DOCUMENTO AD USO ESCLUSIVO DEGLI STUDENTI ALL'INTERNO DEL CORSO

Corso di Informatica e logica giuridica a.a. **2014-15**

(prof. Romano Oneda)

PRINCIPALI ARGOMENTI PROPONIBILI NEL COLLOQUIO D'ESAME

(trattati a lezione [L] / esposti nelle dispense del corso [D] o nel libro di testo [T])

1. *definizione di 'digitale' ed 'analogico'; conversione da digitale ad analogico (digitalizzazione, dematerializzazione) : campionamento, quantizzazione.*
2. *Il segno: significante e significato; asse sintagmatico e paradigmatico; il fonema e gli allofoni; il grafema e gli allografi; il glifo.*
3. *Il suono e la voce: timbri vocalici, consonanti; forme d'onda e spettro armonico: sintesi di Fourier*[L].
4. *Dal fonema al grafema: corrispondenze ed aspetti problematici nella scrittura storica di varie lingue (digrammi, trigrammi ecc.)* [L].
5. *La codifica ASCII standard ed estesa; la codifica UNICODE ; UTF8; BabelMap* [L].
6. *La rappresentazione binaria (256 simboli) e la codifica in base64: i più importanti utilizzi.*
7. *I font come mediatori tra i bit e i pixel nella rappresentazione informatica*[L].
8. *La rappresentazione (rappresentante e rappresentato) e la copia: il problema dell'originale elettronico.*
9. *La rappresentazione su canali non visuali: la codifica Braille, la codifica Morse.*
10. *La firma chirografa: caratteristiche ed aspetti funzionali.*
11. *Il bit come unità elementare di informazione; operazioni binarie e codifica binaria* [T], [D].
12. *Gli operatori logici binari; collegamenti in serie e in parallelo.*
13. *Quantità di informazione e riduzione dell'incertezza, entropia e ridondanza* [T], [D].
14. *L'analisi della frequenza dei grafemi nell'indagine linguistica e crittografica* [L].
15. *La rappresentazione numerica: le cifre, il sistema di rappresentazione posizionale polinomiale binario, decimale, esadecimale. La numerazione romana.*
16. *I collegamenti di comunicazione con l'esterno: l'interfaccia input-output, le principali periferiche* [T], [D].

17. *La memorizzazione dei dati (temporanea, permanente): gli strumenti analogici e digitali* [T], [D].

18. *Le reti di calcolatori e la trasmissione dei dati* [T].

19. *Gli indirizzi IP; il dominio dei nomi (DNS); struttura degli URL* [T], [D].

20. *Il protocollo HTTP e il linguaggio HTML nella costituzione dei link* [L].

21. *L'interazione tra esseri umani e calcolatori come problema di comunicazione* [T].

22. *La casualità e i giochi di azzardo; il computer come generatore di sequenze random e pseudorandom; il sito 'www.random.org'*[L].

23. *La ridondanza informativa e la compressione lossy e lossless dei file.*

24. *La steganografia classica e digitale* [D],[L].

25. *L'editor esadecimale ed Edxor come strumenti di laboratorio: caratteristiche ed esempi di utilizzo.*

26. *La funzione della chiave nella crittografia simmetrica e asimmetrica; plain text e cipher text.*

27. *La crittografia classica: il cifrario di Cesare e la sostituzione monoalfabetica; la sostituzione polialfabetica (il cifrario di Vigenère).*

28. *La macchina elettromeccanica Enigma: struttura e funzionamento [L].*

29. *Il cifrario perfetto (Vernam, OTP) nelle versioni classica e digitale; perché l'OTP viene definito matematicamente indecifrabile.*

30. *Il problema dell'integrità dei dati trasmessi; le funzioni di controllo; parità; checksum; CRC ; codici di controllo e correzione degli errori.*

31. *Le funzioni di hash: definizione, caratteristiche, impronta, collisioni, nomi delle funzioni più utilizzate.*

32. *Le funzioni di hash: principali ambiti di utilizzo in Internet [L].*

33. *I codici a barre monodimensionali e bidimensionali; il codice EAN, il codice ISBN; il codice UNIPV.*

34. *Il codice fiscale individuale: il decreto istitutivo, la struttura, il calcolo della lettera di controllo. L'omocodia.*

35. *I codici bancari: i parametri bancari, BBAN, IBAN e codici di controllo.*

36. *L'aritmetica modulare: moduli, classi di congruenza, operazioni in modulo, divisori dello zero.*

37. *L'esponenziazione modulare e le tabelline applicative: esercizi* [L].

38. *Il problema degli inversi nell'aritmetica modulare.*

39. *La funzione toziente PHI(n) e il teorema di Eulero.*

40. *Lo scambio delle chiavi secondo l'algoritmo di Diffie-Hellman.*

41. *Il cifrario RSA e il problema della fattorizzazione.*

42. *La firma elettronica e digitale: la generazione delle chiavi e la procedura di apposizione della firma.*

43. *Tipologia delle firme nella normativa italiana.*

44. *Tipologia funzionale delle chiavi nella normativa italiana.*

45. *La firma elettronica e digitale: la procedura di verifica della firma.*

46. *Il certificato della chiave pubblica: PKI e certificatori accreditati.*

47. *Il dispositivo sicuro di firma: smartcard e token. Caratteristiche e funzionamento.*

48. *Responsabilità e obblighi del certificatore; le liste di revoca e di sospensione.*

49. *I certificati qualificati: caratteristiche e dati contenuti nel certificato.*

50. *La marca temporale come certificato; il supporto della validazione temporale alla firma elettronica.*

51. *La busta crittografica* ***.p7m****: funzione e contenuto.*

52. *La procedura di spedizione del questionario finale.*

53. *Applicazioni della firma elettronica: la PEC [D].*

54. *Principali tecniche di esplorazione delle funzionalità cerebrali. La risonanza magnetica funzionale. ([D] 8-9-10-11-17-18-21) .*

55. *Aspetti critici nell'impiego delle nuove tecnologie di imaging in ambito forense ([D] 14-16-22).*

56. *L'onda P300, lie detectors e test di attendibilità ([D] 23-24-25-26-27-28-29-30).*

57. *Principali aree cerebrali implicate nella costruzione del comportamento sociale e delle inclinazioni morali ([D] 32-38-39-40-41-44-45-46).*

58. *Aggressività ed empatia ([D] 35-36-37-47-48-49-51-52).*

59. *Il phishing e le tecniche di social engineering [L].*

60. Il virus ransomware TorrentLocker [L].

FONTI

[T] = *L.Mari, G.Buonanno, D.Sciuto,* Informatica e cultura dell'informazione, 2°ed. 2013, McGraw-Hill

[D] = ig2014.pdf; La crittografia nella firma digitale.pdf; NEUROSCIENZE_IN_LAW.pdf; Marconi-PEC.pdf

[L] = argomenti trattati a lezione, senza precisa corrispondenza nelle dispense fornite, o esercitazioni laboratoriali

oneda
romano

Firmato digitalmente da oneda romano
ND: c=IT, o=non presente, cn=oneda romano, serialNumber=IT:NDORMN40D14D150N, givenName=romano, sn=oneda, dnQualifier=11683381
Data: 2014.12.08 17:10:09 +01'00'