

Tratto dal Testo
Ettore Panella - Giuseppe Spalierno
Corso di Telecomunicazioni 2
Edizioni Cupido

CAPITOLO SESTO

INTERNET, SICUREZZA E PRIVACY

1. Generalità

Internet è una rete di computer che consente di collegare tra loro, tramite un sofisticato sistema di gestione, host appartenenti a reti diverse: è, quindi, una "rete di reti" che unisce reti di computer di tutto il mondo in modo estremamente efficace.

In fig.1 è rappresentato un collegamento tra 4 reti denominate A, B, C e D e la modalità secondo cui un utente privato remoto può accedere alle risorse di qualsiasi computer di qualsiasi rete disponendo di un adattatore remoto di rete, come il modem analogico o l'adattatore ISDN o ADSL, e di un permesso di accesso al nodo 3 della rete D tramite linea telefonica, di solito commutata.

Internet utilizza i gateway o router (instradatore) con la funzione di collegamento tra più reti.

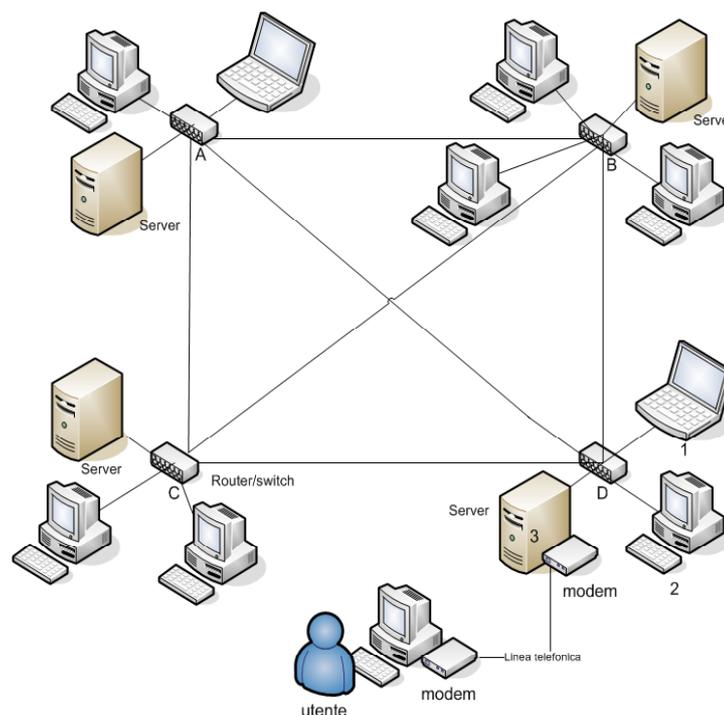


Fig.1. - Collegamento tra 4 reti A, B C e D e collegamento di un utente remoto al nodo 3 della rete D.

La tecnica di trasmissione utilizzata da internet è a *commutazione di pacchetto e servizio a datagramma* come è stato esaminato nel precedente capitolo.

Il *gateway* è un dispositivo di rete dotato di software che è in grado di stabilire il percorso che deve compiere un pacchetto di dati per transitare da una rete locale all'altra.

Il gateway deve occuparsi anche della trasformazione strutturale del pacchetto in quanto la successiva rete locale di transito può essere completamente diversa da quella corrente.

In tutto il mondo vi sono centinaia di milioni di utenti internet ed il loro numero cresce continuamente.

Internet, quindi, è l'insieme di migliaia di reti collegate da protocolli che consentono agli utenti di ciascuna di esse di comunicare o di utilizzare i servizi situati su una qualsiasi delle reti componenti.

Il protocollo utilizzato è il TCP/IP (Transmission Control Protocol / Internet Protocol).

1.1. Breve storia di internet

Per mantenere attiva la struttura delle comunicazioni degli Stati Uniti nell'evento di una guerra nucleare, un'agenzia del governo, la *Advanced Research Project Agency* (ARPA) sviluppò, alla fine degli anni 60, un nuovo tipo di rete a commutazione di pacchetto (packet switching) che iniziò a collegare 4 computer: tre in California ed uno in Utah usando il *Network Control Protocol* (NCP). Tale rete, conosciuta come *ARPAnet*, nei primi anni 70 rappresentava il cuore di una serie di reti.

Agli inizi degli anni 80 la *National Science Foundation* creò una propria rete, la NSFNET, funzionante a 56Kbps, molto veloce per gli standard di allora.

La NSFNET divenne la principale rete portante di internet (definita "backbone" - spina dorsale) che utilizzava il protocollo TCP/IP.

La rete si dimostrò ben presto un successo vero e proprio e furono sempre più le università che aderirono all'iniziativa collegando i propri sistemi. Nel 1986 vi erano più di 5000 computer (host) collegati ad internet.

Gli studenti delle università che hanno utilizzato internet si sono resi conto di quanto la rete potesse essere un valido strumento per uso personale e di lavoro. Ben presto piccole aziende si collegarono in numero crescente. Le BBS commerciali incominciarono a fornire l'accesso ad internet e nacquero i *service provider* che consentivano a chiunque avesse un computer e un modem di collegarsi alla *rete delle reti*.

La crescita demografica di internet continua ancora oggi, soprattutto nei paesi in via di sviluppo. Nei paesi più industrializzati, come l'Italia, si è quasi raggiunta la saturazione.

Inizialmente la maggior parte delle informazioni disponibili su internet erano di nazionalità americana e di natura scientifica, attualmente i siti in internet sono di utenti privati, di servizi e commerciali.

Internet non è posseduta né gestita da una singola autorità ma per mantenere uno standard nei protocolli fu istituita nel 1992 l'Internet Society.

