Curs 5

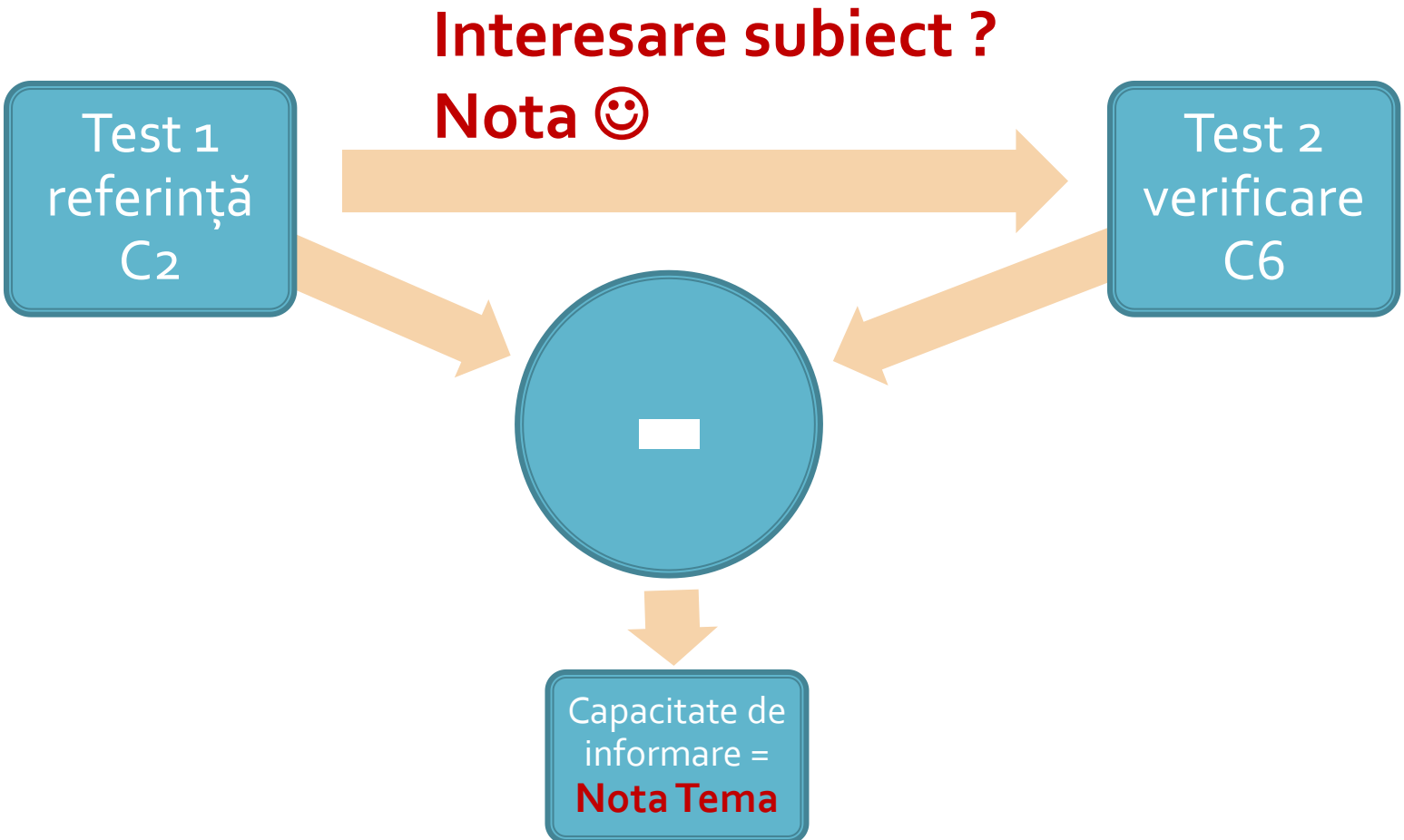
2012/2013

Tehnologii Web

Recapitulare

Tema pentru acasa

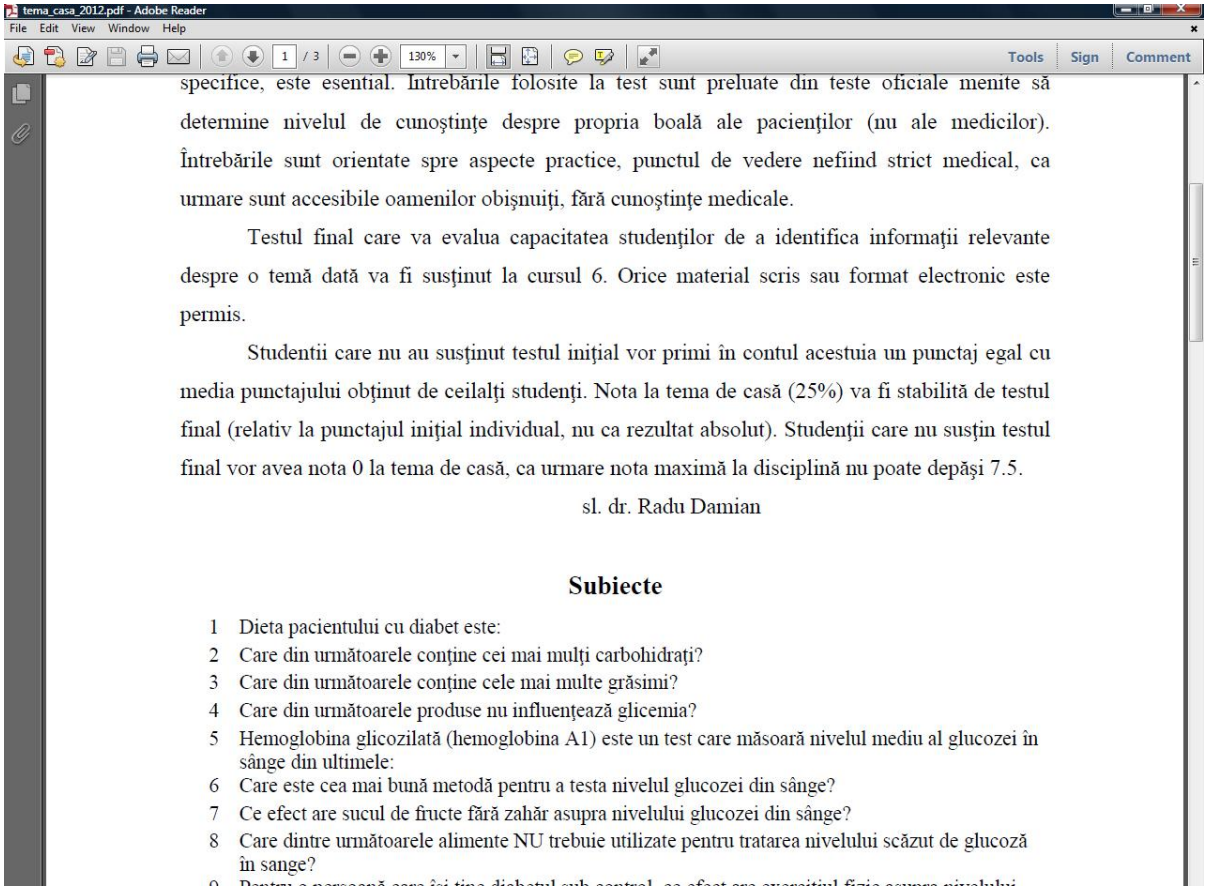
- curs 6, prezenta obligatorie, 25% din nota



Subiecte – online

http://rf-opto.etti.tuiasi.ro

Pagina in limba romana ≠ Pagina in limba engleza



specifice, este esential. Întrebările folosite la test sunt preluate din teste oficiale menite să determine nivelul de cunoştinţe despre propria boală ale pacienţilor (nu ale medicilor). Întrebările sunt orientate spre aspecte practice, punctul de vedere nefiind strict medical, ca urmare sunt accesibile oamenilor obişnuiţi, fără cunoştinţe medicale.

Testul final care va evalua capacitatea studenţilor de a identifica informaţii relevante despre o temă dată va fi susţinut la cursul 6. Orice material scris sau format electronic este permis.

