Informatica Aplicata

(Utilizarea Calculatoarelor si Servicii Internet)

Sl.dr.ing. Serban Oprisescu

Securitate

SECURITATEA INFORMATIILOR PE INTERNET

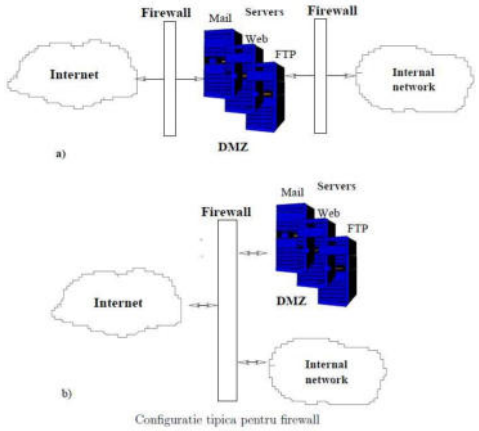
Securitatea informatiilor pe Internet

- firewall-uri
- criptografie

Firewall-uri

- fire wall - (zid de foc) <=>zid ignifug
  - receptioneaza,
  - analizeaza si
  - iau decizii pentru toate pachetele sosite inainte ca acestea sa ajunga in celelalte parti ale retelei interne.
- este primul program care receptioneaza si prelucreaza traficul de intrare, si este ultimul care prelucreaza traficul de iesire

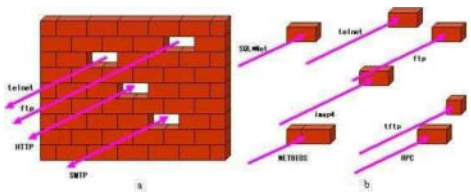
Firewall-uri



Configuratie tipica pentru firewall

Firewall-uri

- tipuri de firewall:
  - la nivel aplicatie (proxy-uri) - complex
  - la nivel retea (filtrare de pachete)
- politici de filtrare
  - permite sau refuza pachetul pe baza adresei sursa
  - permite sau refuza pachetul pe baza portului destinatie
  - permite sau refuza pachetele pe baza protocolului utilizat.



Criptografia

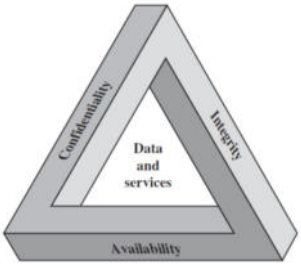
- problema securitatii datelor transmise prin Internet
- exemple ce necesita protectie:
  - informatii despre carti de credit
  - corespondenta privata sau secreta
  - date personale, informatii secrete ale unor companii
  - informatii legate de conturi bancare, trimise in timpul unor tranzactii
- criptarea datelor, adica procesul de codare a informatiei astfel incat numai cel care detine cheia sa poata decripta datele

7

Noțiuni de securitate informatică*

Securitatea unui sistem informatic = Protecția acordată unui sistem informatic, în scopul de a atinge obiectivele de menținere a integrității, disponibilității și confidențialității resurselor sistemului (hardware, software, firmware, informații / date și transmiterea lor).

Confidențialitate: datele să nu fie dezvăluite persoanelor neautorizate / dreptul individual de a dezvălui date personale.
Integritate: informația să nu fie alterată / modificată voit și neautorizat; sistemul informatic să funcționeze fără intervenții neautorizate.
Disponibilitate: sistemul să poată funcționa optim și fără întreruperi.



*William Stallings, Network Security Essentials, ediția a 4-a

8

Noțiuni de securitate informatică

Concepte adiționale

- **Autenticitate**: proprietatea de a fi autentic verificabil și de încredere; încrederea în autenticitatea unei transmisii, unui mesaj. Autentificarea utilizatorilor.
- **Responsabilitate**: Un sistem trebuie să păstreze log-uri pentru a putea identifica și izola tentativele de intruziune neautorizată și de a descoperi sursa acestora.

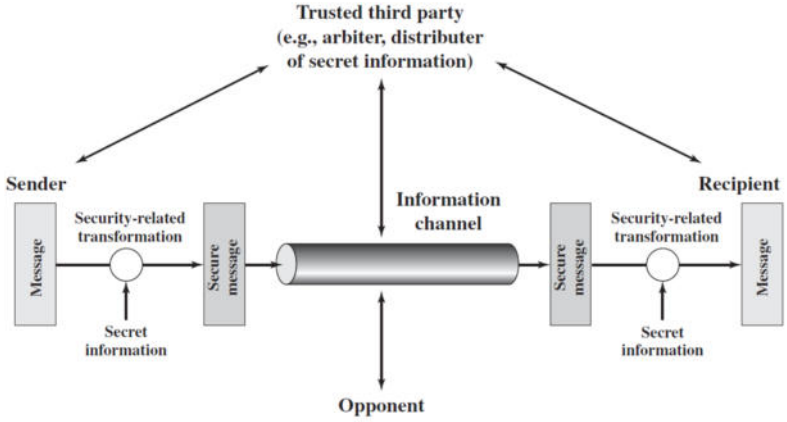
La dezvoltarea unui mecanism / algoritm de securitate trebuie întotdeauna luate în calcul toate atacurile posibile asupra mecanismelor vizate.

