Comunicazioni in codice 4403

La prova è rivolta agli studenti della classe quinta di un Istituto Tecnico Industriale ad indirizzo Elettronica e Telecomunicazioni e coinvolge le seguenti discipline: inglese, diritto, storia, sistemi elettronici, telecomunicazioni.

Conoscere l'evoluzione e l'impiego dei codici nei vari campi delle telecomunicazioni
Conoscere le problematiche delle trasmissioni in codice
Riconoscere elementi lessicali e sintattici della lingua inglese
Conoscere i principi che regolano il perfezionamento del contratto alla luce delle nuove tecnologie

Strumenti consentiti: calcolatrice, dizionario di lingua inglese.
Tempo previsto: 2 ore.

Testo

Per migliaia di anni, re, regine e generali hanno avuto bisogno di comunicazioni efficienti per governare i loro paesi e comandare i loro eserciti. Nel contempo, essi compresero quali conseguenze avrebbe avuto la caduta dei loro messaggi in mani ostili: informazioni preziose sarebbero state a disposizione delle nazioni rivali e degli eserciti nemici. Fu il pericolo dell'intercettazione da parte degli avversari a promuovere lo sviluppo di codici e cifre, tecniche di alterazione del messaggio destinate a renderlo comprensibile solo alle persone autorizzate (...). Oggi le nostre telefonate rimbalzano dai satelliti e i nostri e-mail passano attraverso catene di elaboratori elettronici; in entrambi i casi le occasioni di intercettazione sono innumerevoli, e la nostra privacy è messa a repentaglio. In modo analogo, sempre più transazioni sono effettuate via Internet e la tutela della privacy è indispensabile tanto ai grandi operatori quanto al singolo cliente. La crittografia è il solo strumento in grado di garantire la riservatezza di tutti e il successo del commercio telematico.

Simon Singh, *Codici & Segreti*, Rizzoli, 1999, "Introduzione", pp. IX, X

1) Il momento perfezionativo del contratto, quando i contraenti sono lontani, si ha al momento:

a. della spedizione della proposta
b. dell'accettazione della proposta

c. del ricevimento dell'accettazione
d. della spedizione dell'accettazione.

2) Il momento perfezionativo del contratto telematico on line (quando il sito web contiene tutti gli elementi essenziali della proposta contrattuale) si attua:
a. secondo lo schema dell'offerta al pubblico nel momento e nel luogo in cui un navigatore trasmette la dichiarazione negoziale di accettazione al titolare del sito contenente l'offerta
b. quando il titolare del sito riceve l'accettazione
c. quando avviene il pagamento
d. al momento della consegna del bene oggetto della contrattazione.

3) Il diritto d'autore sul software, quale rappresentazione della mente umana, è caratterizzato:
a. dalla temporaneità dello sfruttamento economico e dall'immaterialità del bene che ne costituisce l'oggetto
b. dalla prescrittibilità del diritto morale di paternità dell'opera
c. da un diritto solo morale di paternità dell'opera
d. da un diritto solo patrimoniale di paternità dell'opera legato all'utilizzo per finalità lucrative.

4) La negoziazione in video conferenza in tempo reale è assimilabile a quella tra persone presenti o a quella tra persone lontane? (*max 6 righe*)

5) Come si può conciliare il diritto alla riservatezza, tutelato dal nostro ordinamento, con il potere del curatore fallimentare di aprire la corrispondenza del fallito? (*max 6 righe*)

6) Nel 1835 è stata effettuata la prima trasmissione telegrafica su conduttore, utilizzando il codice:
a. Baudot
b. Bell
c. Morse
d. CCITT N. 5.

7) Le telescriventi utilizzano il codice:
a. Morse
b. CCITT N. 5
c. ASCII
d. EBCDIC.

8) In una trasmissione dati, al fine di ridurre il tasso di errore, si effettua una codifica:
a. di sorgente
b. di linea
c. di canale
d. PCM.