Studentii care nu au susţinut testul iniţial vor primi în contul acestuia un punctaj egal cu media punctajului obţinut de ceilalţi studenţi. Nota la tema de casă (25%) va fi stabilită de testul final (relativ la punctajul iniţial individual, nu ca rezultat absolut). Studenţii care nu susţin testul final vor avea nota 0 la tema de casă, ca urmare nota maximă la disciplină nu poate depăşi 7.5.

sl. dr. Radu Damian

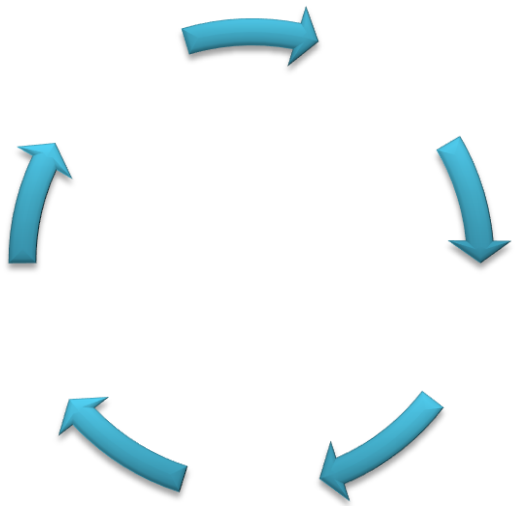
Subiecte

1 Dieta pacientului cu diabet este:
2 Care din următoarele conţine cei mai mulţi carbohidraţi?
3 Care din următoarele conţine cele mai multe grăsimi?
4 Care din următoarele produse nu influenţează glicemia?
5 Hemoglobina glicozilată (hemoglobina A1) este un test care măsoară nivelul mediu al glucozei în sânge din ultimele:
6 Care este cea mai bună metodă pentru a testa nivelul glucozei din sânge?
7 Ce efect are sucul de fructe fără zahăr asupra nivelului glucozei din sânge?
8 Care dintre următoarele alimente NU trebuie utilizate pentru tratarea nivelului scăzut de glucoză în sange?

