

Securitatea sistemelor informatice

Principiile de baza ale securitatii

Curs 1

Anul III, Informatica
2022-2023

Adela Georgescu
Facultatea de Matematica – Informatica
Universitatea Bucuresti



Informatii administrative

- Cadre didactice



Adela Georgescu

adela@fmi.unibuc.ro adela.georgescu@unibuc.ro

Laborator

George Teseleanu, Paul Cotan,
Daniel Popescu, Cristian Matei

Organizarea si evaluare

1. Organizare:

- » 2h curs / sapt
- » 2h laborator / sapt

2. Evaluare

- » 3p teme laborator
- » 1p teme Moodle
- » 6p examen scris




3. Conditii de promovare

$\geq 5p$

- **Moodle** – materiale de curs si laborator



Securitatea sistemelor informatice este esentiala

- Atacuri recente:
 - ✓  2021 – datele a 700 milioane (92%) utilizatori au fost expuse
 - ✓  2019 – datele a 533 milioane utilizatori au fost expuse
 - ✓  2018 – toate parolele utilizatorilor accesibile rețelei interne
- ...si multe altele

Securitatea sistemelor informatice este esentiala

- Atacuri mai vechi: HeartBleed
- Vulnerabilitate grava in libraria criptografica OpenSSL
 - Lipsa verificarii marginilor inainte de a copia in memorie un input “ne-sanitizat”
 - O eroare de **implementare**, iar nu de criptografie
- Permite oricui de pe internet sa citeasca memoria sistemelor protejate de versiunile vulnerabile OpenSSL
 - Chei secrete
 - Parole
 - Pachete decriptate primite prin conexiunea SSL
- Descoperit in martie 2014, existent din 2012



Top 10 produse vulnerabile in 2022

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	6879
2	Android	Google	OS	4639
3	Fedora	Fedoraproject	OS	3645
4	Ubuntu Linux	Canonical	OS	3555
5	Mac Os X	Apple	OS	3019
6	Linux Kernel	Linux	OS	2942
7	Windows 10	Microsoft	OS	2889
8	Iphone Os	Apple	OS	2738
9	Windows Server 2016	Microsoft	OS	2676
10	Chrome	Google	Application	2518

Sursa: <https://www.cvedetails.com/top-50-products.php?year=2022>

CVE (Common Vulnerabilities and Exposures) Program – identifica, catalogheaza vulnerabilitatile cibernetice

Domenii de securitate

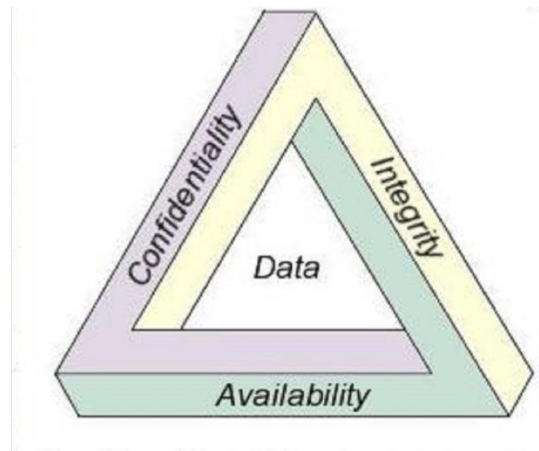
- **Computer Security** – protejeaza date si resurse (de regula se refera la sistemele computerizate)
 - Security policies, access control, malware etc.
- **Network Security** – protejeaza date in timpul transmisiei si comunicarii
- **Web Security** – protectie fata de un atacator web
- **Software Security** - protejeaza software-ul folosit intr-un sistem computerizat

Structura cursului

- Introducere in securitate: principii generale
- Introducere in criptografie, criptografia istorica
- Criptografia cu cheie secreta: criptare, coduri de autentificare a mesajelor, hashing
- Criptografia cu cheie publica: criptare, semnaturi digitale
- PKI, protocoale de securitate pentru retele (TLS)

Amenințări și obiectivele securității

- Triada C-I-A (confidentiality, integrity, availability)
- **Confidentialitate** – bunurile protejate pot fi *vazute* doar de persoanele autorizate
- **Integritate** - bunurile protejate pot fi *modificate* doar de persoanele autorizate
- **Disponibilitate (availability)** - bunurile protejate pot fi *utilizate* doar de persoanele autorizate



Principiile securitatii

- Criptografice

- ✓ Principiul lui Kerkoff: doar cheia este secreta, constructia (algoritmul) e publica
- ✓ Principiul separarii cheilor: chei diferite pentru scopuri diferite
- ✓ Principiul diversitatii: foloseste tipuri diferite de algoritmi

Principiile securitatii

- Alte principii
 - Principiul simplitatii: keep it simple
 - **Securitate implicita** (*security by default*):
trebuie gandita de la inceput, iar nu adaugata mai tarziu

