Lecture 5

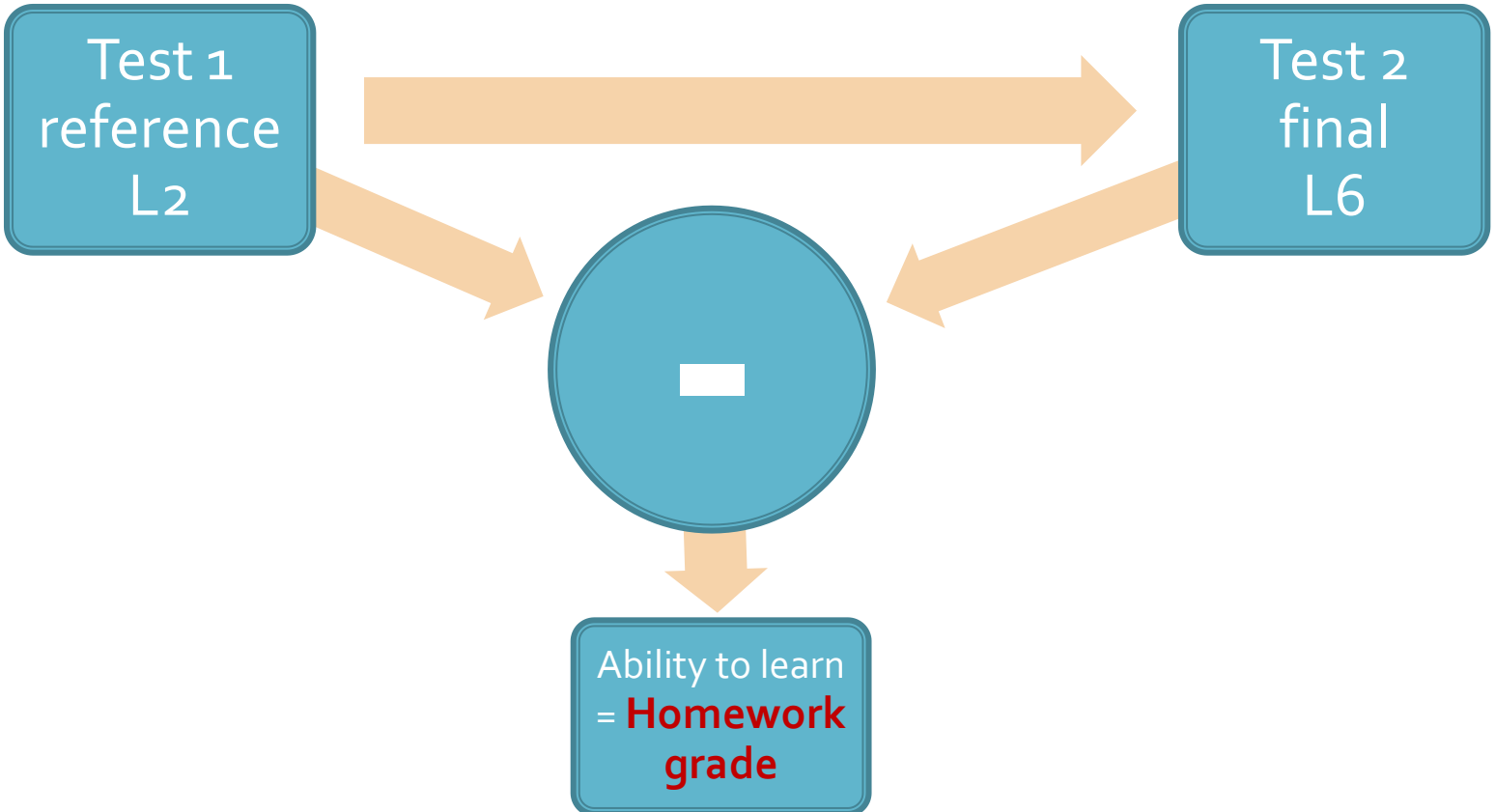
2012/2013

Internet Programming Techniques

Refresher

Homework

- lecture 6, **mandatory presence**, **25% grade**
  - **December 13, 2012**



Topics – online

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

subiecte_eng.pdf - Adobe Reader

The final test will assess students' ability to identify relevant information on a given topic by difference from the reference test (lecture 2) and will be held during lecture 6. All written and electronic materials are allowed.

Students who did not pass the reference test will receive by default an initial score equal to the average score of other students. The homework grade (25%) will be determined by the final test (relative to the individual reference score, the absolute value of the second score is irrelevant). Students who do not pass the final test will have a grade equal to 0 for the homework, thus a maximum 7.5 for the entire discipline.

sl. dr. Radu Damian

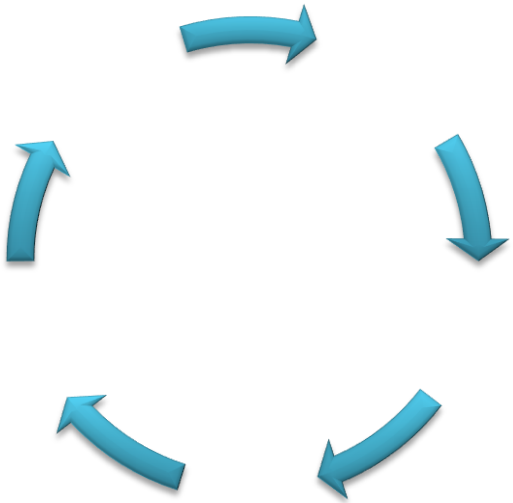
Topics

1 The diabetes diet is:
2 Which of the following is highest in carbohydrate?
3 Which of the following is highest in fat?
4 Which of the following is a "free food"?
5 Glycosylated hemoglobin (hemoglobin A1) is a test that is a measure of your average blood glucose level for the past:
6 Which is the best method for testing blood glucose?
7 What effect does unsweetened fruit juice have on blood glucose?
8 Which should NOT be used to treat low blood glucose?
9 For a person in good control, what effect does exercise have on blood glucose?
10 Infection is likely to cause:
11 For a diabetes patient, the best way to take care of his/her feet is to:
12 Eating foods lower in fat decreases the risk for:

Impressive?