Impresionant?

- Intel® Itanium® processors (codenamed Tukwila)
- 2 miliarde tranzistoare pe CPU
- >3 miliarde operatii pe secunda
- **Nivel redus de complexitate al operatiilor elementare**

- Un programator n-a venit la servici de **trei zile**.
- Colegii de servici au venit la el acasă şi-l găsesc pe acesta **chel**, dormind în cadă, ţinând în mâini un şampon.
- Au luat şamponul şi s-au apucat să citească instrucţiunile de folosire:
  - Clătiţi părul cu apă.
  - Aplicaţi şamponul
  - Frecaţi
  - Aşteptaţi două minute
  - Clătiţi părul cu apă
  - **Repetaţi procedura**.



Aplicatii Internet

Aplicatii Internet

- ~~Web~~
- ~~E-mail~~
- ~~Forum~~
- ~~FTP~~
- ~~Chat~~
- ~~Instant messaging~~
- ~~RSS feeds~~
- ~~Internet Time~~
- ~~P2P~~

Email

Retele de socializare - Discutii

- Care retea?
- Motive?
- Probleme?

- 1 subiect la examenul final
  - obligatoriu frecventarea macar **o data** a macar **unei** retele sociale

Concepte

Concepte

- Tipuri de date
- Malware
- Criptare
- ~~Cautare a informatiilor~~

Tipuri de date

- Web
  - HTML (.html, .htm, .asp, .php)
  - suport – Cascading style sheets, Javascript (.css, .js)
  - imagini
- Date
  - XML, RSS
  - Binare (fisiere oarecare)
  - Aplicatii
    - Java – limbaj interpretat
    - Active X (Internet Explorer)
    - Flash (.swf) – Adobe Flash Player
    - Silverlight (Microsoft)

Tipuri de date

- Documente
  - Portable Document Format (.pdf) – Adobe Reader
  - altele
- Imagini
  - Dimensiunea extrem de importanta (90 -95 % din cantitatea de date web sunt imagini)
  - Formate:
    - jpg – fotografii
    - gif – desene, animatie, transparenta
    - png – desen vectorial, transparenta

Tipuri de date

- Multimedia – streaming
  - Audio (CD: 1411.2kbs, compresat: 128-320kbs)
    - mp3 – MPEG 1 Layer 3
    - wma – Windows Media Audio
  - Video
    - avi – Audio Video Interleave
    - wmv – Windows Media Video
    - swf

Malware

- Malicious Software
  - Virus
    - cod executabil
    - reproducere si distributie daca e lansat in executie
  - Worm
    - reproducere si distributie prin transmisie activa prin retea
  - Profit
    - Spyware: aflare de informatii generale si comunicare pe internet
    - Key logger: informatii confidentiale urmate de furt
    - Dialers: acces nedorit la servicii cu plata
- Firewall si Antivirus active si la zi
- Fara click automat: Think before you click

Criptare

- Hash Value – valoare calculata cu un anumit algoritm
  - Data: 10667; Algoritm Hash: Data x 143; Valoare Hash:1525381; 143: cheie
  - Daca stiu algoritmul si valoarea Hash pot afla datele
- Sisteme de criptare
  - simetrice – aceeasi cheie utilizata la criptare/decriptare si expeditor/destinatar
  - asimetrice
    - cheie publica
    - cheie privata

Criptare

- chei asimetrice
  - cheie publica
    - a destinatarului – la criptare
    - a expeditorului – la verificarea semnaturii digitale
  - cheie privata (~ 3 ori)
    - a destinatarului – la decriptare
    - a expeditorului – la semnare digitala
- exemplu: A trimite un mesaj lui B
  - B isi face cunoscuta **oricui** cheia publica
  - A gaseste cheia publica a lui B ("lacat")
  - A cripteaza mesajul cu cheia publica a lui B ("cutie"+"lacat")
  - A trimite mesajul criptat pe cai nesigure ("posta/prieten")
  - Mesajul poate fi decriptat **numai** cu cheia privata a lui B ("cheie" pentru "lacat")