Principiile securitatii

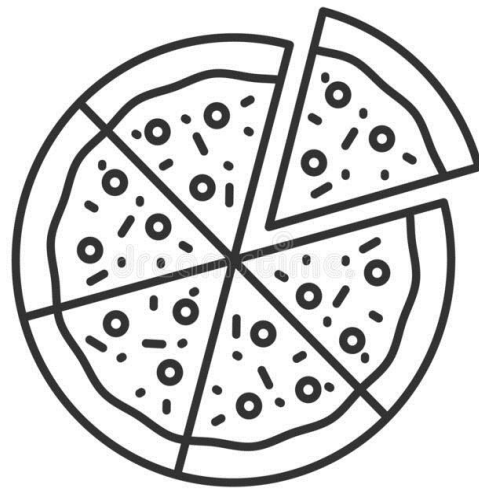
- Alte principii

- Principiul increderii minime (*principle of minimal trust*): minimizarea numarului de entitati carora le acordam incredere
- Principiul celei mai slabe verigi (*principle of the weakest link*): securitatea unui sistem este data de punctul sau cel mai slab
- Principiul celui mai mic privilegiu (*least privilege*): se acorda **exact** privilegiul necesar pentru efectuarea unei activitati

Principiile securitatii

- Principiul modularitatii: totul trebuie pastrat modular
- Defence in depth – securitate la diverse nivele

Criptografie si Securitate

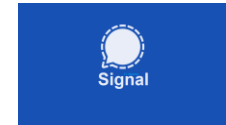


Criptografie

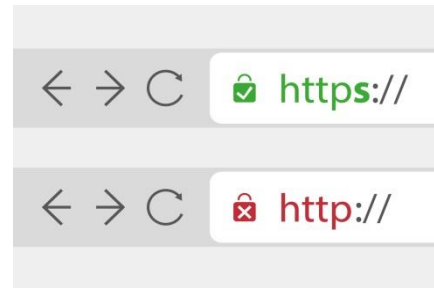
Securitate

Criptografia cotidiana

- Aplicatii de mesagerie



- Acces internet prin https



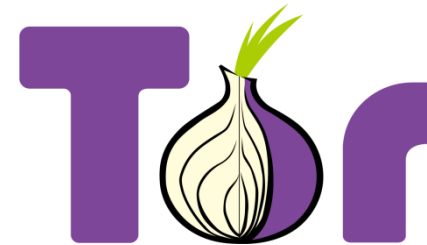
- ATM



- Bitcoin



- Tor: navigare anonima pe web



-

Cateva statistici

- 2017 - Veracode -a 2-a problema de securitate a aplicatiilor - utilizarea nesigura a criptografiei:

- Folosirea de algoritmi criptografici nesiguri (MD5, DES, etc.)



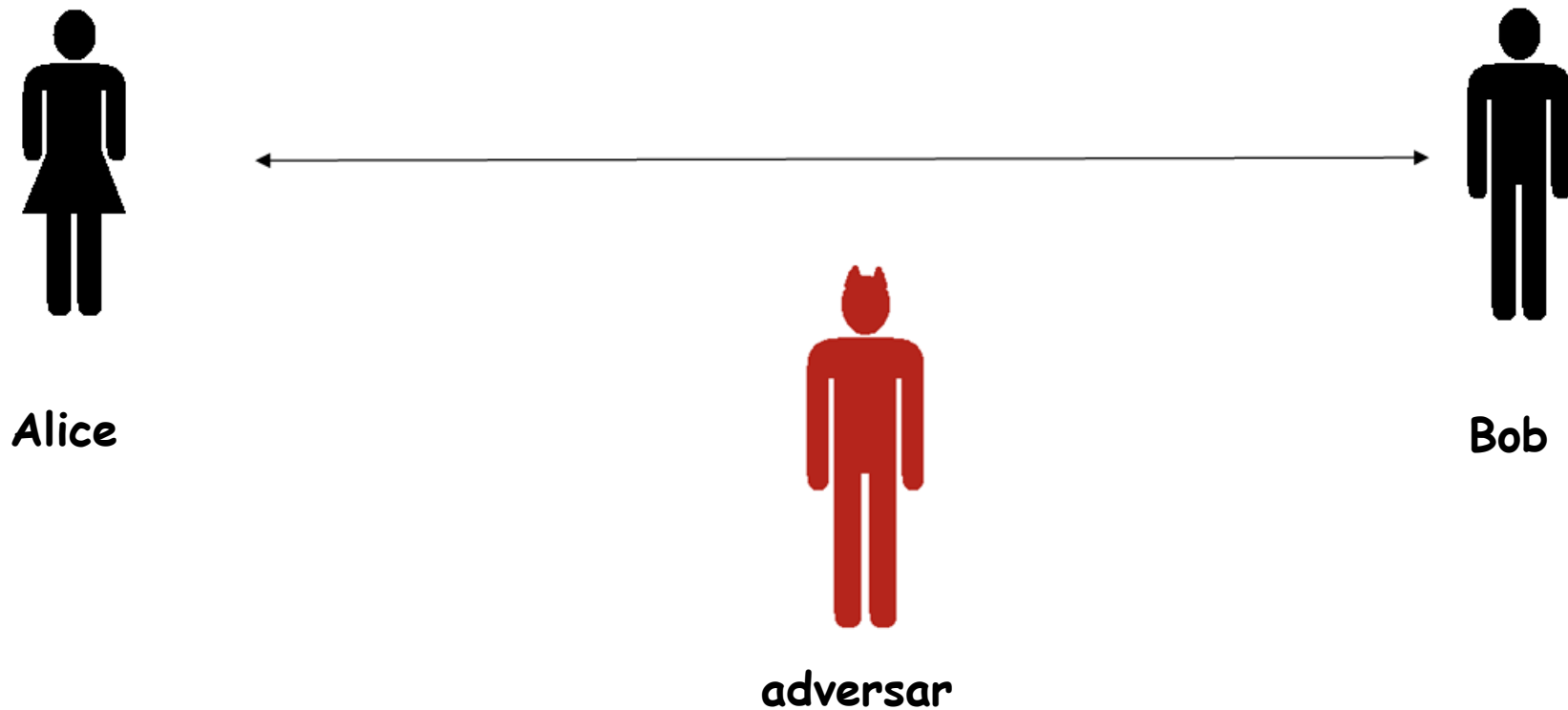
- Validarea necorespunzatoare a certificatelor



