Pentru fiecare cheie se decriptează textul şi se verifică dacă este cel corect. Acest tip de atac reuşeşte întotdeauna deoarece parcurgînd fiecare cheie vom trece inevitabil şi peste cheia folosită pentru criptare. Atacul poate fi realizat practic doar în cazul în care spațiul cheilor posibile este mic, altfel timpul necesar parcurgerii lor este mult prea mare. Din acest motiv, pentru a descuraja atacurile prin forță brută, este recomandat ca cifrurile să aibă un număr foarte mare de chei posibile.

1.5 Standarde de criptare

O metodă pentru a păstra securitatea informației este folosirea unor **algoritmi secreți**. Dacă doar Alice şi Bob cunosc algoritmul, atunci am putea presupune că oricine ascultă mesajele schimbate între ei nu va putea să le înțeleagă. În realitate însă este dificil acest lucru. Pe de o parte ei vor trebui să-şi scrie singuri programele software care implementează algoritmul respectiv, lucru destul de dificil, iar pe de altă parte, de-a lungul timpului s-a constatat că nici un algoritm nu este infailibil, şi că mai devreme sau mai tîrziu acesta poate fi spart, fără chiar ca Alice şi Bob să ştie acest lucru. Daca Alice va dori să comunice şi cu alte persoane, atunci va trebui să aibă cîte un algoritm pentru fiecare persoană, lucru deja extrem de dificil. Cu toate acestea, folosirea unor astfel de algoritmi secreți care nu se cunosc public este practicată chiar şi în zilele noastre. Foarte multe sisteme, inclusiv sisteme de operare şi diverse dispozitive folosesc acest lucru în mod curent, fără a lua foarte în serios implicațiile din punct de vedere al securității.

Deoarece este dificilă proiectarea şi implementarea unui algoritm bun de criptare, implicînd un efort considerabil, iar sistemele informatice fiind foarte diferite, s-a impus de-a lungul timpului necesitatea **standardizării** în criptografie, în special a algoritmilor şi a protocoalelor folosite. Avantajele majore oferite de standardizare sint compatibilitatea şi interoperabilitatea sistemelor. Avînd un algoritm de criptare care este standardizat, iar dacă implementarea acelui algoritm pe diferite sisteme respectă acel standard, atunci vom fi siguri ca un acelaşi mesaj codificat pe ambele sisteme, cu aceleaşi chei, vom obține acelaşi rezultat. Este mult mai uşor să avem un algoritm standard care este deja implementat în diferite sisteme pe care să-l putem folosi. E drept că va trebui să avem încredere în cei care au proiectat algoritmul şi că nu există nici un punct

slab în algoritm care să poată fi exploatat de un eventual criptanalist. De obicei standardizarea este făcută de organizații care ne asigură că acest lucru nu este posibil, sau foarte puțin probabil.

Există diferite standarde pentru diferite aspecte din criptografie:

- standarde pentru algoritmi: DES, AES, 3DES, RSA, RC4
- standarde pentru funcții matematice de tip hash: MD5,SHA1,HMAC
- standarde pentru semnături digitale: DSA, RSA
- standarde pentru criptarea în rețele wireless: WEP, WPA, WPA2
- standarde pentru criptarea în rețele GSM: A5/1, A5/2
- standarde pentru securitatea rețelelor Internet: documente RFC
- standarde pentru autentificare: Kerberos, RADIUS
- standarde pentru protocoale de conectare la servere: SSH

1.6 Teme şi exerciții

1. Să se descrie cîteva sisteme în care se foloseşte criptarea. Să se explice de ce acest lucru este necesar în aceste cazuri.

1.7 Bibliografie

1. Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Wiley, 1996, ISBN 978-0471117094.

2. Gordon, John, "The Story of Alice and Bob", after dinner speech at The Zurich Seminar , April 1984, (online http://downlode.org/Etext/alicebob.html).

3. Shirey, N., "Internet Security Glossary, Version 2", RFC 4949. August 2007, (online http://tools.ietf.org/html/rfc4949).

4. Kessler, Gary C., "An Overview of Cryptography", Hanbook on Local Area Networks, Auerbach, 1999.

5. Kessler, Gary C., "An Overview of Cryptography", (online 2013 http://www.garykessler.net/library/crypto.html).