9

Noțiuni de securitate informatică

Tipuri de atacuri:

- **Atacuri pasive:** ”ascultarea” pe traseul informației / analiza statistica a traficului
- **Atacuri active:**
  - mascaradă = o terță parte își alocă o falsă identitate
  - modificarea mesajelor = schimbarea de nume, date, sume, destinație etc.
  - denial of service = atac asupra disponibilității unui sistem



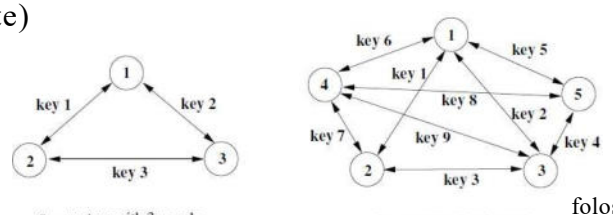
10

Criptografia

- Fiecare sistem de criptare contine 4 parti fundamentale:
  - mesajul ce trebuie criptat
  - mesajul criptat
  - algoritmul de criptare, ce este o functie matematica folosita pentru criptarea unui mesaj
  - cheia (sau cheile), ce poate fi un numar, un cuvant sau o fraza ce este utilizat in algoritmul de criptare.

Criptografia cu cheie privata

- expeditorul si destinatarul folosesc **aceeasi cheie** comuna
- distributia cheii
- este denumita si **criptografie simetrica**
- presupune existenta unei cai sigure de a transmite datele, (care daca exista atunci nu mai are sens transmiterea cheii secrete)



a – system with 3 people

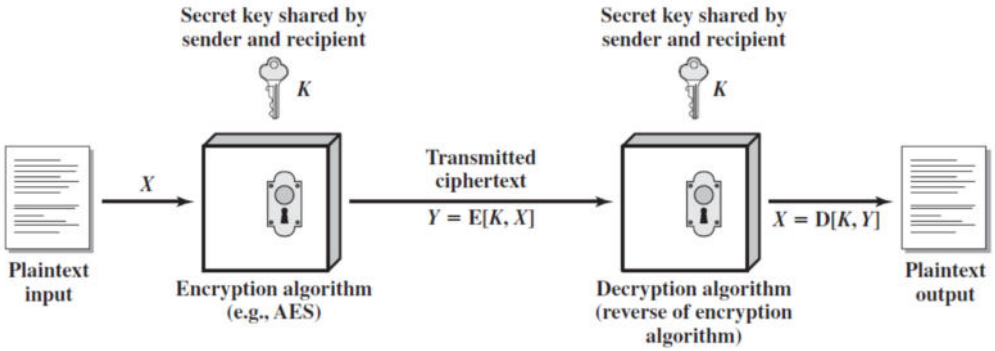
b – system with 5 people

Criptografia cu cheie secreta

folosirea unui centru de distribuire a cheilor

Criptarea simetrică*

3 Componente: mesaj (plaintext), algoritm de criptare și cheie secretă.



Mesajul cifrat (ciphertext) depinde de plaintext și de cheia secretă.

Cerințe:

- adversarul să nu poată decripta mesajul nici afla cheia dacă se află în posesia mesajului cifrat, chiar dacă are câteva perechi plaintext - ciphertext.
- cheia secretă trebuie distribuită într-un mod securizat.
- algoritmul folosit este de obicei public și ușor implementabil hard.

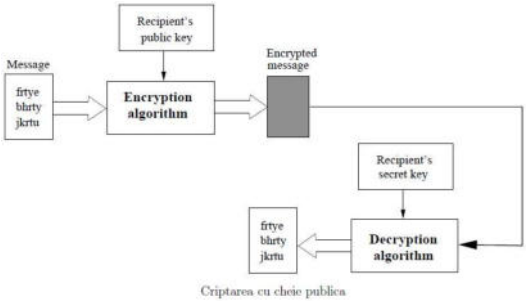
*William Stallings, Network Security Essentials, ediția a 4-a

Criptografia cu cheie privata

- Algoritmii utilizati in criptarea cu cheie secreta
  - DES: Data Encryption Standard - utilizeaza o cheie pe 56 de biti.
  - 3DES (triple DES), care utilizeaza chei pe 112 biti, utilizeaza algoritmul DES de 3 ori, cu 2 chei diferite.
  - RC2, RC4: Rivest's Code, este denumit dupa coinventatorul algoritmului cu cheie publica RSA
  - IDEA (International Data Encryption Algorithm). Utilizeaza cheie pe 128 de biti
  - AES: Advanced Encryption Standard, standard de criptare anuntat in octombrie 2000. Se utilizeaza chei de 128, 192 sau 256 de biti.