Coduri simetrice

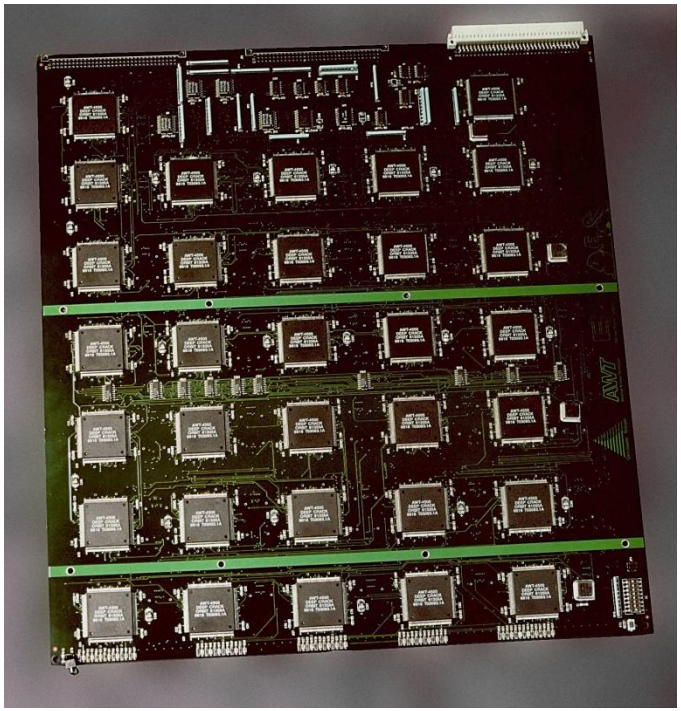
- OTP – One Time Pad – **singurul** cod dovedit matematic sigur (nepractic)
- DES (56b) Data Encryption Standard; 3DES
- AES (128, 192, 256b) Advanced Encryption Standard
- Blowfish
- Twofish (128, 192, 256b)
- Arcfour

Securitate coduri simetrice

- Forta bruta
  - 32 biti – 2^{32} pasi ~10^9 – oricine
  - 40 biti – 2^{40} pasi ~10^{12} – 1 saptamana cu 1 calculator modern
  - 56 biti – Effort substantial
    - retea de calculatoare in comun – cateva luni
    - hardware specializat (scump) – rapid: accesibil pentru
      - guverne
      - org. criminale
      - companii mari

Securitate coduri simetrice

- Forta bruta
  - 64 biti – Pot fi sparte
    - acum – guvernele mari
    - in cativa ani de:
      - guverne mici
      - org. criminale
      - companii mari
  - 80 biti – siguranta pentru cativa ani
  - 128 biti – siguranta pe viitor (10^9 pasi/s – mai mult decat varsta universului)