Sempre nel 1992 il CERN di Ginevra introdusse un sistema multimediale ad ipertesto con tecnologia client/server denominato "World - Wide - Web", attualmente il sistema più usato in internet.

Nello stesso anno il National Center for Supercomputing Application (NCSA) presso l'Università of Illinois rilasciò il software Mosaic che consente l'utilizzo del WWW e la NSFNET fu potenziata a 44.736Mbps.

Nel 1994 la NSF cambiò strategia trasferendo il controllo del "backbone" ad entità commerciali ed abolendo le restrizioni sul traffico commerciale.

2. I servizi di internet

Gli inserzionisti del mondo internet sono numerosissimi ed appartengono a categorie molto differenti: università, scuole, "provider", enti pubblici, società sportive, ditte commerciali, utenti privati, medici, ingegneri, professionisti, ecc.

Il materiale offerto è per lo più gratuito. I documenti di un certo interesse (legislazioni, norme tecniche, ecc.) sono forniti a pagamento o previo una sottoscrizione di abbonamento.

Tale materiale spazia dalle semplici informazioni sulle tematiche di interesse dell'inserzionista sotto forma di testo, immagini statiche o dinamiche, suoni, filmati, ecc., a del materiale di supporto di tipo testo a sfondo culturale, tecnico, sociale ed altro, software freeware e shareware¹.

I servizi fondamentali, a cui un utente internet può accedere, permettono di visualizzare le pagine "Web" scelte fra le innumerevoli disponibili, salvare su disco i file di particolare interesse e trasmettere i propri file su rete ad un gruppo di utenti o ad un solo utente internet.

2.1. WWW (*World Wide Web = La grande ragnatela mondiale*)

Noto anche come W3, è il sistema di navigazione ipermediale (ipermediale = ipertestuale + multimediale: ipertesto = collegamento da un testo ad un altro mediante la pressione del pulsante del mouse; multimediale = presenza di immagini, suoni e filmati), oggi il più diffuso, che integra testo, immagini, suono ed animazione.

Grazie alla sua semplicità di uso internet si è diffuso nel mondo in questi ultimi anni a ritmi vertiginosi.

Il WWW si avvale del protocollo HTTP (HyperText Transfer Protocol) che permette il trasferimento di dati strutturati in modo ipertestuale.

Nella rete internet sono presenti numerosissimi file di testo dal nome indecifrabile.

Come fare ad orientarsi e a scegliere quello che interessa a noi? Il problema è stato brillantemente risolto nel 1992 al CERN di Ginevra: l'idea è quella di utilizzare la realtà ipertestuale per collegare tra loro tutte queste informazioni e per presentarle in forma grafica senz'altro più accattivante.

Il sistema funziona come l'help di Windows: facendo clic su una voce sottolineata (voce calda hotword) si ottiene sul monitor il relativo documento.

Il linguaggio utilizzato, denominato HTML (HyperText Markup Language), consente, attraverso l'uso di semplici comandi impartiti in formato ASCII, di definire titoli, paragrafi, liste, figure e link (collegamenti) remoti e locali.

Attualmente è disponibile la versione 4 di HTML.

Esistono specifici programmi che consentono di generare file ipertestuali in linguaggio HTML: questi sono noti come editor di HTML.

Oltre alle pagine web scritte con i comandi dell'HTML, sono presenti in internet documenti cosiddetti dinamici perché realizzati automaticamente in funzione delle informazioni richieste dall'utente attraverso la compilazione di un modulo.

¹ Freeware = Di libero utilizzo; Shareware = In prova in forma limitata per un tempo limitato.

Le pagine web dinamiche sono impaccettate da un application server, residente sul computer server del provider.

L'application server è un vero e proprio linguaggio di programmazione che accetta in input i dati inviati dall'utente e genera, in output, la pagina web elaborata arricchita, eventualmente di dati prelevati da un database anch'esso residente sul server.

Tra questi application server ricordiamo il PHP (Hypertext PreProcessor), ASP (Active Server Page) e JSP (Java Server Page).

Nel mondo Windows, le pagine scritte in HTML sono visualizzate con appositi programmi che gestiscono testo, grafica, suono, animazioni.

Tali programmi sono denominati *browser* (sfogliatori) e sono: Microsoft Internet Explorer, Netscape Navigator, Opera, Mozilla, ecc.

Alcuni di questi pacchetti software, con certe limitazioni di utilizzo, sono gratuiti, di libero uso, disponibili su numerose piattaforme operative ed importabili via internet in formato compresso come, ad esempio, il formato ZIP.

2.1.1. Internet Explorer

I sistemi operativi Windows 98, ME, XP della Microsoft includono il programma Internet Explorer per la navigazione in internet. L'ultima versione attualmente disponibile è la 6.0 SP2. Per passare alla versione 6.0 SP2 è sufficiente disporre di un CD allegato in omaggio alle riviste mensili del settore elettronico, informatico e telematico. L'installazione dell'ultima versione riconosce e cancella preventivamente le eventuali versioni precedenti.

In figura 2 si mostra la schermata parziale di Internet Explorer 6.0.

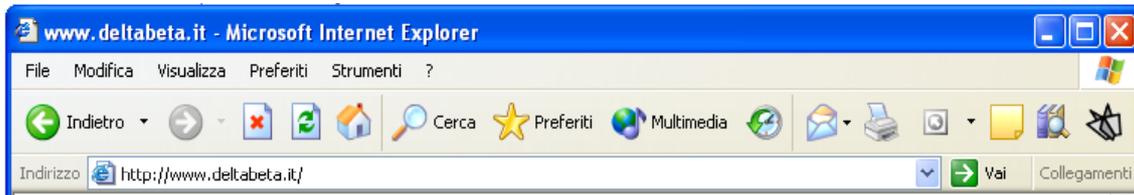


Fig.2. – Schermata parziale di Microsoft Internet Explorer versione 6.0 SP2.