- Intel® Itanium® processors (codenamed Tukwila)
- 2 billions transistors on each CPU
- >3 billions operations per second
- **Low level of complexity, elementary operations**

- 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**.



Internet Applications

Internet Applications

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

Email

Social Networks - discussions

- Which network?
- Reasons?
- Problems?

- 1 topic on the final exam!
  - obligation to attend at least **once** at least **one** social network

Other Internet Related Concepts

Searching on the Internet

Homework!

Concepts

- Data types
- Malware
- Encryption
- ~~Searching on the Internet~~

Data types

- Web
  - HTML (.html, .htm, .asp, .php)
  - support – Cascading style sheets, JavaScript (.css, .js)
  - images
- Free format data
  - XML, RSS
  - Binary (any file)
  - Software
    - Java – interpreted programming language
    - Active X (Internet Explorer)
    - Flash (.swf) – Adobe Flash Player
    - Silverlight (Microsoft)

Data types

- Documents
  - Portable Document Format (.pdf) – Adobe Reader
  - others
- Images
  - Binary size is extremely important (90 -95% of web data are images)
  - Formats:
    - jpg – photographs
    - gif – drawings, animation, transparence
    - png – vector graphics, transparence

Data types

- Multimedia – streaming
  - Audio (CD: 1411.2kbs, compressed: 128-320kbs)
    - mp3 – MPEG 1 Layer 3
    - wma – Windows Media Audio
  - Video
    - avi – Audio Video Interleave
    - wmv – Windows Media Video
    - swf
    - streaming – play **while** data arrives

Malware

- Malicious Software
  - Virus
    - executable code
    - reproduction and distribution when/if launched
  - Worm
    - reproduction and distribution by active transmission over the network
  - Profit
    - Spyware: finding basic information and disclose it over the Internet
    - Key logger: confidential information followed by theft
    - Dialers: unwanted access to paid services
- **Firewall and Antivirus: active and updated**
- No automatic click: **Think before you click**

Encryption

- Hash Value – a value computed with a certain algorithm
  - Data: 10667; Hash algorithm : Data x 143; Hash Value: 1525381; 143: Encryption key
  - If you know the algorithm and the hash value you can find the original data
- Encryption systems
  - symmetrical– the same key used for encryption/decryption and sender/recipient
  - asymmetrical
    - public key
    - private key

Encryption

- asymmetrical keys
  - public key
    - of the recipient – used on encryption
    - of the sender – used on check of digital signature
  - private key (~ 3 times larger)
    - of the recipient – used on decryption
    - of the sender – used on digitally signing
- example: A sends a message to B
  - B publishes his public key (**anyone** can know/use it)
  - A finds B's public key ("lock")
  - A encrypts the message with B's public key ("box"+"lock")
  - A sends the encrypted message via unsecured channel ("mail/friend")
  - Message can be decrypted **only** with B's private key ("key" for "lock")

Symmetric-key algorithms

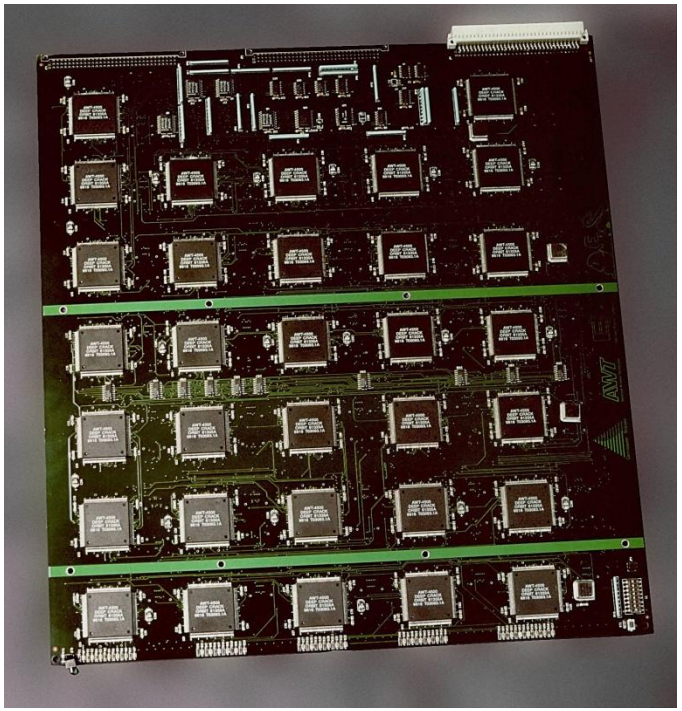
- OTP – One Time Pad – **only** algorithm mathematically proven as unbreakable (not practical)
- DES (56b) Data Encryption Standard; 3DES
- AES (128, 192, 256b) Advanced Encryption Standard
- Blowfish
- Twofish (128, 192, 256b)
- Arcfour