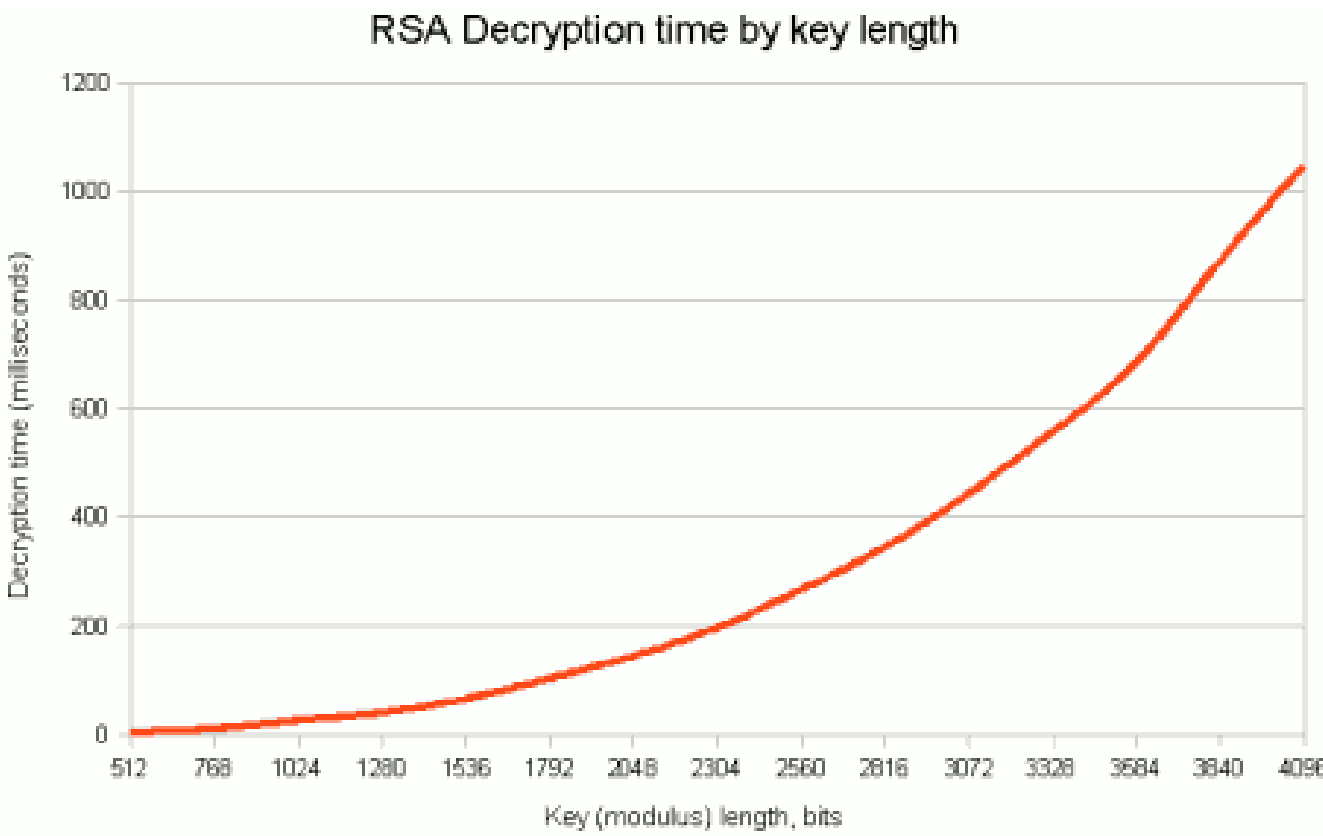


Coduri asimetrice

- DSS – Digital Signature Standard
- RSA – Rivest, Shamir, Adleman
- Forta bruta
  - 256 biti – usor de spart
  - 512 biti – retea de calculatoare in cateva luni
  - 768 biti – momentan sigure dar nu pe termen lung
  - 1024 biti – sigure pentru 5-10 ani
  - 2048 biti – sigure pentru 50 ani
  - Microsoft forteaza 1024 biti pentru certificate in Windows din Octombrie 2012