Barra del titolo

Fornisce il titolo della pagina Web che si sta consultando, il nome del programma (Microsoft Internet Explorer) ed i tre classici interruttori di riduzione ad icona, ingrandimento e chiusura.

Barra dei menù

La barra successiva fornisce i consueti menù a tendina: *File*, *Modifica*, *Visualizza*, *Preferiti*, *Strumenti*, ?

File. Contiene, sostanzialmente, le voci presenti nell'omonimo menù file degli applicativi di Windows e precisamente: nuovo, apri, modifica, salva, anteprima di stampa, stampa, invia, importa ed esporta. È interessante, del comando salva, la modalità "Pagina Web, completa": vengono salvati sia il testo che gli oggetti multimediali come le immagini e viene creata una cartella, con lo stesso nome del file salvato, che contiene gli oggetti presenti nella pagina. Il comando anteprima di stampa, assente nelle precedenti versioni, permette di visionare l'impaginazione complessiva prima di iniziare la stampa.

Modifica. Anche in questo menù ritroviamo le voci tipiche di altri programmi che sono: *taglia, copia, incolla, seleziona tutto, trova.*

Visualizza. Consente di visualizzare o nascondere le varie barre degli strumenti, le dimensioni del carattere, il codice HTML della pagina in esame, di passare alla pagina precedente, successiva o alla pagina di partenza, di visualizzare la pagina a tutto schermo.

Preferiti. È un menù particolare di Explorer. Esso contiene gli indirizzi di pagine Web di notevole importanza già presenti nel programma o inseriti da noi stessi. È sufficiente fare click col mouse sulla voce che ci interessa per accedere a quel sito. Le prime due voci sono: *Aggiungi a Preferiti* e *Organizza Preferiti*. Se si desidera memorizzare l'indirizzo della pagina che sta esplorando è sufficiente attivare il comando *Preferiti/Aggiungi a Preferiti*. In tal caso si aggiunge, nell'elenco delle pagine Web inserite in *Preferiti*, il titolo della pagina corrente. Se l'elenco delle pagine inserite in *Preferiti* è molto lungo è possibile organizzarle in cartelle attivando il comando *Preferiti/Organizza Preferiti*.

Strumenti. La voce più importante di tale menù è senza dubbio *Opzioni Internet*. Questo comando consente di cambiare le impostazioni del programma.

? Il menù contrassegnato col punto interrogativo fornisce un comodo *help in linea*.

Barra dei pulsanti standard

La barra degli strumenti posta al rigo successivo a quello dei menù contiene dei pulsanti corrispondenti alle funzioni di uso frequente. Essi sono:

indietro, per visualizzare sul monitor la pagina Web precedente;

avanti, per visualizzare quella successiva;

termina per interrompere, durante la navigazione, l'acquisizione dei dati di una pagina Web;

aggiorna, per ottenere l'eventuale nuova versione di una pagina Web;

pagina iniziale, per visualizzare la pagina con cui si apre la sessione Internet Explorer;

cerca, per cercare una parola all'interno del documento visualizzato;

preferiti, per accedere alla lista dei documenti inseriti in "preferiti";

multimedia, per accedere alle risorse multimediali locali e remote;

cronologia, per avere l'elenco dei siti visitati di recente;

schermo intero, per visualizzare la pagina Web a schermo intero;

posta, per leggere o inviare un messaggio col programma di posta predefinito;

stampa, per stampare la pagina Web o una sua parte;

modifica, per modificare, con apposito programma, il contenuto di una pagina Web;

discussione, consente l'attivazione di una discussione collegandosi ad un server di discussione;

ricerche, permette di ottenere il significato e la traduzione in altra lingua del termine inserito nella casella di testo;

organizzatore ricerche, permette di conservare ed organizzare le ricerche effettuate in un file.

Barra dell'indirizzo

In essa si può scrivere l'indirizzo ipertestuale della pagina Web che vogliamo visitare. Il pulsante a discesa posto sulla destra consente di scegliere velocemente uno degli indirizzi già inseriti in precedenza nella barra degli indirizzi.

Le varie barre sono personalizzabili per cui non è escluso che ognuno di noi possa avere altre barre o altre voci in quelle precedentemente descritte.

In figura 3 si mostra la schermata di Opzioni Internet. La scheda “Generale” consente di stabilire la pagina iniziale, le impostazioni o l’eliminazione dei file

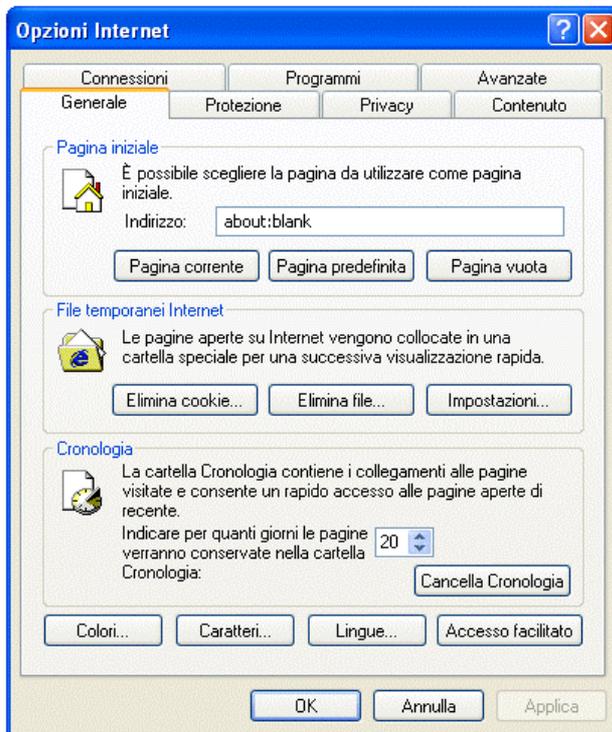


Fig.3. – Scheda “Generale” di Opzioni Internet.

temporanei e la cancellazione di *Cronologia*. I file temporanei sono quelli che sono stati visitati durante la navigazione in internet. Essi vengono memorizzati su hard disk in una cartella denominata “Internet Temporary files”.