Symmetric-key security

- Brute force
  - 32 bits – 2^{32} steps ~10^9 – anyone
  - 40 bits – 2^{40} steps ~10^{12} – 1 week on a modern computer
  - 56 bits – Substantial effort
    - a network of computers working together – months
    - specialized hardware (expensive) – fast: accessible for:
      - governments
      - crime organizations
      - large companies

Symmetric-key security

- Brute force
  - 64 bits – on the reach of:
    - now – large governments
    - in a few years:
      - small governments
      - crime organizations
      - large companies
  - 80 bits – security for a few years
  - 128 bits – security for the future (10^9 steps/s – more than the age of the Universe to decrypt)

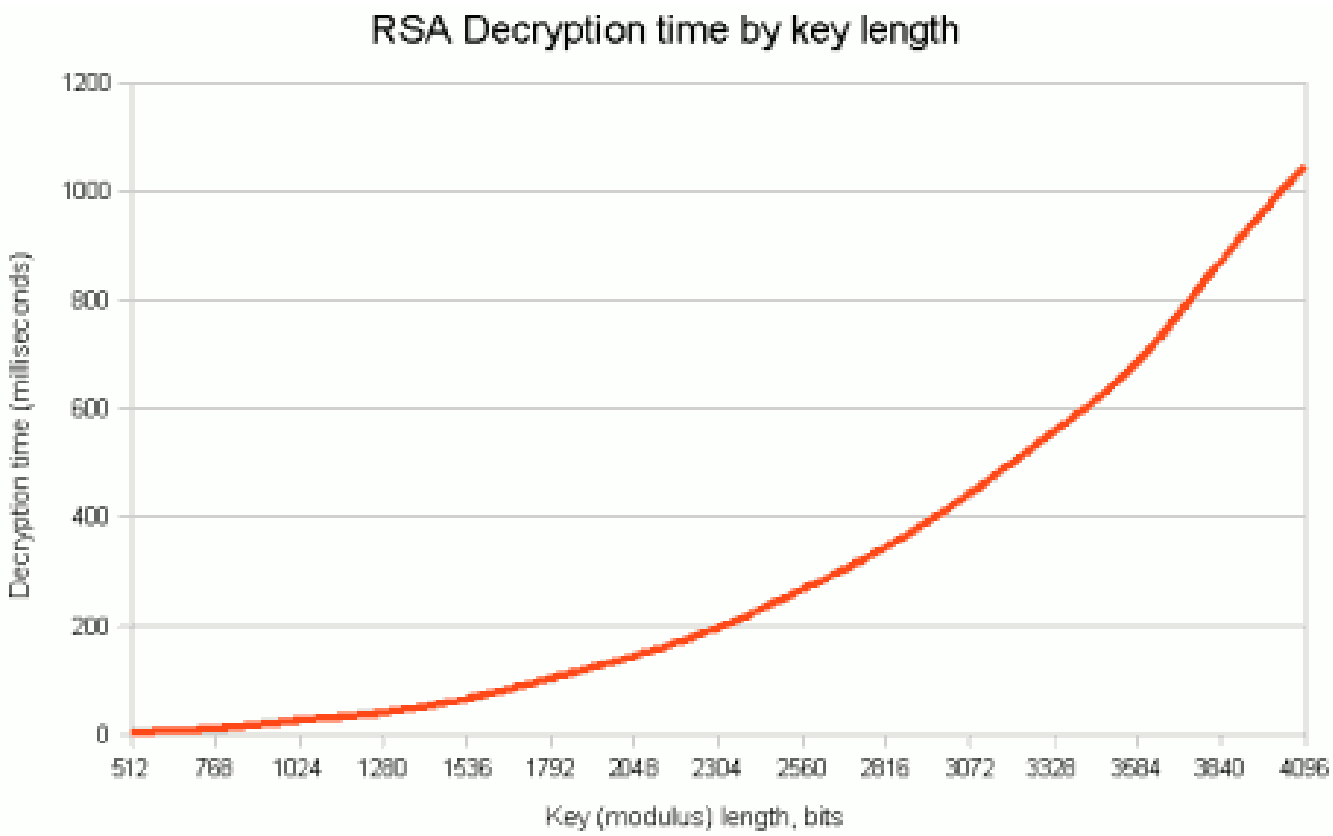


Asymmetric-key security

- DSS – Digital Signature Standard
- RSA – Rivest, Shamir, Adleman
- Brute force
  - 256 bits – easy to break
  - 512 bits – a network of computers working together – months
  - 768 bits – short term secure (not years)
  - 1024 bits – secure for 5-10 years
  - 2048 – secure for 50 years
  - Microsoft forced 1024 bits keys in Windows on October 2012

