DOCUMENTO AD USO ESCLUSIVO DEGLI STUDENTI ALL'INTERNO DEL CORSO

Corso di Informatica e logica giuridica 2013-14

(prof. Romano Oneda)

PRINCIPALI ARGOMENTI PROPONIBILI NEL COLLOQUIO D'ESAME

(trattati a lezione / esposti nelle dispense del corso o nel libro di testo)

- *definizione di 'digitale' ed 'analogico'; conversione da digitale ad analogico (digitalizzazione, dematerializzazione) : campionamento, quantizzazione.*
- *Il segno: significante e significato; asse sintagmatico e paradigmatico; il fonema e gli allofoni; il grafema e gli allografi; il glifo.*
- *La codifica ASCII standard ed estesa; la codifica UNICODE ; UTF8; BabelMap.*
- *La rappresentazione binaria (256 simboli) e la codifica in base64.*
- *I font come mediatori tra i bit e i pixel nella rappresentazione informatica.*
- *La rappresentazione (rappresentante e rappresentato) e la copia: il problema dell'originale elettronico.*
- *La rappresentazione su canali non visuali: la codifica Braille, la codifica Morse.*
- *La firma chirografa: caratteristiche ed aspetti funzionali.*
- *Il bit come unità elementare di informazione; operazioni binarie e codifica binaria* (libro, dispense).
- *Quantità di informazione e riduzione dell'incertezza, entropia e ridondanza* (libro, dispense).
- *La rappresentazione numerica: le cifre, il sistema di rappresentazione posizionale polinomiale binario, decimale, esadecimale.*
- *I collegamenti con l'esterno, input output, le principali periferiche* (libro, dispense)
- *La memorizzazione dei dati (temporanea, permanente): gli strumenti analogici e digitali* (libro, dispense)
- *Le reti di calcolatori e la trasmissione dei dati* (libro)
- *Gli indirizzi IP; il dominio dei nomi (DNS); struttura degli URL* (dispense, libro)
- *L'interazione tra esseri umani e calcolatori come problema di comunicazione* (libro)

- *La casualità e i giochi di azzardo; Il computer come generatore di sequenze random e pseudorandom; il sito 'www.random.org'.*
- *La ridondanza informativa e la compressione lossy e lossless dei file.*
- *La steganografia classica e digitale.*
- *L'editor esadecimale ed Edxor come strumenti di laboratorio.*
- *La funzione della chiave nella crittografia simmetrica ed asimmetrica; plain text e cipher text*
- *La crittografia classica: il cifrario di Cesare e la sostituzione monoalfabetica; la sostituzione polialfabetica (il cifrario di Vigenère).*
- *La macchina elettromeccanica Enigma: struttura e funzionamento.*
- *Il cifrario perfetto (Vernam, OTP) nelle versioni classica e digitale; perché l'OTP viene definito matematicamente indecifrabile.*
- *Il problema dell'integrità dei dati trasmessi; le funzioni di controllo; parità; checksum; CRC ; codici di controllo e correzione degli errori.*
- *Le funzioni di hash: definizione, caratteristiche, impronta, collisioni, nomi delle funzioni più utilizzate.*
- *Le funzioni di hash: principali ambiti di utilizzo in Internet.*
- *I codici a barre monodimensionali e bidimensionali; il codice EAN, il codice ISBN; il codice UNIPV.*
- *Il codice fiscale: il decreto istitutivo, la struttura, il calcolo della lettera di controllo.*
- *I codici bancari: i parametri bancari, BBAN,IBAN e codici di controllo.*
- *L'aritmetica modulare: moduli, classi di congruenza, operazioni in modulo, divisori dello zero.*
- *Il problema degli inversi nell'aritmetica modulare.*
- *La funzione toziente Phi(n) e il teorema di Eulero.*
- *Lo scambio delle chiavi secondo l'algoritmo di Diffie-Hellman.*
- *Il cifrario RSA e il problema della fattorizzazione*
- *La firma elettronica e digitale: la generazione delle chiavi e la procedura di firma*
- *Tipologia delle firme nella normativa italiana.*
- *Tipologia funzionale delle chiavi nella normativa italiana.*
- *La firma elettronica e digitale: la procedura di verifica della firma*
- *Il certificato della chiave pubblica: PKI e certificatori accreditati.*
- *Il dispositivo sicuro di firma: smartcard e token. Caratteristiche e funzionamento.*

- *Responsabilità e obblighi del certificatore; le liste di revoca e di sospensione*
- *I certificati qualificati: i dati contenuti nel certificato*
- *La marca temporale; il supporto della validazione temporale alla firma elettronica*
- *La busta crittografica p7m: funzione e contenuto*
- *La procedura di spedizione del questionario finale*

DIGITAL FORENSICS

- *Mezzi di ricerca della prova e mezzi di prova – ratio, distinguo e strumenti* (primo incontro, varie slide)
- *L'informatica forense – definizione e inquadramento* (slide n. 3 prof. Barili)
- *I mezzi di prova scientifici – lo standard Daubert* (slide 8 prof. Barili e slide 10 avv. Currà del terzo seminario)
- *Requisiti delle procedure informatiche di ricerca e acquisizione della prova* (slide 11 e ss. prof. Barili)
- *Analisi post-mortem di un sistema informatico* (slide 19 e ss. Rebus)
- *La live forensics* (slide 25 e ss. Rebus)
- *Le investigazioni difensive - principio di parità tra accusa e difesa* (slide 10 Rebus e varie slide secondo seminario)
- *I requisiti legali dell'evidenza digitale* (slide 10 e ss. avv. Vaciago)
- *Bit-stream copy* (slide 8 e 9 avv. Vaciago e 19 e ss. Rebus)
- *Accertamenti tecnici ripetibili e accertamenti tecnici irripetibili* (slide terzo incontro).