La cartella *Cronologia* contiene i collegamenti alle pagine visitate e consente un rapido accesso alle pagine aperte di recente.

I quattro pulsanti in basso consentono di modificare i colori dei link ai siti non visitati e visitati, il tipo di carattere da usare per le pagine web che non specificano il font, la lingua scelta nel caso di siti con versioni in diverse lingue, l’eliminazione della formattazione per semplificare la visualizzazione della pagina.

Le altre schede di Opzioni Internet consentono di proteggere i propri dati da “occhi indiscreti” quando si inviano moduli compilati con le proprie generalità o con gli estremi della propria carta di credito, limitare a siti attendibili il collegamento ad internet impedendo, ad esempio, il collegamento a siti con contenuto violento o pornografico, di impostare e personalizzare il tipo di connessione, i programmi per la posta elettronica, la videoconferenza, l’editing HTML, ecc.

Merita un cenno l’impostazione del Server Proxy. Il Server Proxy, è un computer che conserva le pagine Web che gli utenti hanno richiesto e visitato. Se un altro utente che ha impostato il Server Proxy desidera visitare la pagina americana della Sony presente all’indirizzo www.sony.com, ad esempio, e questa è stata memorizzata nell’hard disk del Server Proxy, sarà quest’ultimo a fornire all’utente la pagina richiesta. In questo modo si velocizza il collegamento evitando così, di inoltrare la richiesta di nodo in nodo fino al sito originale della Sony.

Il server Proxy, periodicamente, controlla se le pagine memorizzate sono state, nel frattempo, modificate; in tal caso le aggiorna. Per evitare di saturare ben presto l’area di memoria disponibile, il Proxy cancella le pagine Web memorizzate non richieste da più tempo.

2.1.2. Navigazione

Per poter accedere direttamente ad una pagina Web pubblicata su internet, è necessario indicare nel campo "Indirizzo", presente in tutti i “browser”, l’indirizzo inequivocabile di quel documento.

Tale indirizzo prende il nome di URL (Uniform Resources Locator) ed individua il tipo di servizio richiesto, l'indirizzo del server nel quale è presente il documento e l'indirizzo, con struttura a directory, del documento stesso.

Commentiamo, ad esempio, il seguente URL:

<http://www.deltabeta.it/elettronica/elettronica.htm>

http ci informa che vogliamo utilizzare il protocollo per il trasferimento di ipertesti (Hyper Text Transfer Protocol);

:// indicano la separazione tra il tipo di protocollo e l'indirizzo che si trova a destra;

www.deltabeta.it è il nome del server, cioè del computer che conserva nella sua memoria di massa il documento in questione;

elettronica è la sottodirectory in cui si trova il documento **elettronica.htm**.

Si notino le barre inclinate per l'individuazione del percorso; esse non sono quelle rovesciate, tipiche del DOS, ma seguono la filosofia Unix.

Il WWW integra, in buona parte, anche le attività di internet che verranno esaminate nei successivi paragrafi.

Per ottenere tali servizi è necessario porre nel campo "Indirizzo" del programma browser i seguenti comandi:

Servizio	Indirizzo	Effetto
www	http://www.libero.it	per accedere al sito Web del provider <i>libero</i>
e-mail	mailto:r.bianchi@tin.it	per inviare posta elettronica all'utente r.bianchi del provider <i>tin</i>
interno	file:///A:\home.htm	per visualizzare su monitor il file home.htm residente nel drive A
telnet	telnet://launchpad.unc.edu	lancia l'applicativo telnet in grado di comunicare col il computer di nome launchpad.unc.edu. Il nostro computer diventa, così, un terminale remoto.
ftp	ftp://ftp.libero.it/pub	richiama la directory <i>pub</i> del server <i>ftp.libero.it</i> . Cliccando su un file della directory che appare sul monitor si effettua la ricezione del file in questione.
newsgroup	news: it.istruzione.scuola	Viene caricato l'elenco dei documenti appartenenti al gruppo di discussione <i>it.istruzione.scuola</i>

2.2. Posta Elettronica (E-Mail)

Nota come e-mail (Electronic Mail), la posta elettronica consente di inviare il documento scritto al computer in forma elettronica all'utente destinatario senza la necessità di stamparlo ed inviarlo per posta convenzionale o per fax.

La possibilità di inviare posta istantaneamente e in una qualsiasi località del mondo ha affascinato tutti ed in particolare il mondo universitario e commerciale.

I primi servizi di posta elettronica erano strutturati in funzione dei terminali e degli ambienti operativi specifici. Nacquero, così, sistemi commerciali come CompuServe e MCI mail ed altri che avevano il difetto di essere autonomi e chiusi.

Successivamente, attraverso una qualche forma di "gateway", è stato possibile inviare posta elettronica tra sistemi diversi.

Oggi tutti i sistemi di posta elettronica sono collegati ad internet per cui è possibile lo scambio di informazioni tra sistemi differenti.

L'invio della posta elettronica via internet avviene specificando l'indirizzo del destinatario.

L'indirizzo di posta elettronica si compone di due parti: il nome dell'utente, scelto dallo stesso utente e il nome del suo provider.

