DOCUMENTO AD USO ESCLUSIVO DEGLI STUDENTI ALL'INTERNO DEL CORSO

Corso di Informatica e logica giuridica a.a. **2015-16**

(prof. Romano Oneda)

PRINCIPALI ARGOMENTI PROPONIBILI NEL COLLOQUIO D'ESAME

[STUDENTI FREQUENTANTI E NON FREQUENTANTI]

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*. [D]
12. *Gli operatori logici binari; collegamenti in serie e in parallelo.*
13. *Quantità di informazione e riduzione dell'incertezza, entropia e ridondanza.* [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.* [D]

17. *La memorizzazione dei dati (temporanea, permanente): gli strumenti analogici e digitali.* [D]
18. *Le reti di calcolatori e la trasmissione dei dati*.
19. *Il protocollo HTTP e il linguaggio HTML, in particolare nella costituzione dei link.* [L]
20. *Il browser e l'interazione Client-Server nel web.*
21. *L'interazione tra esseri umani e calcolatori come problema di comunicazione: le interfacce.*
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; plaintext e ciphertext.*
27. *La crittografia classica: il cifrario di Cesare e la sostituzione monoalfabetica; Rot 13; 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. *Il phishing e le tecniche di social engineering. [L]*
54. *Gli attacchi DDOS e gli honeypot.*
55. *Gli indirizzi IP v.4 e v.6: la quaterna puntata; indirizzi statici e dinamici.*
56. *L'URL: significato e composizione funzionale.*
57. *Il DNS: significato e funzione.*
58. *Il prompt dei comandi Windows e l'utilizzo di ping, arp e tracert; l'indirizzo MAC. [L]*
59. *L'homunculus e le mappe corticali. [L]*
60. *L'integrazione uomo-macchina; gli automi. [P.G.Milanesi: http://ig.unipv.it/2016/ig/Automi_a_Giudizio.pdf]*
61. *Neuroni naturali e artificiali. [id]*
62. *Le reti neurali. [id]*

63. Coscienza e coscienza artificiale. [id]

LETTURE IN PROGRAMMA DAI LIBRI DI TESTO

[STUDENTI FREQUENTANTI] - Da **IL *COMPUTER E IL GIURISTA*** di Giovanni ZICCARDI:

I: Un approccio tripartitico: tecnica, informatica, diritto
II: La ricerca delle informazioni giuridiche
III: Atti giuridici scritti al computer: regole di stile, interoperabilità e sicurezza tecnica
IV: Il dato digitale e la sua protezione
V: La posta elettronica e il processo civile telematico
VI: L'attività del giurista in Internet: web, *social network*, deontologia

[STUDENTI NON FREQUENTANTI] - Da ***L'AVVOCATO HACKER*** di Giovanni ZICCARDI:

I: Il percorso verso la conoscenza - II: Essere hacker (anche) nella professione legale – III: Dieci percorsi introduttivi da seguire – IV: L'importanza di un sistema operativo libero – V: Il fattore umano quale elemento imprescindibile per la sicurezza - VI: Il funzionamento e la scelta del personal computer – VII: la tastiera – VIII: la memoria – IX: Il sistema operativo – X: Multiutenza e password – XI: Cartelle e directory – XII: Compressione e archiviazione delle informazioni – XIII: La gestione dei documenti – XIV: La videoscrittura – XV: Gli standard documentali e la interoperabilità - XVI: La funzione e la procedura di stampa – XVII: Cancellare il dato in modo sicuro – XVIII: Nascondere le informazioni – XIX: Il recupero delle informazioni cancellate o nascoste – XX: Preservare l'integrità e la disponibilità del dato: l'arte del backup – XXI: Trasmettere le informazioni in sicurezza – XXII: Operare in ambienti non sicuri – XXIII: Proteggere le informazioni da virus e da accessi dall'esterno – XXIV: La protezione della privacy personale: alcune linee guida – XXV: La privacy dell'attività professionale – XXVI: La sicurezza dei computer dello studio, della rete e dei documenti – XXVII: Le *portable apps* – XXVIII: La redazione di una policy o disciplinare di sicurezza per l'uso quotidiano (anche professionale) – XXIX: Le macchine virtuali – XXX: Il corretto utilizzo della posta elettronica in locale e sul web - XXXI: Cercare i dati da fonti aperte: la *open source intelligence* (OSINT) - XXXII: Le tracce digitali – XXXIII: Investigare nel personal computer – XXXIV: La registrazione sonora e visiva di eventi – XXXV: Interpretare il dato: gli *headers* delle e-mail e il *tracing* di un indirizzo IP – XXXVI: Un'introduzione alla digital forensics – XXXVII: Relazionarsi con hacker ed esperti informatici – XXXVIII: Considerazioni conclusive.

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