Timp necesar pentru decriptare

- Decriptare valida (cu cheie) a unui bloc de date (P4)
- 4096b – 1s

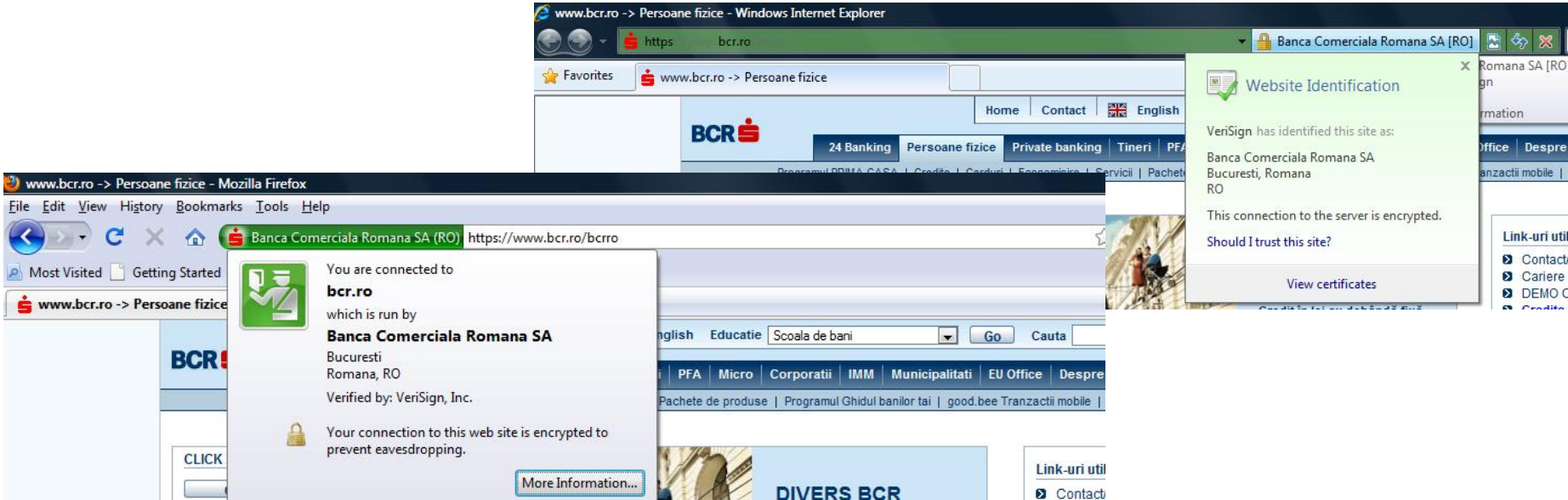


Wireless

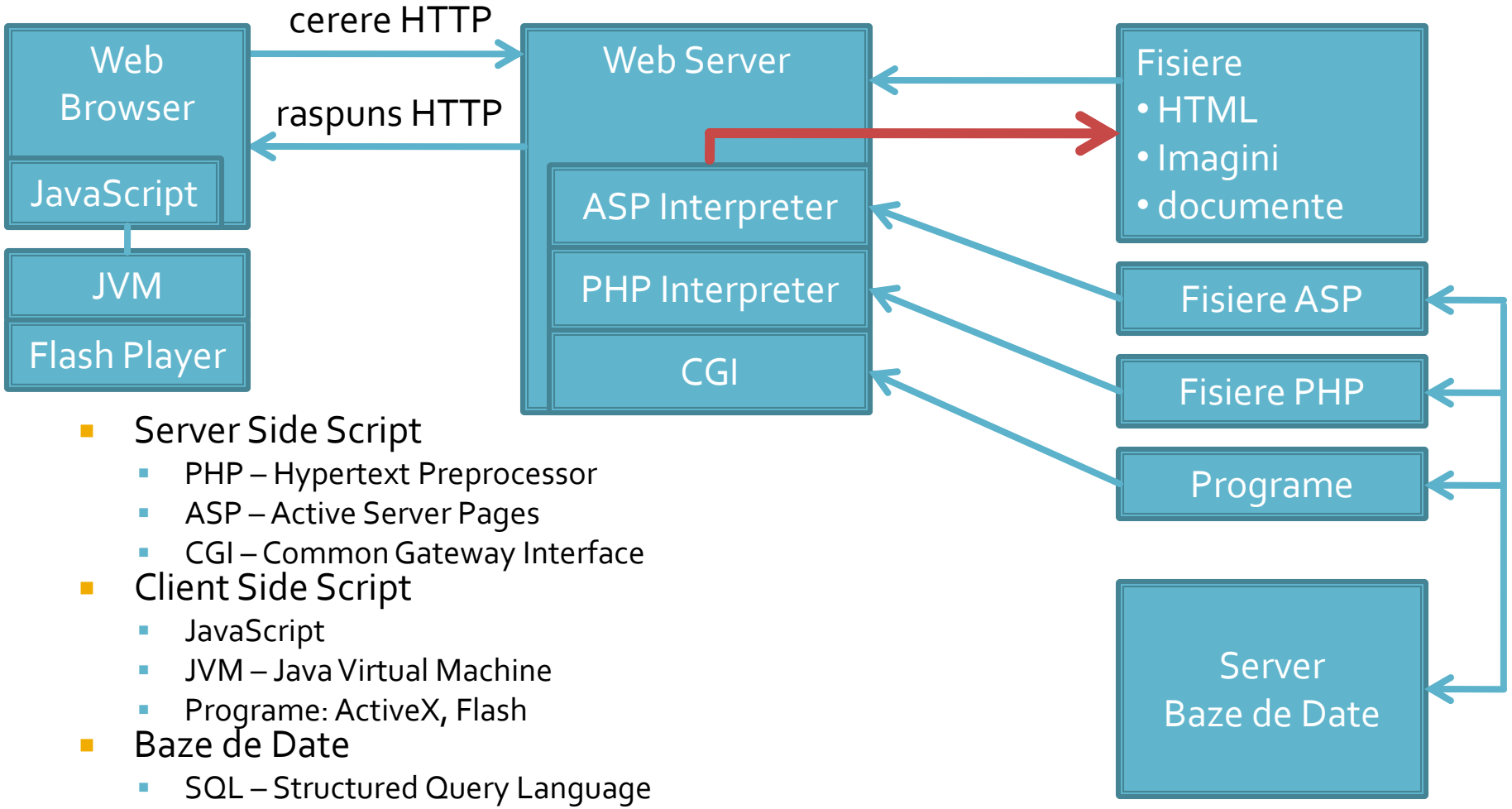
- WEP
  - Wired Equivalent Privacy
  - **Nesigur**
- WPA
  - Wi-Fi Protected Access
  - compatibil hardware cu WEP
- WPA2
  - 802.11i standard (AES)
- PSK/EAP/TKIP/AES
- End-to-End encryption (>2,3 OSI)

Certification Authorities

- Certificatele digitale asigura identitatea celui (nominalizat) care ofera o cheie publica
  - Verisign (si altele)
    - implicit acceptate
    - ~400$/an
  - Certificate proprii /Open Source
    - implicit neacceptate dar pot fi acceptate fortat