Criptografia cu cheie publica

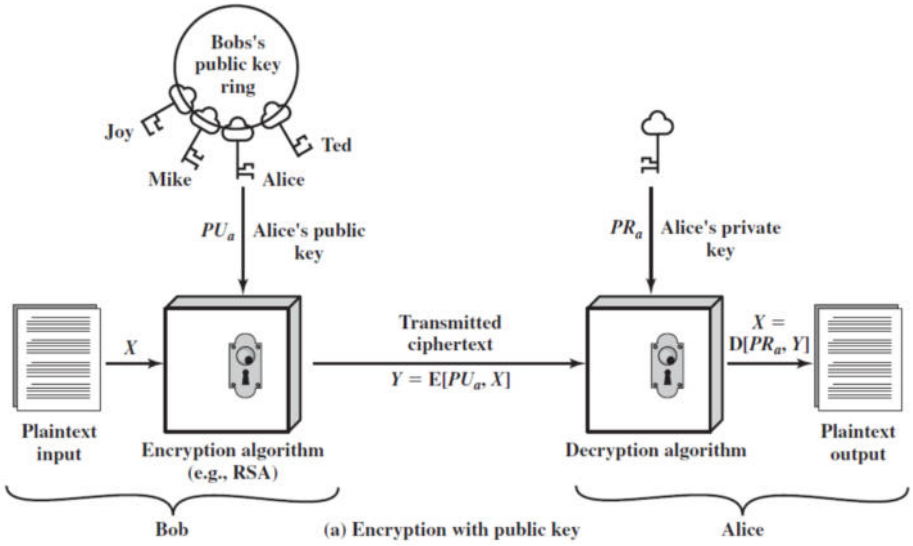
- printr-un proces matematic se creaza doua chei separate. Unmesaj criptat cu una din chei poate fi decriptata cu cealalta cheie.
- prima cheie, cea folosita pentru criptare este cheia publica, si cealalta folosita pentru decriptare este cheia secreta
- **criptografie asimetrica**
- algoritmul RSA (Rivest-Shamir-Adleman)



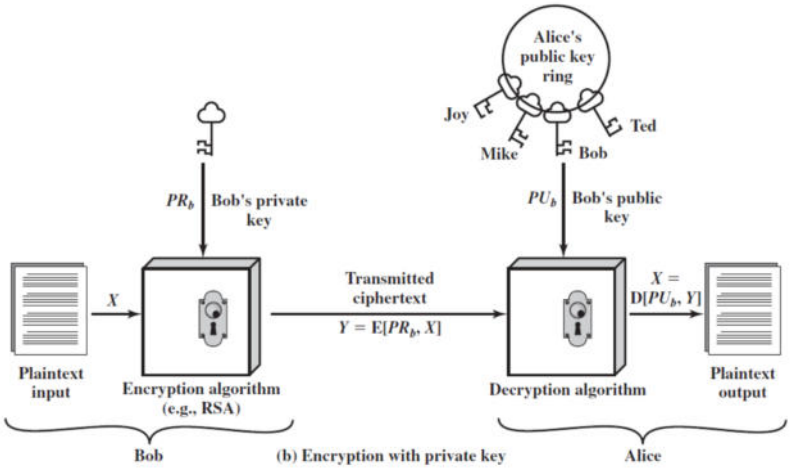
Criptarea cu cheie publica

Criptografia cu cheie publică

Propusă inițial de Diffie și Hellman în 1976 este un concept revoluționar.
Algoritmii se bazează pe funcții matematice și nu pe operații binare.
Se folosesc **două chei** diferite: **1 cheie publică** și **1 cheie privată**.



Criptografia cu cheie publică



Una din chei de folosește pentru criptare, iar cealaltă pentru decriptare.
Cheia privată este menținută secretă, iar cea publică se distribuie.
Ex: figura (a) mesajul criptat cu PUa poate fi decriptat doar cu PRa.
Fig (b): mesajul criptat cu PRb poate fi decriptat doar cu PUb.

17

Criptografia cu cheie publică

Aplicații ale criptografiei cu cheie publică:

- Criptare / decriptare clasică (în general mai lentă decât cea simetrică)
- Semnătură digitală – semnarea mesajului = criptarea cu cheia privată a mesajului sau a codului hash al mesajului
- Schimbul de chei între părți.

Algoritm	Criptare/ Decriptare	Semnătură digitală	Schimb de chei
RSA	Da	Da	Da
Diffie-Hellman	Nu	Nu	Da
DSS	Nu	Da	Nu
Curbe eliptice	Da	Da	Da

Cerințe de bază:

- O cheie nu poate fi dedusă din perechea ei
- Mesajul nu poate fi decriptat cunoscând cheia publică și mesajul criptat
- Este ușor de generat o pereche de chei (privată și publică)

18

Opțional: semnătura digitală