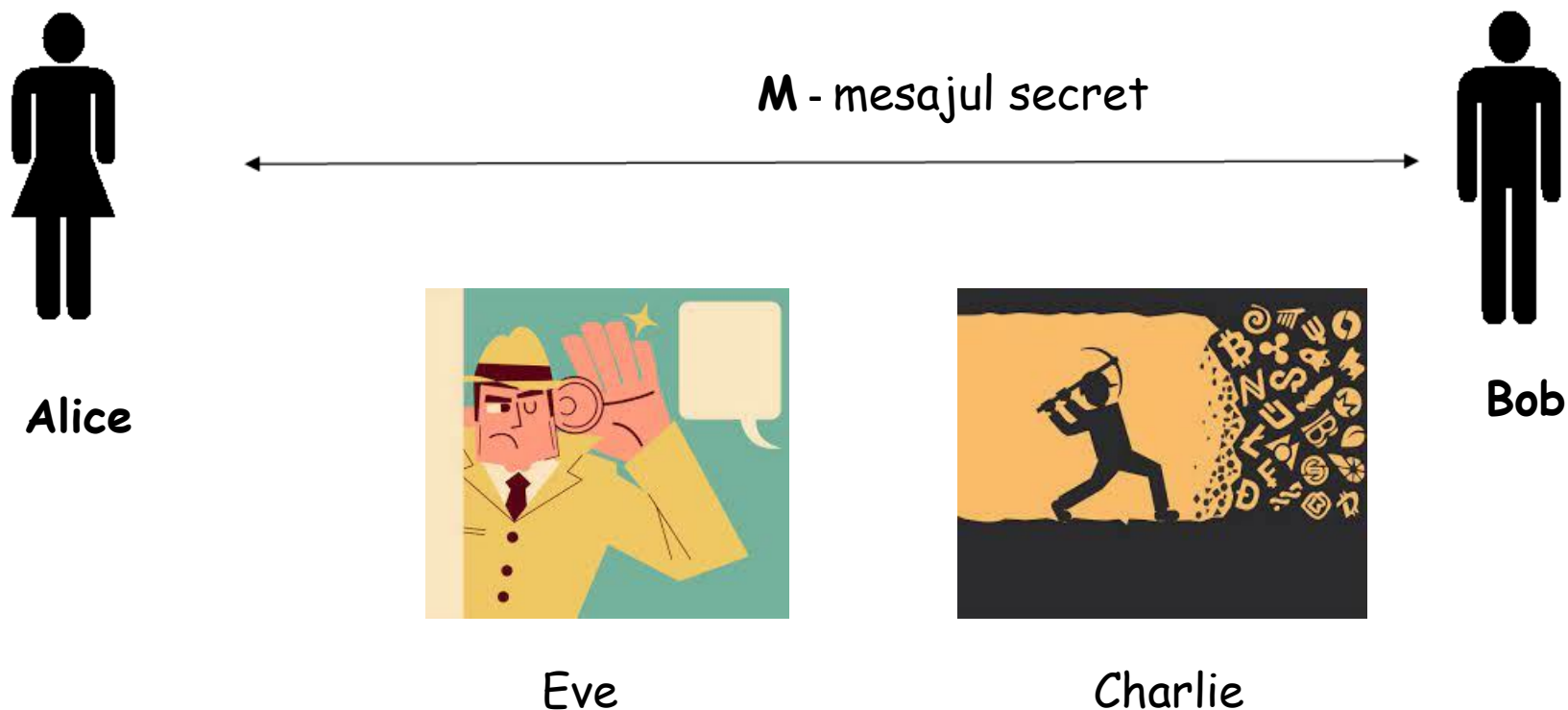
- Stocarea de informatii sensibile in clar
- Putere de criptare neadecvata



Ce este criptografia?