Decryption time

- Valid decryption time for a block of data (P4)
  - 4096 – 1s

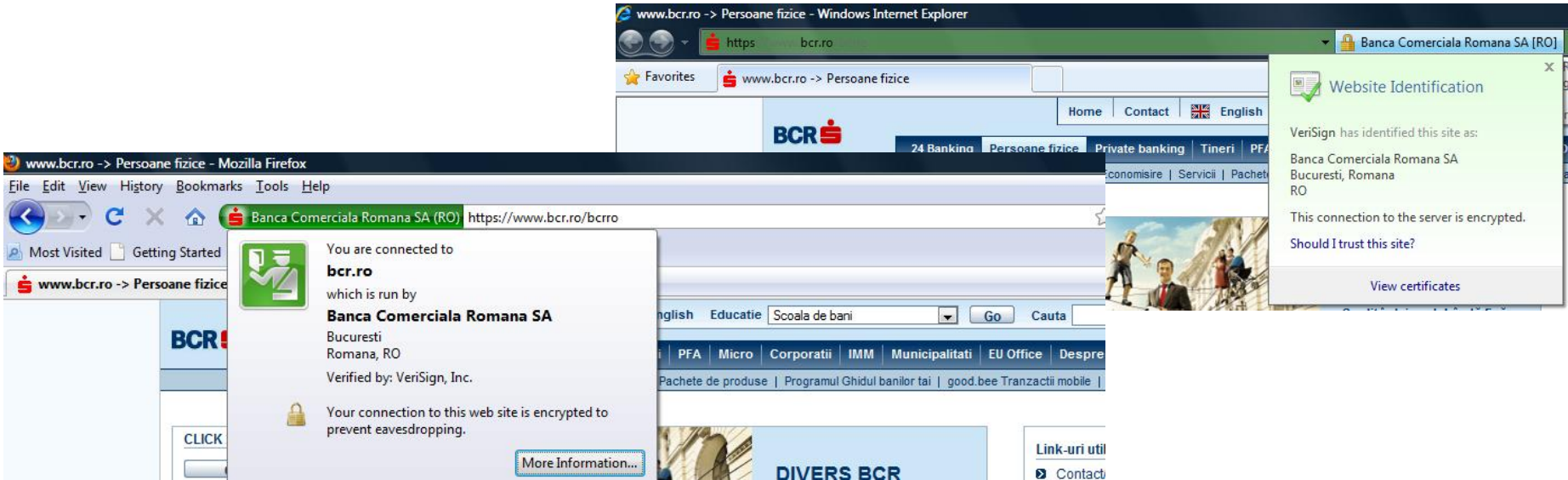


Wireless

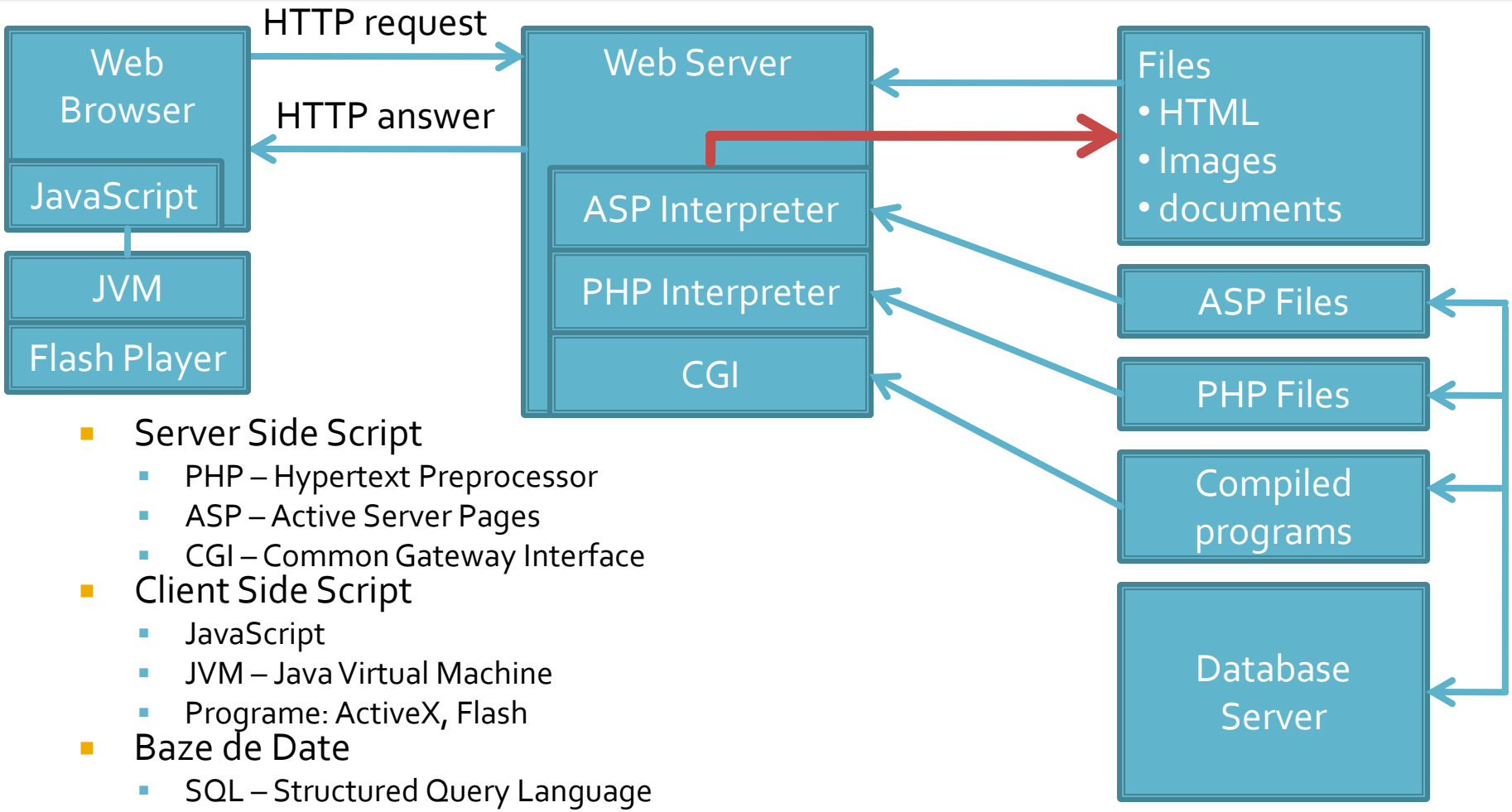
- WEP
  - Wired Equivalent Privacy
  - **Not secure**
- WPA
  - Wi-Fi Protected Access
  - hardware compatible with WEP
- WPA2
  - 802.11i standard (AES)
- PSK/EAP/TKIP/AES
- End-to-End encryption (>2,3 OSI)