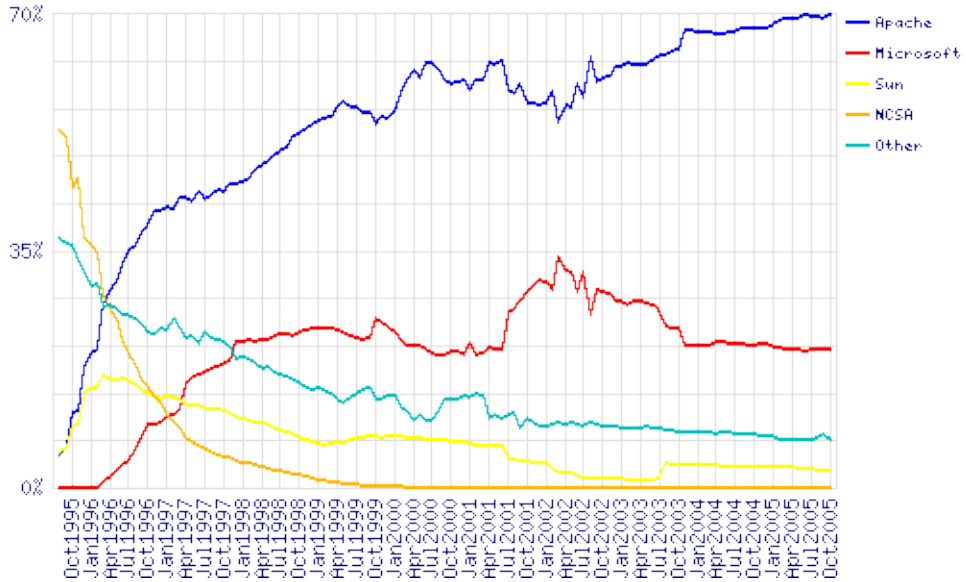
Tehnologia server-elor Web



- Server Side Script
  - PHP – Hypertext Preprocessor
  - ASP – Active Server Pages
  - CGI – Common Gateway Interface
- Client Side Script
  - JavaScript
  - JVM – Java Virtual Machine
  - Programe: ActiveX, Flash
- Baze de Date
  - SQL – Structured Query Language
  - MySql – open Source
  - Microsoft SQL Server
  - Oracle

Tehnologia server-elor Web

- PHP – Hypertext Preprocessor
  - initial – Personal Home Page
  - open source
  - C++
  - Apache
- ASP – Active Server Pages
  - Microsoft
  - VBasic
  - IIS
- Java/JavaScript
  - Sun
  - Masina Virtuala Java



HTML

HTML vs. C++

```
int i,a;
for (i=1;i<=10;i++) {
  a=2*i;
  printf("%d\n",a);
  }
```

```
<p>Text Text Text <font color="red">Text
</font>Text Text Text</p>
<p>Text <strong>Text </strong>Text Text
Text Text Text
</p>
```

- C++/Pascal/etc.
  - actiuni
  - genereaza date
- HTML/XHTML/etc.
  - forma
  - a datelor existente

HTML

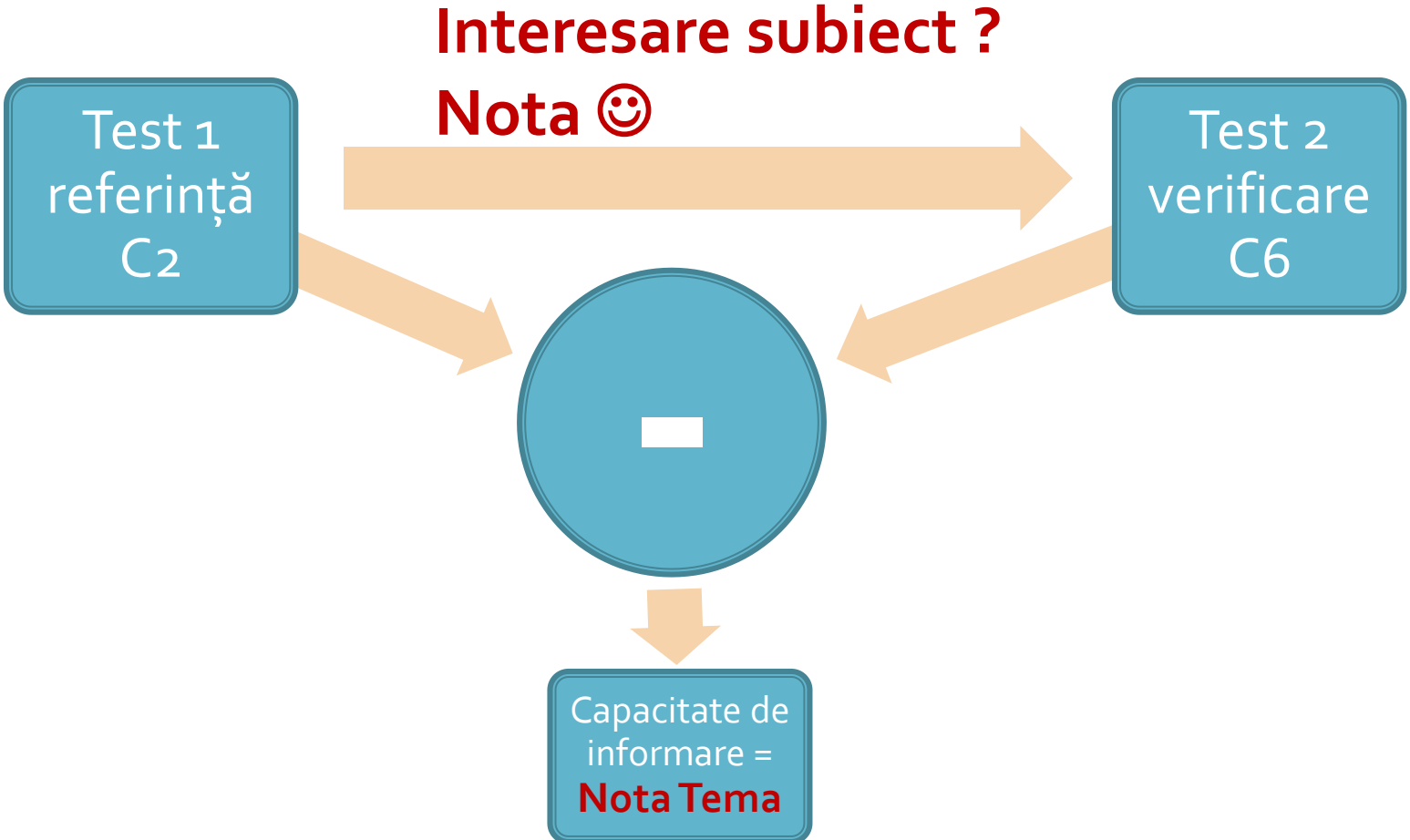
- Hyper Text Markup Language
- bazat pe SGML - Standard Generalized Markup Language (ISO 8879:1986 SGML)
- Tim Berners Lee, 1989
- Mosaic – 1993
- HTML 2.0 – Noiembrie 1995
  - IETF – Internet Engineering Task Force -> 1996
- HTML 3.0 Draft 1995
- HTML 3.2
  - WWW Consortium **http://www.w3c.org** ->1996
- HTML 4.0 – 18.12.1997
- HTML 4.01 – 24.12.1999
- HTML 5.0 Draft – Ianuarie 2008 (11, Last Call – mai 2011), oficial prevazut pentru 2014

