UNIVERSITÀ degli STUDI di PAVIA

DIPARTIMENTO DI GIURISPRUDENZA

Collegio GHISLIERI

Centro di Comunicazione e Ricerca

Area di Diritto e Informatica

Programma del corso di INFORMATICA E LOGICA GIURIDICA

a. a. 2016-2017 (primo semestre)

(prof. Romano Oneda)

PARTE GENERALE

L'INFORMAZIONE E LA COMUNICAZIONE

Il lato umano

- Cenni sulle neuroscienze e sulle tecniche sperimentali di indagine del cervello.
- I sensori dell'informazione come interfaccia con il mondo fisico: i canali sensoriali. La trasmissione dei segnali nei due sensi lungo le vie nervose: gli effettori.
- Sensazione e percezione.
- Mente e cervello.
- Il problema dell'io e della coscienza; i qualia.

Le protesi dei sensi

- Il potenziamento delle capacità sensoriali attraverso gli strumenti ottici, meccanici, elettronici ecc.
- La sinestesia; la realtà virtuale ed aumentata.
- Le disabilità sensoriali e gli ausili.
- L'intelligenza artificiale e la robotica: ausilio o minaccia per l'umanità?

Il lato macchina

- L'interfaccia uomo-computer-uomo (input, output). L'Internet delle cose (IoT).
- La conversione analogico-digitale (digitalizzazione, campionamento, quantizzazione, 'dematerializzazione'.
- Il bit come unità di misura dell'informazione.
- Gli operatori binari e la programmazione del microprocessore: cenni sui linguaggi di programmazione e sui livelli operativi.
- Le rappresentazioni e le codifiche come interfaccia operativa funzionale al rapporto uomo-macchina.
- I simboli binari utilizzati come operatori logici e numerici.

- La rappresentazione numerica: il numero e le cifre, il sistema di rappresentazione romano, i sistemi di rappresentazione posizionale-polinomiale binario, decimale, esadecimale.
- La costruzione del mondo binario.
- Ordine e disordine; casualità, entropia e il caos.

Cenni di linguistica e semiotica

- Il processo di significazione: significante, significato, referente, simboli.
- Fonologia: la segmentazione, il fonema, gli allofoni, le coppie minime, il grafema, gli allografi, il glifo.
- I simboli; gli alfabeti; le codifiche ASCII e UNICODE. L'alfabeto fonetico fonetico internazionale (IPA)
- Il linguaggio come strumento di comunicazione: i vincoli linguistico-sintattici in opposizione alla casualità e all'incremento entropico.
- L'analisi delle frequenze dei caratteri come indicatore delle caratteristiche delle varie lingue.
- La costruzione di unità complesse a partire da un insieme di simboli: paradigma e sintagma. La ridondanza funzionale ed espressiva nella comunicazione linguistica.
- La riduzione della ridondanza: strategie linguistiche (sostituenti, anafora, catafora ecc.).
- La compressione della ridondanza informatica: i file zip e le tecniche utilizzate (*lossy*, *lossless* ecc.).

La trasmissione informatica

- La compressione dei dati nella comunicazione digitale.
- Il controllo di integrità dei dati e la correzione dell'errore.
- La ridondanza come presupposto e strumento di controllo e correzione.
- L'importanza dei numeri primi negli algoritmi di controllo.
- Controlli di parità, *checksum*, CRC ecc.
- I limiti dei codici di controllo.
- Esempi di codici di controllo: il codice ISBN, EAN, Matricola UNIPV, codice fiscale, codici bancari e IBAN.
- I codici a barre mono e bidimensionali come supporti di memorizzazione digitale non convenzionale (cartacei ecc.).
- Le funzioni di hash come risposta alle insufficienze dei codici di controllo.

PARTE MONOGRAFICA

IL DOCUMENTO DIGITALE E LA FIRMA ELETTRONICA

Dalla carta al bit

- La firma chirografa: caratteristiche ed aspetti funzionali.
- La rappresentazione (rappresentante/rappresentato) e la copia: il problema dell'originale elettronico.
- Supporti cartacei e supporti ottici, magnetici ed elettronici; prospettive future di memorizzazione.

Il calcolo discreto

- L'aritmetica modulare: moduli, classi di congruenza, operazioni in modulo, divisori dello zero.
- Gli inversi nell'aritmetica modulare.
- La funzione toziente *phi(n)* e il teorema di Eulero: applicazioni crittografiche.