9) Nel modello ISO/OSI il livello preposto alla individuazione e correzione di errore è:
a. il livello fisico
b. il livello di rete
c. il livello di link
d. il livello di trasporto.

10) Descrivere le caratteristiche del codice AMI (Alternate Mark Inversion). (*max 3 righe*)

11) Spiegare l'utilità della codifica Manchester e in che cosa consiste. (*max 5 righe*)

12) Un numero non intero in notazione scientifica è rappresentato in forma esponenziale. Nei linguaggi la codifica della notazione scientifica è indicata come rappresentazione in virgola mobile. Il nome deriva dal fatto che la posizione della virgola decimale tra le cifre che costituiscono:
a. la caratteristica dipende dal valore della mantissa
b. la mantissa non dipende dal valore della caratteristica
c. la mantissa e quelle che costituiscono la caratteristica non varia
d. la mantissa dipende dal valore della caratteristica.

13) Si analizzi il seguente algoritmo, scritto in linguaggio simbolico.

Acquisisci una stringa di M caratteri
Assegna all'indice n il valore 1
Assegna all'indice i il valore 1
Finché $n \leq M$
Leggi l'ennesimo carattere
Trascrivi l'ennesimo carattere nel corrispondente numero binario in codice ASCII
Memorizza i sette bit del codice ASCII in A[i] A[i+1]... A[i+6]
Incrementa n di 1 unità
Incrementa i di 7 unità
Ripeti il ciclo
Assegna all'indice i il valore 1
Finché $i<7M$
Scambia A[i] con A[i+1]
Incrementa i di 2 unità
Ripeti il ciclo

L'algoritmo trasforma il testo in chiaro in un testo cifrato in caratteri ASCII in cui, per trasposizione, è scambiata:
a. la prima con la seconda cifra binaria, la terza con la quarta e così via
b. la prima con la seconda cifra binaria, la terza con la quarta e così via. Se il testo in chiaro genera una sequenza dispari di cifre binarie, l'ultimo bit resterà immutato
c. la prima con la seconda cifra binaria, la terza con la quarta e così via. Se il testo in chiaro genera una sequenza dispari di cifre binarie c'è indeterminazione sull'ultima cifra
d. la prima con la seconda cifra binaria, la terza con la quarta e così via. Il messaggio cifrato è significativo solo se il testo in chiaro genera una sequenza pari di cifre binarie.

14) In un URL (Uniform Resource Locator) la stringa di testo è suddivisa in:
a. tipo di accesso al documento, nome dell'host computer che contiene l'informazione, percorso per raggiungere il file contenente l'informazione
b. percorso per raggiungere il file contenente l'informazione, tipo di accesso al documento, nome dell'host computer che contiene l'informazione
c. percorso per raggiungere il file contenente l'informazione, nome dell'host computer che contiene l'informazione
d. nome dell'host computer che contiene l'informazio-

ne, tipo di accesso al documento, percorso per raggiungere il file contenente l'informazione.

15) I sistemi di crittografia a chiave pubblica prevedono l'uso di:
a. una sola chiave elettronica privata che permette di codificare e decodificare il messaggio
b. una chiave elettronica pubblica che permette di decodificare il messaggio e una chiave elettronica privata che ne permette la codifica
c. una chiave elettronica pubblica che permette di codificare il messaggio e una chiave elettronica privata che ne permette la decodifica
d. una sola chiave elettronica privata che permette di codificare e decodificare il messaggi.

16) Giulio Cesare per proteggere le sue missive ricorreva spesso alla scrittura in codice. Un esempio è dato dall'algoritmo noto come cifratura di Cesare. Esso prevede di sostituire ciascuna lettera del messaggio in chiaro con la lettera che nell'alfabeto ordinario si trova tre posizioni più avanti. Si scriva, in un linguaggio di propria conoscenza, il segmento di programma che permette di trasformare un messaggio in chiaro nel corrispondente messaggio cifrato, utilizzando i caratteri ASCII dell'alfabeto inglese.