I due campi sono separati dal carattere @ (at = presso).

Ad esempio, l'indirizzo e-mail del signor "Mario Rossi" avente "orizzonte" come provider italiano, potrebbe essere:

mario.rossi@orizzonte.it

Il titolare di un indirizzo di posta elettronica può inviare e ricevere posta.

Inizialmente la posta elettronica prevedeva il solo scambio di messaggi in formato testo ed i programmi di gestione si avvalevano di comandi da impartire a carico dell'utente. Oggi è possibile allegare ad un messaggio anche dei file binari contenenti programmi o immagini.

I programmi di posta elettronica consentono un'ampia personalizzazione di più caselle di posta elettronica e più profili utente. Possono memorizzare i messaggi trasmessi e ricevuti, consentono la creazione di sottocartelle per l'archiviazione dei messaggi, la gestione di una rubrica contenente gli indirizzi di posta dei nostri interlocutori.

Lo scambio della posta elettronica avviene nel seguente modo:

- Il mittente, utilizzando il software che gli consente di trasmettere la posta, digita l'indirizzo di posta elettronica del destinatario ed il messaggio da inviare. L'indirizzo del mittente è inserito automaticamente;
- Terminata la compilazione del testo, il mittente esegue il comando di invio;
- La posta viene trasmessa mediante il protocollo SMTP (Simple Mail Transfer Protocol), porta 25, al proprio nodo: quest'ultimo, esaminato l'indirizzo del server destinatario provvede all'inoltro della posta verso quel server;
- Il server destinatario riceve la posta e la registra nella memoria di massa nell'area riservata (casella postale) all'utente destinatario;
- L'utente destinatario, dopo aver acceso il proprio computer ed attivato il software di posta elettronica, esegue un controllo nella propria casella postale (Ricevi posta): se c'è posta il server destinatario "svuota" la casella postale trasferendo i dati nel computer dell'utente destinatario utilizzando un protocollo di nome POP3 (Post Office Protocol versione 3), porta 110. È possibile leggere la posta senza svuotare la casella postale. In tal caso il destinatario riceve la copia della posta giacente nella propria casella che continua a conservare i vari messaggi.

Per meglio comprendere il funzionamento si può ricorrere alla metafora dell'inoltro di una lettera postale convenzionale.

Una lettera è costituita da tre parti: destinatario, mittente e testo che si vuole inviare.

Il mittente imbuca la lettera (operazione invia).

L'operatore postale porta il contenuto della buca al più vicino ufficio postale (trasferimento dati tramite il protocollo SMTP al proprio server).

L'ufficio postale trasmette la lettera all'ufficio postale più vicino al destinatario (trasferimento dati da nodo a nodo).

L'ufficio postale destinatario, tramite il postino, pone la lettera nella casella postale dell'utente.

L'utente destinatario apre la sua casella e raccoglie la posta (trasferimento dati dal server destinatario, tramite protocollo POP3, all'utente destinatario).

2.2.1. Mailing list

Una Mailing list, o lista postale, è costituita da un gruppo di utenti che intendono produrre o semplicemente leggere della documentazione su certi temi specifici.

L'iscrizione alla Mailing List è, generalmente, libera e gratuita e può avvenire in modo automatico inviando la richiesta per posta elettronica al computer "list server" di cui si conosce l'indirizzo oppure ad un responsabile che ha la facoltà di accogliere la richiesta o di respingerla.

La Mailing list ha un moderatore col compito di controllare il corretto funzionamento del sistema. Alle volte il moderatore interviene nella discussione per fornire chiarimenti, consulenze o per ribadire il regolamento interno della lista.

In alcune liste postali il moderatore ha la facoltà di controllare il contenuto della posta in arrivo e di pubblicare solo quella che ha attinenza al filo conduttore (thread) della discussione e di cestinare quelle offensive, cariche di insulti o altro, purtroppo sempre in agguato sulla rete.

L'utente che produce un documento per la lista, inoltra il messaggio per posta elettronica al computer "list server"; quest'ultimo lo ritrasmette, sempre via e-mail, a tutti gli iscritti alla lista.

La Mailing-list è, quindi, un gruppo di discussione chiuso ai suoi iscritti.

2.2.2. Outlook Express

Il programma di posta elettronica *Microsoft Outlook Express* consente la gestione della posta elettronica in entrata ed in uscita ed inoltre consente la lettura delle news di Usenet.

Il programma, pur essendo freeware, consente il multiaccount, il filtraggio dei messaggi in arrivo e la gestione dei profili.

Il *multiaccount* consiste nella possibilità di scaricare posta avendo numerosi indirizzi di posta elettronica mentre il *filtraggio* dei messaggi in arrivo consente di smistare automaticamente le e-mail nella cartelle da noi predefinite in base a delle condizioni rispettate dalla e-mail in ricezione.

La creazione delle identità permette a più utenti di utilizzare Outlook Express e la Rubrica dello stesso computer. Due diversi membri di una famiglia possono, ad esempio, condividere un solo computer. Se si crea un'identità per ciascuno, ognuno potrà eseguire l'accesso con la propria identità e quindi visualizzare la propria posta e i propri contatti. Una volta creata la propria identità, è possibile organizzare i contatti nel modo desiderato creando delle sottocartelle.

Si possono creare due o più identità protette o meno da password, modificare le impostazioni di una identità, cancellare una identità.

Nella figura 4 si mostra la schermata tipica di Outlook Express in cui, nella parte inferiore, si scorgono 4 settori: Cartelle, Contatti, Lista dei messaggi, contenuto del messaggio.