Certification Authorities

- The digital certificate certifies the ownership of a public key by the named subject of the certificate
  - Verisign (and others)
    - accepted by default
    - ~400$/year
  - Open Source certificates
    - not accepted by default, but can be overridden



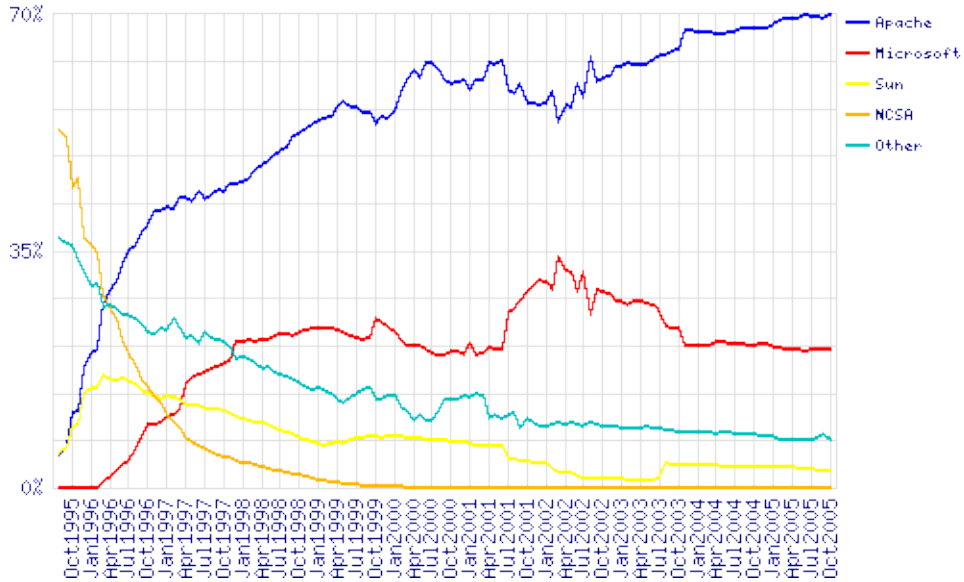
Web server Technology



- 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
  - initially – Personal Home Page
  - open source
  - C++
  - Apache
- ASP – Active Server Pages
  - Microsoft
  - VBasic
  - IIS
- Java/JavaScript
  - Sun
  - Java Virtual Machine



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.
  - actions
  - generates data
- HTML/XHTML/etc.
  - form
  - of existing data

Javascript, PHP, ASP

HTML

- Hyper Text Markup Language
- based on SGML - Standard Generalized Markup Language (ISO 8879:1986 SGML)
- Tim Berners Lee, 1989
- Mosaic – 1993
- HTML 2.0 – November 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 – January 2008 (25, October 2012), official release for 2014

XHTML

- based on XML - Extensible Markup Language
- XHTML 1.0 – January 2000 (HTML 4.01 enforcing XML syntax rules)
- XHTML 1.1 – May 2001
- XHTML 2.0 Draft
  - 2008 – v.9
  - **NO** support from major browsers
  - no backward compatibility with HTML
  - "expired"
- XHTML 5.0 Draft
  - parallel with HTML 5.0

HTML/XHTML vs XML

- XML
  - designed to **describe** data (structure/content)
  - oriented towards data **content**
  - a method to **transmit** information, platform and hardware **independent**
- HTML/XHTML
  - designed to **display** data
  - oriented towards the **form** of that data
  - a method to **display data, uniformly**, platform and hardware **independent**