17) La prima trasmissione in simultanea tra più nazioni è avvenuta a:
a. New York nel 1911
b. Parigi nel 1913
c. Mosca nel 1917
d. Roma nel 1918.

18) La realizzazione del RDT (Radio Detector Telemeter 1936) permise l'introduzione del metodo di 'rilevazione' delle immagini ed ebbe un ruolo fondamentale nella II guerra mondiale. In quale battaglia ciò avvenne?
a. Battaglia Maginot
b. Battaglia d'Inghilterra
c. Battaglia di Sebastopoli
d. Battaglia di Norvegia.

19) Che cosa significa lottizzazione del sistema informativo?
a. Unione di più reti di comunicazione
b. Creazione di aree di comunicazione di massa
c. Spartizione di cariche e uffici sulla base dell'area politica di appartenenza
d. Processo di decentramento informativo.

20) Le moderne tecnologie informatiche e telematiche hanno permesso, dal dopoguerra ad oggi, di evitare un conflitto bellico diretto tra le grandi potenze. Come è stato definito questo periodo?
a. Di non belligeranza
b. Guerriglia
c. Guerra di postazione
d. Guerra fredda.

21) In quale anno ha inizio la comunicazione internazionale via cavo?
a. 1913
b. 1945
c. 1956
d. 1943.

22) Quando nascono le prime reti TV private?
a. 1954 (Telemontecarlo)
b. 1961 (Telestudio)
c. 1971 (Canale 5)
d. 1973 (Tele Biella via cavo).

23) For thousands of years, kings and queens have needed efficient communications means to:
a. rule their countries and their armies
b. rule their countries
c. rule their armies
d. send messages to other kings and queens.

24) Codes and secret alphabets were developed because kings and queens:
a. were sure precious information could fall into enemy hands
b. were happy precious information could fall into enemy hands
c. liked inventing new alphabets
d. were afraid precious information could fall into enemy hands.

25) Fill in the blanks with the correct word.
Today we have ..... privacy.
a. very little
b. a lot of
c. a lot
d. much.

26) Cryptography is:
a. used to send messages
b. the only way to guarantee privacy in our day-to-day use of Internet
c. used to avoid privacy
d. used because the users like it.

27) Nowadays, our phone calls and our e-mails go through:
a. telephone lines
b. cables
c. a series of computers
d. the wall.

28) Say why the need for cryptography has developed to such extent. (*max 5 lines*)

29) Describe the telematic transmission of messages. (*Approx. 8 lines*)

30) Describe the concept of privacy as regards the transmission of information by telematic means. (*Approx. 5 lines*)

---

31) La negoziazione in video conferenza in tempo reale è assimilabile a quella tra persone:
a. lontane
b. presenti, perché l'incontro di volontà concordanti tra le parti avviene contestualmente
c. presenti, purché l'accettazione arrivi entro 30 giorni dalla negoziazione
d. lontane, purché sia espresso il diritto di recesso.

32) Il curatore fallimentare può aprire la corrispondenza del fallito?

a. Sì, sempre
b. No, mai
c. Sì, ma solo nel caso di condanna del fallito
d. Sì, ma solo con il consenso del fallito.

33) Nel codice AMI (Alternate Mark Inversion) per trasmettere:
a. in livello basso del segnale dati si utilizzano alternativamente successioni di impulsi di polarità positiva e negativa con ritorno a zero e per trasmettere il livello alto si usa il livello zero
b. in livello alto del segnale dati si utilizzano alternativamente successioni di impulsi di polarità positiva e negativa con ritorno a zero e per trasmettere il livello basso si usa il livello zero
c. in livello alto si usano due impulsi con ritorno a zero ciascuno di durata pari alla metà del livello alto; il livello basso viene trasmesso inalterato
d. in livello basso si usano due impulsi con ritorno a zero ciascuno di durata pari alla metà del livello basso; il livello alto viene trasmesso inalterato.