Le cartelle hanno una struttura a directory e contengono le classiche cartelle di default di posta elettronica: *posta in arrivo*, *posta in uscita*, *posta inviata*, *posta*

eliminata e bozze. È possibile creare nuove cartelle di posta per meglio smistare i messaggi ricevuti e quelli inviati.

In “Contatti” troviamo la lista di utenti a cui abbiamo risposto o utenti da noi inseriti manualmente.

Nella parte destra compare la lista dei messaggi di cui è possibile immediatamente sapere il mittente, l’oggetto e la data ed orario dei messaggi ricevuti. Si noti che sono visualizzati due messaggi provenienti da Alice residenti nella sottocartella Alice di Posta in arrivo. Selezionando la cartella Posta inviata si vedrebbe sulla destra la lista dei messaggi inviati con i campi del destinatario, oggetto, la data e l’orario ed infine l’account col quale si è inviato quel messaggio di posta.

In basso a destra compare il contenuto del messaggio selezionato.

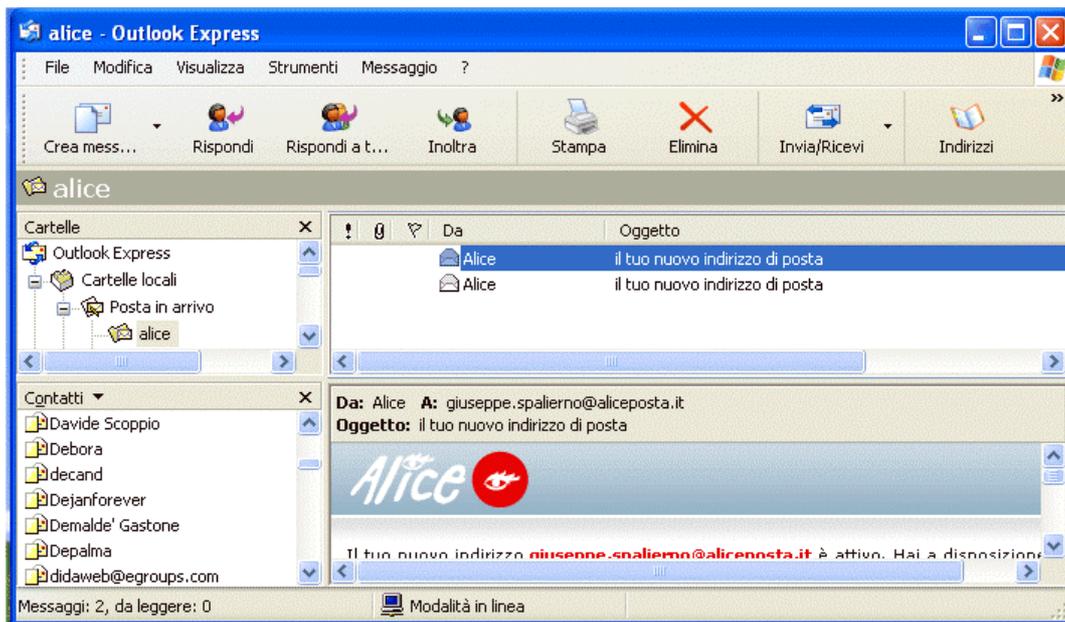


Fig.4. – Tipica schermata parziale di Outlook Express.

La barra dei menù contiene le voci: file, modifica, visualizza, strumenti, messaggio, ?

Senza dilungarci sulla descrizione delle voci contenute nei vari menù, ci limitiamo a dire che col *menù file* è possibile aprire, salvare, esportare, importare, stampare messaggi di posta elettronica e gestire le identità.

Il *menù modifica* consente di copiare, spostare, trovare, eliminare, svuotare cartelle e messaggi di posta.

Il *menù visualizza* consente svariate modalità di visualizzazione del programma e dei messaggi.

Il *menù strumenti*, di notevole importanza, consente di inviare o ricevere posta, di attivare newsgroup, di personalizzare, nelle modalità desiderate, le prestazioni del programma e di gestire gli account.

Il *menù messaggio* consente un certo numero di operazioni sui messaggi come generare un nuovo messaggio, rispondere ad un messaggio ricevuto, marcare un dato messaggio, ecc.

L’ultimo menù, infine, ci fornisce un adeguato *Help* in linea e scaricabile da Internet.

Il programma possiede, inoltre, una rubrica nella quale possiamo inserire tutti i dati di amici, parenti e conoscenti, dal loro indirizzo al loro numero telefonico.

La *barra degli strumenti* sotto quella dei menù presenta una serie di icone corrispondenti alle funzioni più frequenti svolte col programma in questione.

In particolare per scrivere un nuovo messaggio di posta si fa click sul primo pulsante a sinistra denominato “Crea messaggio”, i successivi tre pulsanti consentono di rispondere al mittente, a tutti i componenti della lista postale (mailing list) e di inoltrare un messaggio ricevuto ad un nuovo destinatario.

I pulsanti successivi consentono la stampa, l’eliminazione (trasferimento nella cartella posta eliminata), l’invio e la ricezione, l’utilizzo della rubrica e la ricerca di un messaggio.

Account

Quando si installa per la prima volta il programma di posta elettronica Outlook Express si deve fornire il proprio “account” (accredito) consistente nel proprio nome, indirizzo di posta elettronica, nome del server di posta elettronica per posta in uscita secondo il protocollo SMTP ed il nome del server di posta elettronica per posta in entrata secondo il protocollo POP3. È possibile, inoltre, aggiungere altri account di posta elettronica. Per far ciò si attiva il comando *account* dal menù *strumenti*.

Si ottiene la schermata del tipo mostrato in figura 5.

Attivando la linguetta “Posta Elettronica” è possibile, per un account di posta elettronica, aggiungere, rimuovere, modificare le proprietà, renderlo predefinito ed altro.