HTML Concepts 1

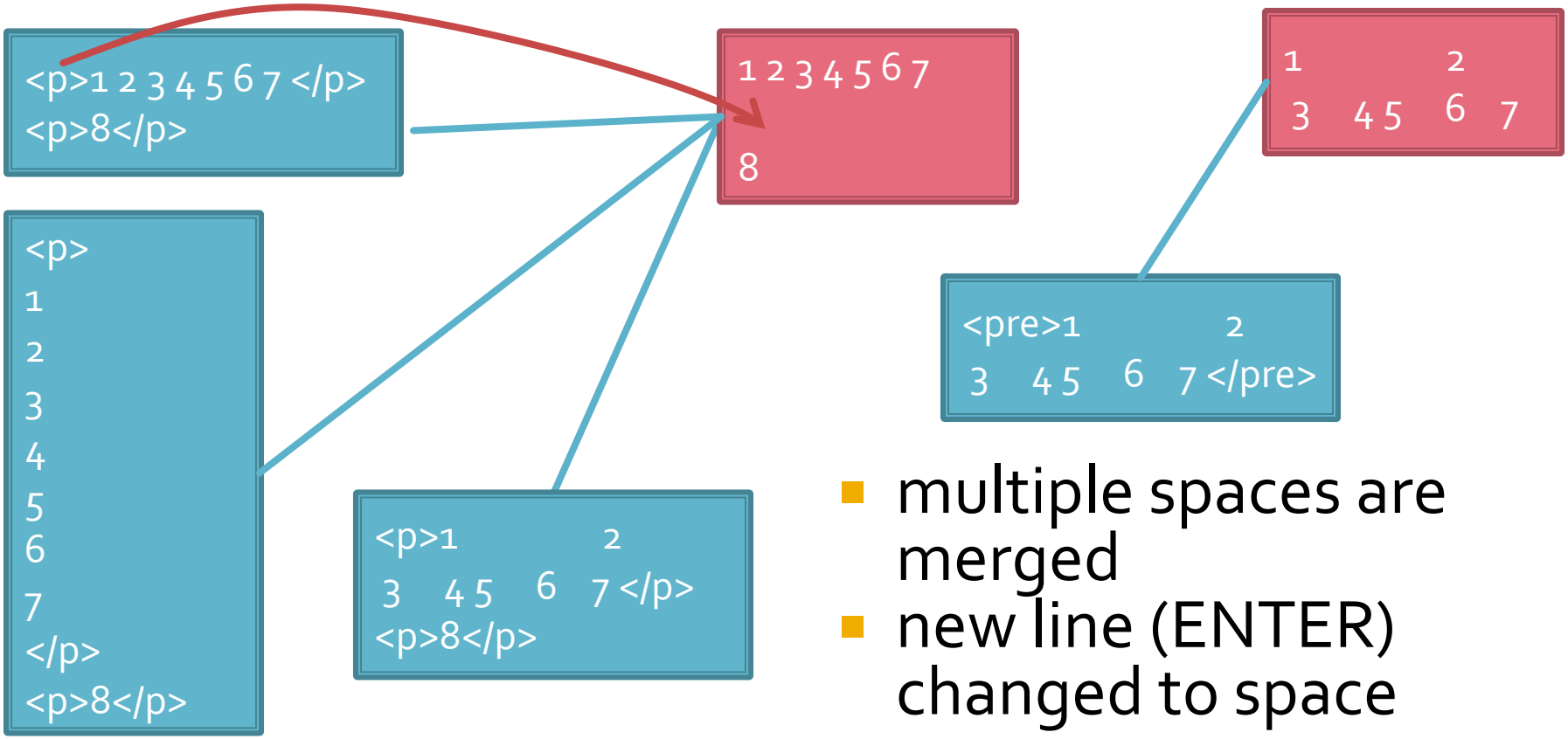
- An HTML document is an ASCII document (Notepad) containing **tags**, interpreted and displayed by browser (View Source)
- Tags: (etichete, marcaje – RO), <>
  - individual: <X/>
    - ex:
 (
 - HTML)
  - container: <X> Continut_oarecare</X>
    - ex: Un paragraf
    - Tag **X** impose the way **"Continut_oarecare"** will be displayed on the screen
    - most tags are container

HTML Concepts 2

- Case sensitivity:
  - HTML: indifferent - <html>=<HTML>=<HtMl>
  - XHTML: mandatory lower case <html>
- Comments:
  - <!-- …….. -->
  - no “--” or “>”

HTML and Format

- Format of the source document (ASCII) is irrelevant
  - only exception: <pre>....</pre>



- multiple spaces are merged
- new line (ENTER) changed to space

Minimal HTML Document

```
<!DOCTYPE .....>
<html>
<head>
....
</head>
<body>
....
</body>
</html>
```

```
<!DOCTYPE .....>
<html>
<head>
....
</head>
<frameset>
....
</frameset>
</html>
```

Attributes

- Options (properties) of the tag, used to detail the effect of that particular tag
- In container tags, introduced only in the starting tag
  - ceva
- Attributes are keywords and their name must be correctly spelled. (XML allows user defined attributes, but not HTML and XHTML)
- Attribute value, both:
  - keywords
  - user defined

Major differences XHTML vs. HTML

- Tag inclusion, mandatory
  - <X>....<Y>....</Y>.....</X>
  - <X>....<Y>....</X>.....</Y>
- Tags must be always closed
  - .... , <br />, <meta .... />
  - .... , <br>, <meta .... >
- Tags must be written in lower case
  - , <br />, <frameset>
  - <P>, <BR />, <FrAmesET>
- Attributes must be lowercase and their values written between quotation marks
  - , <table width="100">, <font color="red">
  - , <table width=100>, <font COLOR=red>
- All information must be enclosed inside <html>... </html> container tag

HTML

1. The structure of an HTML document

Structure of an HTML document

- a line containing HTML version information
- Document data: enclosed between <html> and </html>
  - Header
    - a declarative header section, generally with **NO** visual effect
    - <head> </head>
  - Document content
    - information to be displayed on the screen
    - <body> </body>
    - <frameset> </frameset>

DTD

- Document Type Definition
- First line in any HTML document conforming to:
  - **HTML 4.0 Strict DTD**
    - <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
    - no deprecated elements
  - **HTML 4.0 Transitional DTD**
    - <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
    - with deprecated elements
  - **HTML 4.0 Frameset DTD**
    - <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset //EN" "http://www.w3.org/TR/html4/frameset.dtd">
    - with deprecated elements and frames
- **Deprecated elements** – Deprecated elements are defined in the reference manual but have been outdated by newer constructs (their use is not recommended as they may become obsolete in future versions)

Minimal HTML Document

```
<!DOCTYPE .....>
<html>
<head>
....
</head>
<body>
....
</body>
</html>
```

```
<!DOCTYPE .....>
<html>
<head>
....
</head>
<frameset>
....
</frameset>
</html>
```