34) La codifica digitale bifase Manchester consiste:
a. nell'utilizzare un periodo di onda quadra per codificare il livello alto e un periodo con fase opposta per codificare il livello basso del segnale dati
b. nell'utilizzare un periodo di onda quadra per codificare il livello alto lasciando inalterato il livello basso del segnale dati
c. nell'invertire alternativamente i livelli alti, lasciando inalterati quelli bassi del segnale dati
d. nell'invertire la fase del segnale dati ad ogni periodo di clock.

35) Il codice ASCII è uno standard per la conversione di:
a. caratteri alfabetici, numerici e di altro tipo in numeri
b. caratteri alfabetici, numerici e di altro tipo in cifre
c. soli caratteri alfabetici in numeri
d. soli caratteri numerici e di altro tipo in cifre.

36) Cryptography developed to such extent:
a. to protect the information being sent through telematic means
b. because people liked secret codes
c. because people wanted to make it difficult for others to understand them
d. to diffuse the information being sent through telematic means.

37) The telematic transmission of data:
a. involves the use of wire
b. involves the use of copper cables
c. involves the use of computers and the Internet
d. doesn't involve any of the above.

38) Privacy in the transmission of data refers to:
a. the protection of the data to be sent
b. the protection of your money
c. the protection of a secret
d. none of the above.

Chiavi di correzione ed elementi di adeguatezza.

1) c. 2) a. 3) a. 4) Può essere assimilata a quella tra persone presenti, perché l'incontro di volontà concordanti tra le parti avviene contestualmente, ed è questo che la legge richiede per il perfezionamento del contratto. 5) L'ordinamento, come principio generale, considera i diritti del singolo come attenuabili di fronte al superiore interesse della collettività. Il caso della corrispondenza del fallito controllata dal curatore può essere spiegato alla luce di questo principio. 6) c. 7) b. 8) c. 9) c. 10) Per trasmettere il livello alto si usano alternativamente impulsi di polarità positiva e negativa, mentre il livello basso si trasmette con lo zero. 11) Si evitano componenti continue del segnale dati e si utilizza un periodo di onda quadra per codificare il livello alto e un periodo con fase opposta per codificare il livello basso. 12) d. 13) b. 14) a. 15) c. 16) Si riporta un possibile segmento di programma in linguaggio C che, data la stringa frase [...] genera una stringa codificata frase 1 [...]

```
for(i=0;frase[i]!='\0';i++)
  {
  if(isalpha(frase[i])) /*Si verifica se il carattere è di tipo alfabetico.*/
  { frase1[i]=frase[i]+3; /*Si assegna ad ogni carattere di frase1[] il
            carattere ASCII che si trova tre posizioni più avanti.*/
      if(frase[i]=='X') frase1[i]='A'; /*I caratteri X,Y,Z e x,y,z */
      if(frase[i]=='x') frase1[i]='a';
      if(frase[i]=='Y') frase1[i]='B'; /*vengono sostituiti rispettivamente*/
      if(frase[i]=='y') frase1[i]='b';
      if(frase[i]=='Z') frase1[i]='C'; /*dai caratteri A,B,C e a,b,c.*/
      if(frase[i]=='z') frase1[i]='c';
    }
  else frase1[i]=frase[i];
 }
 frase1[i]='\0';.
```

17) b. 18) b. 19) c. 20) d. 21) c. 22) d. 23) a. 24) d. 25) a. 26) b. 27) c. 28) The need for this technique has developed to such extent to protect information travelling over a medium which can be accessed by anyone. 29) We call the process of transferring information from one place to another telematic when we use a telematic means to do it. 30) The idea of privacy in telematic transmissions concerns the protection of the data being sent. 31) b. 32) a. 33) b. 34) a. 35) a. 36) a. 37) c. 38) a.