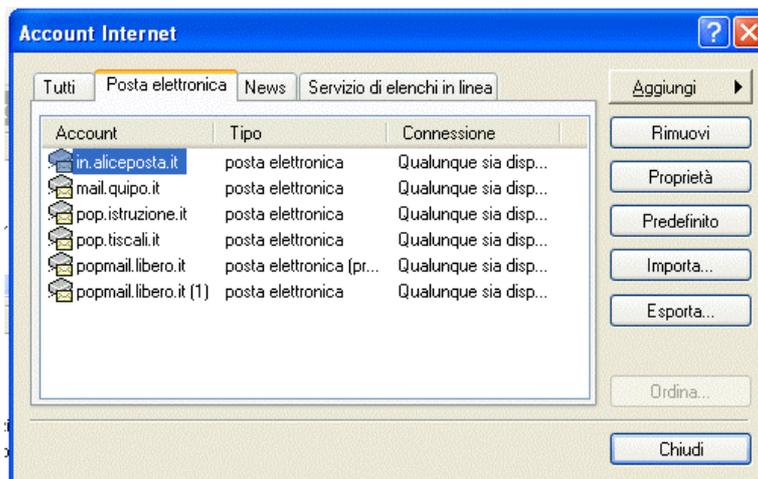


Fig.5. – Finestra per la creazione, modifica ed eliminazione di account di posta elettronica.

Creazione ed invio di una e-mail

Per creare una e-mail si fa clic sul pulsante *crea messaggio* oppure si deve attivare il comando *nuovo messaggio* dal menù *messaggio*.

Si noti che la finestra del nuovo messaggio presenta la barra dei menù con numerose voci di facile comprensione.

Si ottiene una finestra del tipo mostrato in figura 6 in cui si devono compilare alcuni campi.

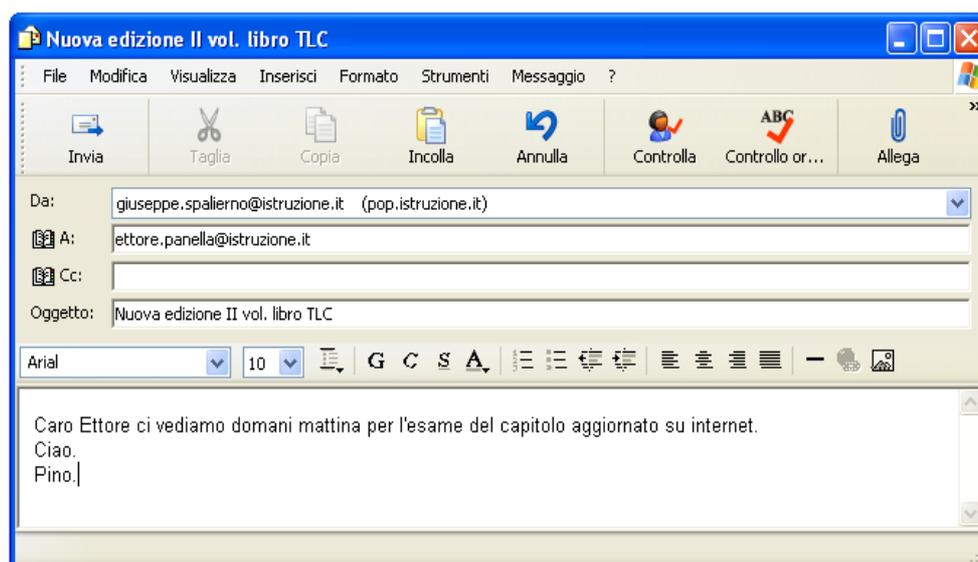


Fig.6. – Finestra per la composizione di un nuovo messaggio di posta elettronica.

Il campo *Da:* risulta compilato in automatico con l'account di posta di default. Agendo sulla freccia della casella a discesa è possibile scegliere l'account, tra quelli disponibili, col quale si vuole inviare il messaggio di posta. Nel campo *A:* si inserisce l'indirizzo di posta elettronica del destinatario. L'indirizzo può essere inserito manualmente oppure, se presente, lo si preleva dalla rubrica. Il campo *Cc:* significa Copia Conforme (oppure Carbon Copy) e contiene, eventualmente, l'e-mail di altri utenti che riceveranno il messaggio per conoscenza, non essendo loro i diretti destinatari.

Nel campo *A:* e nel campo *Cc:* si possono inserire due o più indirizzi e-mail tra loro separati da un punto e virgola.

Nel campo *oggetto* si inserisce l'oggetto del messaggio. Nel riquadro in basso, infine, si inserisce il messaggio vero e proprio che possiamo formattare utilizzando i comandi disponibili nella barra degli strumenti di formattazione (Font, dimensione, Grassetto, Corsivo, Sottolineato, ecc.).

È possibile allegare al messaggio uno o più file facendo clic sul pulsante che rappresenta la graffetta nella barra degli strumenti posta nella parte alta della finestra oppure eseguendo il comando *Allegato* dal menù *Inserisci*.

Se l'allegato è un file di grosse dimensioni si preferisce utilizzare un programma compressore come winzip www.winzip.com o winrar www.winrar.com per ridurre le dimensioni dell'allegato, ammesso che questo sia ragionevolmente comprimibile. Infatti vi sono alcune tipologie di file, come le immagini GIF, JPG, l'audio MP3, ecc. che sono già compressi per natura e quindi l'operazione di compressione non fornisce vantaggi apprezzabili.

È possibile allegare ad un messaggio due o più file contemporaneamente (oppure un unico file compresso che contiene un insieme di file).