Header section – HEAD

- <head>…</head>
- Attributes:
  - lang: language information<head lang="ro"> …
  - dir: text direction
    - RTL <head dir="RTL">
    - LTR: default
- Contains
  - Always
    - TITLE: <title>…</title>
    - META: <meta … />
  - Usually
    - LINK: <link … />
    - SCRIPT: <script>…</script>

Header section – HEAD

- TITLE
  - <title>…</title>
  - normally, **NOT** displayed on the screen
  - browsers usually use the title (not on the page but on the title/tab bar)
  - Extremely important for search engines
    - Untitled document = ☹
- LINK
  - <link … />
  - defines support files needed to achieve intended display: css (styles), js (JavaScript)
    - <link rel="stylesheet" type="text/css" href="ea.css" />
    - <link rel="icon" href="favicon.ico" type="image/x-icon" />
- SCRIPT
  - <script>…</script>
  - introduction "on the fly" of the scripts
    - <script language="JavaScript1.2" type="text/javascript">
      <!--
      function MM_swapImgRestore() { //v3.0
      var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
      }
      //-->
      </script>

Header section – META

- <meta … />
- information **about** the document
- Attributes
  - name:
    - type of information
    - can be standard / nonstandard
  - http-equiv
    - control of HTTP protocol
  - scheme
    - standard schemes
  - content
    - actual content of the information defined previously by one of the other 3 attributes

Header section – META

- <meta name="Author" content="Radu Damian" />
- < meta http-equiv="Expires" content="Tue, 15 Oct 2008 14:25:27 GMT" />
- <meta scheme="ISBN" name="identifier" content="0-8230-2355-9" />
- <meta name="keywords" content="ceva1, ceva2, ceva3, Romania">
- <meta name="description" content="Pagina cu ceva-uri">
- <meta name="robots" content="index,follow" />
- <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
- <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-5" />
- <meta http-equiv="Content-Type" content="image/jpeg" />
- <meta http-equiv="Content-Type" content="text/plain" />

Content section – BODY

- <body>…</body>
- Specific Attributes :
  - background: background image
    - <body background = "/images/ceva.jpg">…
  - bgcolor: background uniform color
    - <body bgcolor="white" > …
  - text: text colour
    - <body text= "red">…
  - link, vlink, alink: link colors (general, visited, active)
    - < body link="red" alink="fuchsia" vlink="maroon"> …

Content section – BODY

- General Attributes :
  - lang
  - dir
  - id: unique name of the element
    - used in scripts, DOM model
    - <p id="un nume dupa care sa il gasesc la nevoie">…
  - title: information about that element
    - tooltip in browsers
    - <p title = "ceva despre element">…

Content section – BODY

- General Attributes :
  - class: belonging to a class with common characteristics
    - used with styles: CSS
    - <p class="numele clasei ale carei caracteristici vizuale le folosesc">...
  - Events
    - specific: onload, onunload
    - general: onclick, ondblclick, onmousedown, onmouseup, onmouseover, onmousemove, onmouseout, onkeypress, onkeydown, onkeyup
    - <body onload="preloadImages('images/about_f2.gif')">

Colors

- Specify colors:
  - name:
    - <font color= “black”>…
  - numeric code - # Red (0-256=00-FF), Green, Blue
    - <font color = “#FF0000”>…

Black = "#000000"
Silver = "#C0C0C0"
Gray = "#808080"
White = "#FFFFFF"
Maroon = "#800000"
Red = "#FF0000"
Purple = "#800080"
Fuchsia = "#FF00FF"

Green = "#008000"
Lime = "#00FF00"
Olive = "#808000"
Yellow = "#FFFF00"
Navy = "#000080"
Blue = "#0000FF"
Teal = "#008080"
Aqua = "#00FFFF"

Titles in text (HEADINGS)

- Very important in search engines
- 6 levels (h1 ÷ h6)
- Attributes:
  - align: text alignement = left, center, right, justify
    - <h1 align = "center">...

```
<h1>Titlu H1</h1>
<p>paragraf text normal</p>
<h2>Titlu H2</h2>
<p>paragraf text normal</p>
<h3>Titlu H3</h3>
<p>paragraf text normal</p>
<h4>Titlu H4</h4>
<p>paragraf text normal</p>
<h5>Titlu H5</h5>
<p>paragraf text normal</p>
<h6>Titlu H6</h6>
<p>paragraf text normal</p>
```

Titlu H1

paragraf text normal

Titlu H2

paragraf text normal

Titlu H3

paragraf text normal

Titlu H4

paragraf text normal

Titlu H5

paragraf text normal

Titlu H6

paragraf text normal

Grouping elements

- used to group other elements in order to implement a common action
- …
  - “inline” : group treated as a character/word
- …
  - “block-level” : group treated as a paragraph
- grouping element offer no format characteristics, and no specific attributes
- Attributes:
  - id, class
  - align

ADDRESS Element

- <address>…</address>
- may be used by authors to supply contact information for a document
- usually rendered/displayed as *italic*

```
< address >
<a href="../People/Raggett/">Dave Raggett</a>,
<a href="../People/Arnaud/">Arnaud Le Hors</a>,
contact persons for the <a href="Activity">W3C HTML
Activity</a><br/>
$Date: 1999/12/24 23:37:50 $
</ address >
```