Ce este criptografia?



Inercarea de a mentine proprietatile de securitate in prezenta unui **adversar** pasiv sau activ.

CRIPTOLOGIE



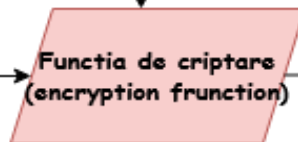
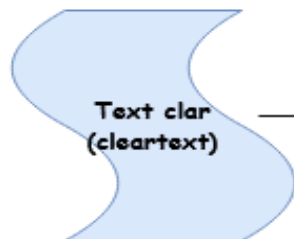
Terminologie

k_e - cheie criptare



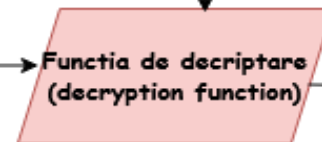
Alice

k_e



Bob

k_d

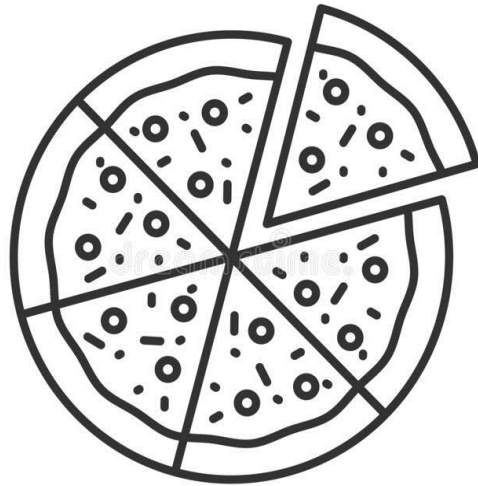


Criptografie simetrica (cheie secreta) :
 $k_e = k_d$
Criptografie asimetrica (cheie publica):
 k_e publica, k_d secreta



Principiul lui Kerckhoff:
funcția de
criptare/decriptare **publica**,
cheia **secreta**

Criptografie si Securitate



Criptografie

Securitate

- **Criptografie**: cum folosim k_e si k_d ca sa asiguram securitatea comunicatiilor pe un canal nesigur
- **Securitate**: cum protejeaza calculatorul/sistemul cheile stocate k_e si k_d de diverse atacuri (virusi, viermi etc.)

Criptografia clasica vs. criptografia moderna

Criptografia
istorica

Criptografia
moderna

1980

- comunicatii secrete
- criptografia ca o arta
- rezervata doar
organizatiilor militare

- criptografia ca o stiinta
- include multe altele pe
langa comunicatii secrete
- disponibila tuturor

Scopul si obiectivele criptografiei

Vom fi interesati sa:

- Definim scopurile de securitate → Principiul 1: definitii formale
- Invatam sa construim algoritmi de criptare si decriptare
- Ne asiguram ca acesti algoritmi de criptare isi ating scopul → Principiul 3: demonstratii de securitate

Ce proprietati de securitate asigura criptografia?

- **Confidentialitatea (mesajelor)** - adversarul nu vede sau nu poate obtine mesajul M
- **Integritatea (mesajelor)** - Alice (sau Bob) trebuie sa isi dea seama daca mesajul primit a fost modificat - asigurata de **MAC sau semnaturi digitale**
- **Autentificarea (expeditorului si a mesajului)** - Bob trebuie sa poata verifica ca mesajul provine de la Alice
- **Ne-repudierea** - Alice nu poate nega ca a trimis mesajul lui Bob

Ce proprietati de securitate
asigura criptografia?

Retineti:

- confidentialitate - criptare
- integritate (fara confidentialitate) - coduri de
autentificare a mesajelor (MAC) sau semnaturi
digitale
- integritate + confidentialitate - criptare
autentificata

Criptografi castigatori ai premiului Turing

- Mai multe personalitati din domeniul criptografiei au castigat premiul Turing de-a lungul timpului.



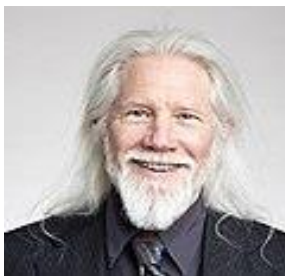
R



S



A



D



H