XHTML

- bazat pe XML - Extensible Markup Language
- XHTML 1.0 – Ianuarie 2000 o reformulare a HTML 4.01 cu mici corectii pentru concordanta cu regulile XML
- XHTML 1.1 – Mai 2001
- XHTML 2.0 Draft
  - 2008 – versiunea 9
  - lipsit de suport din partea browser-elor
  - nu mentine compatibilitatea in urma cu HTML
  - "expirat"
- XHTML 5.0 Draft
  - in paralel cu HTML 5.0

Tema pentru acasa

- curs 6, prezenta obligatorie, 25% din nota

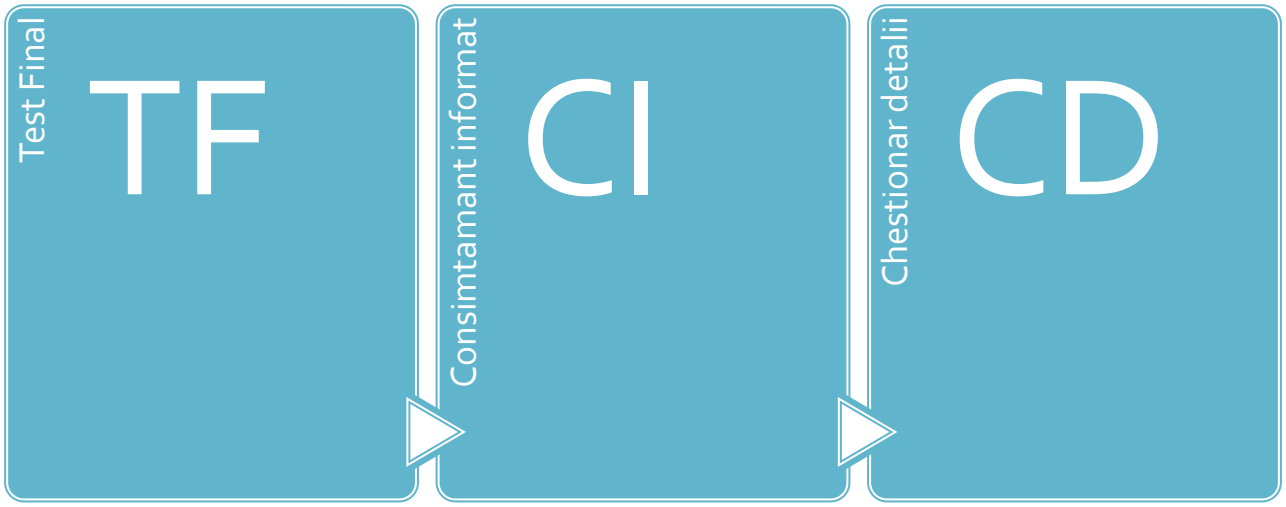


Test initial

- C2
- 38 intrebari
- rezultate: http://rf-opto.etti.tuiasi.ro
- Medie: 13.9 / 38
- 36.5%

Test final

- C6
- 38 intrebari
- Nota ← Progres (C2)



Contact

- Laboratorul de microunde si optoelectronica
- **http://rf-opto.etti.tuiasi.ro**
- **rdamian@etti.tuiasi.ro**
- tema de acasa, curs **6**, **prezenta obligatorie**, **25% din nota**