HTML

2. Aranjarea textului

2.1. Text structurat

- …: evidentiere
  - de obicei italic
- …: evidentiere suplimentara
  - de obicei bold (ingrosat)
- <cite>…<cite>: citat
- <dfn>…</dfn> : definitii
- <code>…</code> : programe
- <samp>…</samp> : rezultat al programelor
- <kbd>…</kbd> : introducere de la tastatura
- <var>…</var> : variabile
- <abbr>…</abbr> : abrevieri
- <acronym>…</acronym> : acronime
- depreciate: …, <i>…<i>

*EM *

**STRONG **

CITE <cite>

DFN <dfn>

CODE <code>

SAMP <samp>

KBD <kbd>

VAR <var>

ABBR <abbr>

ACRONYM <acronym>

2.1. Text structurat

- Citate
  - <blockquote>…</ blockquote >: citat la nivel de bloc
    - de obicei reprezentat cu margine (indent)
  - <q>…</q> : citat in-line
    - de obicei incadrat in ghilimele sau apostroafe
  - Atribut: cite =“adresa la care se gaseste documentul citat”
- Indici/puteri
  - _… : indici
  - […] : puteri

Paragraf Normal

> They went in single file, running like hounds on a strong scent, and an eager light was in their eyes. Nearly due west the broad swath of the marching Orcs tramped its ugly slot; the sweet grass of Rohan had been bruised and blackened as they passed.

John said, “I saw Lucy at lunch, she told me ‘Mary wants you to get some ice cream on your way home.’ I think I will get some at Ben and Jerry's, on Gloucester Road.”

H_2O

10^3

```
<p>Paragraf Normal</p>
<blockquote cite="http://www.mycom.com/tolkien/twotowers.html">
<p>They went in single file, running like hounds on a strong scent,
and an eager light was in their eyes. Nearly due west the broad
swath of the marching Orcs tramped its ugly slot; the sweet grass
of Rohan had been bruised and blackened as they passed.</p>
</blockquote>
<p>John said, <q lang="en-us">I saw Lucy at lunch, she told me
<q lang="en-us">Mary wants you to get some ice cream on your way
home.</q> I think I will get some at Ben and Jerry's, on Gloucester
Road.</q></p>
<p>H<sub>2</sub>O</p>
<p>10<sup>3</sup></p>
```

2.2. Linii si paragrafe

- paragraf : …
  - atribute:
    - align = “left, center, right, justify”
- linie noua :
  - atribute:
    - clear = “none, left, right, all”
  - evitarea aparitiei unei linii noi:
    - nonbreaking space: ,   ,
- despartire in silabe:
  - Hard: - , &#x2D
  - Soft: , ,
- respectarea organizarii sursei: <pre>…</pre>

```
*********  -------
|       |  -------
| image |  --<br>
|       |
*********
-----------------

*********  -------
|       |  -------
| image |  --<br>
|       |  -------
*********  -------
```

2.3. Marcarea modificarilor

- inserare : <ins>…</ins>
  - uzual reprezentat subliniat
  - atribute (nonvizuale):
    - cite = "adresa eventualului document care explica corectia"
    - datetime = "data/timpul" la care a aparut modificarea
- eliminare : ~~…~~
  - uzual reprezentat taiat
  - aceleasi atribute

```
<p>O grupa poate avea <del>25</del> <ins>45</ins> studenti.</p>
```

O grupa poate avea ~~25~~ 45 studenti.

Coduri 1

ASCII			HTML	HTML	
Dec	Hex	Symbol	Number	Name	Description
160	A0				non-breaking space
161	A1	¡	¡	¡	inverted exclamation mark
162	A2	¢	¢	¢	cent sign
163	A3	£	£	£	pound sign
164	A4	¤	¤	¤	currency sign
165	A5	¥	¥	¥	yen sign
166	A6	¦	¦	¦	broken vertical bar
167	A7	§	§	§	section sign
168	A8	¨	¨	¨	spacing diaeresis - umlaut
169	A9	©	©	©	copyright sign
170	AA	ª	ª	ª	feminine ordinal indicator
171	AB	«	«	«	left double angle quotes
172	AC	¬	¬	¬	not sign
173	AD	-			soft hyphen
174	AE	®	®	®	registered trade mark sign
175	AF	¯	¯	¯	spacing macron - overline

Coduri 2

ASCII			HTML	HTML	
Dec	Hex	Symbol	Number	Name	Description
176	B0	°	°	°	degree sign
177	B1	±	±	±	plus-or-minus sign
178	B2	²	²	²	superscript two - squared
179	B3	³	³	³	superscript three - cubed
180	B4	´	´	´	acute accent - spacing acute
181	B5	µ	µ	µ	micro sign
182	B6	¶	¶	¶	pilcrow sign - paragraph sign
183	B7	·	·	·	middle dot - Georgian comma
184	B8	¸	¸	¸	spacing cedilla
185	B9	¹	¹	¹	superscript one
186	BA	º	º	º	masculine ordinal indicator
187	BB	»	»	»	right double angle quotes
188	BC	¼	¼	¼	fraction one quarter
189	BD	½	½	½	fraction one half
190	BE	¾	¾	¾	fraction three quarters
191	BF	¿	¿	¿	inverted question mark

Coduri 3

ASCII			HTML	HTML	
Dec	Hex	Symbol	Number	Name	Description
34	22	"	"	"	double quotes
38	26	&	&	&	ampersand
60	3C	<	<	<	less than sign
63	3E	>	>	>	greater than sign

Contact

- Microwave and Optoelectronics Laboratory
- http://rf-opto.etti.tuiasi.ro
- rdamian@etti.tuiasi.ro
- Homework, lecture 6, mandatory presence, 25% grade
  - December 13, 2012
  - Romanian Version December 14, 2012