Avviamento alla crittografia

- La crittografia come tecnica di selezione esclusiva del destinatario del messaggio.
- La crittografia classica: il cifrario di Cesare e la sostituzione monoalfabetica; la sostituzione polialfabetica (il cifrario di Vigenère).
- Il principio di Kerckhoffs e le chiavi crittografiche: proprietà, caratteristiche e sviluppo tecnico. I cifrari elettromeccanici a chiave simmetrica: la macchina Enigma.
- I cifrari digitali a chiave simmetrica: RSA4, DES, AES.
- Il cifrario perfetto (Vernam, OTP) nelle versioni classica e digitale: perché l'OTP viene definito matematicamente indecifrabile.
- Il problema del trasporto della chiave crittografica.
- Il protocollo a conoscenza zero: la *challenge* crittografica.
- Lo scambio delle chiavi secondo l'algoritmo di Diffie-Hellman.
- La steganografia come supporto alla segretezza della comunicazione

I cifrari a chiave asimmetrica

- Il cifrario RSA e il problema della fattorizzazione.
- Il cifrario RSA e l'aritmetica modulare: struttura e funzionamento. Il cifrario DSA e le curve ellittiche (cenni).
- Il *Qubit* e la computazione quantistica (cenni).

Le funzioni di hash

- Definizione, caratteristiche, l'impronta, le collisioni; cenni sulle funzioni di hash più utilizzate (MD5, SHA1, SHA256, RIPEMD, SHA-3).
- Le funzioni di hash e i loro più rilevanti ambiti di utilizzo in Internet.

Il documento digitale (informatico?)

- I problemi connessi con la definizione e l'individuazione delle caratteristiche specifiche, in relazione al documento cartaceo (analogico???).
- *Bit versus pixel*: i problemi della rappresentazione per l'umano del documento digitale.

La firma digitale

- Firme elettroniche e firma digitale.
- La generazione delle chiavi asimmetriche e la procedura di firma RSA.
- Il dispositivo sicuro di firma: *smartcard* e *token*. Caratteristiche e funzionamento.
- Il certificato della chiave pubblica: PKI e certificatori.
- La procedura di verifica della firma RSA.
- La busta crittografica p7m: funzione e contenuto.
- La firma digitale in PDF; la firma DSA.

- L'identità digitale e la biometria. Lo SPID (Sistema Pubblico di Identità Digitale).
- La firma grafometrica.

La normativa italiana sulla firma elettronica

- Tipologia delle firme elettroniche nella normativa italiana.
- Tipologia funzionale delle chiavi nella normativa italiana.
- Il certificato della chiave pubblica.
- Certificazione qualificata: struttura e contenuto informativo.
- Certificazione temporale: la marca.
- Responsabilità e obblighi del certificatore; le liste di revoca e di sospensione.
- La validità temporale della firma digitale; il supporto della marca temporale.
- La conservazione documentale.

Le applicazioni della firma digitale

- La posta certificata.
- Il processo telematico.
- La carta di identità elettronica.
- La moneta elettronica: cenni sui Bitcoin.

L'informatica forense

- La nozione di prova; la prova in sede civile; la prova in sede penale; la prova in sede lavoristica.
- La prova digitale – Aspetti tecnici.
- La prova digitale – Aspetti giuridici e strumenti d'indagine.
- L'antiforensics.

Il questionario finale individuale di accertamento laboratoriale

- Assistenza tutoriale alla compilazione.
- La procedura di invio (accesso al sito con firma elettronica e validazione temporale).

Testi normativi e didattici di supporto

- **Codice dell'amministrazione digitale** (**CAD**, decreto legislativo 7 marzo 2005, n.82 e successive modifiche e integrazioni)
- **Regole tecniche sulle firme elettroniche** (decreti del Presidente della Repubblica 22 febbraio 2013 e 13 novembre 2014)
- **Testo unico sulla documentazione amministrativa (TUDA)**, decreto del Presidente della Repubblica 28 dicembre 2000, e successive modifiche e integrazioni)

G. ZICCARDI, *Il computer e il giurista*, Milano, Giuffrè, 2015 (pp.180).

G. ZICCARDI, *L'avvocato hacker*, *Informatica giuridica e uso consapevole (e responsabile) delle tecnologie*, Milano, Giuffrè, 2012 (pp. 446).

L.MARI, G.BUONANNO, D.SCIUTO – *Informatica e cultura dell'informazione.* Milano, McGraw Hill, 2013.

In considerazione della vastità del programma e della difficoltà di contenerlo nelle sessanta ore del corso, il programma d'esame sarà pubblicato soltanto a fine corso, e conterrà solamente gli argomenti effettivamente trattati a lezione.