In fase di ricezione di messaggi con file allegati, questi ultimi sono contrassegnati dal simbolo della graffetta. Facendo doppio clic sulla graffetta oppure sul nome del file contenuto nella casella di testo *Allega:*, come si mostra in figura 7, si ottiene una nuova finestra che chiede se si desidera aprire o salvare su disco il file allegato.

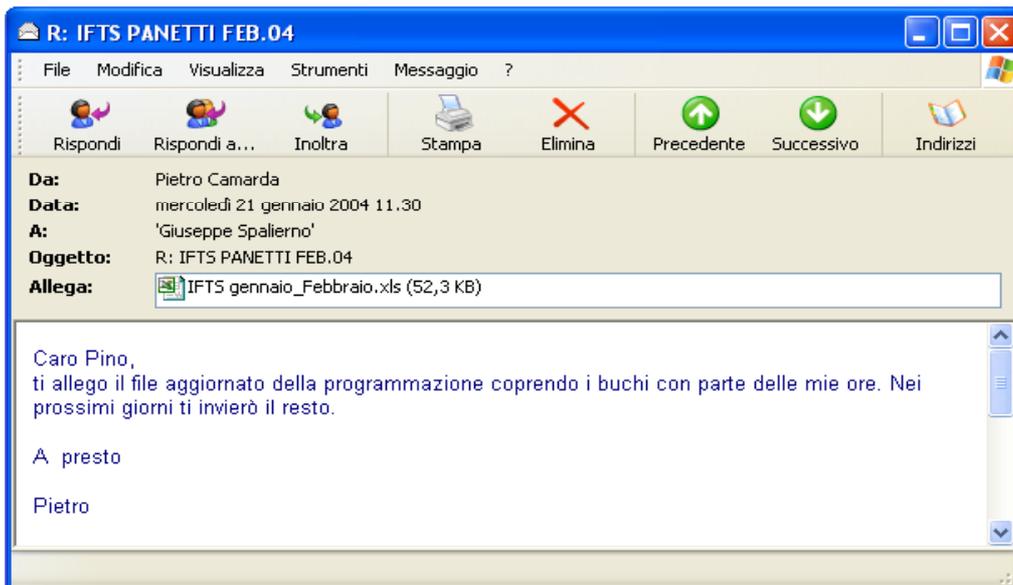


Fig.7. – e-mail con allegato.

Prima di aprire un file allegato occorre accertarsi della provenienza: infatti alle volte esso potrebbe essere un virus che qualche utente malintenzionato ci ha inviato.

2.3. NEWSGROUP

I newsgroup sono gruppi di discussione su specifici argomenti che funzionano con modalità differente dalle mailing-list esaminate precedentemente.

Il protocollo utilizzato è denominato NNTP (Network News Transfer Protocol), porta 119.

Il suo funzionamento è abbastanza simile alla posta elettronica con la differenza che quest'ultima consta nella trasmissione di un messaggio di un singolo utente ad un altro singolo utente (se non si inviano copie in Cc e Bcc e se non si è inseriti in una mailing list, lista postale, nel qual caso un messaggio è inviato a tutti gli aderenti alla lista).

Il documento elaborato col protocollo NNTP viene pubblicato all'interno di una apposita sezione, individuata dall'autore del messaggio, e reso disponibile a chiunque tenti di leggere le "News" pubblicate all'interno di quell'area.

Attualmente esistono nel mondo più di 100.000 gruppi di discussione che spaziano su tutti gli argomenti possibili ed immaginabili. La gestione delle News da parte del provider è piuttosto onerosa: infatti ogni giorno viene generata una quantità di dati che supera il Gbyte.

Riducendo il numero di News si riesce a contenere l'occupazione di memoria centrale del server. L'obiettivo è raggiunto riducendo sia il tempo di vita degli articoli pubblicati (1 mese, 15 giorni, 1 settimana) che il numero dei gruppi di discussione.

Usenet di internet è una gigantesca BBS², una serie di migliaia di conversazioni che si estendono in tutto il mondo. Un messaggio inviato su Usenet può essere letto da un qualsiasi utente internet.

Poichè Usenet è un sistema di discussione pubblica, a causa delle sue enormi dimensioni, gli argomenti sono stati suddivisi in numerose categorie, i *newsgroup*.

I nomi dati ai newsgroup consentono, in modo intuitivo, di comprendere gli argomenti trattati in quel gruppo di discussione.

² Bulletin Board = Banche dati accessibili via modem.

Ad esempio `it.annunci.usato.informatica` è un newsgroup italiano in cui gli utenti inseriscono o rispondono ad annunci sull'usato in campo informatico.

I newsgroup contengono anche centinaia di discussioni sull'argomento ulteriormente suddivisi e raggruppati in argomenti specifici.

Un programma di news è Free Agent che consente di leggere le news anche offline³.

Il programma si presenta con una interfaccia grafica e consente di richiamare dal proprio server l'elenco dei gruppi di discussione. Poiché questi ultimi, a seconda delle capacità del proprio nodo, ammontano a numerose migliaia, si suggerisce di leggere i titoli dei newsgroup a modem spento per evitare inutili spese telefoniche e per individuare quelli che possono interessare.

Successivamente si seleziona col mouse il titolo del gruppo di discussione interessato e si clicca due volte in rapida successione: il nostro computer si collega al server chiedendo l'elenco degli articoli del gruppo di discussione selezionato.

È possibile richiedere l'elenco di tutti gli articoli, o di un numero limitato di essi.

L'elenco degli articoli riporta, per ciascun di essi, la dimensione del documento, l'oggetto, il nome dell'autore, la data e l'ora di inoltro.

Per ricevere, finalmente, un documento si clicca due volte sul relativo titolo.

Si può cliccare su più titoli e in tal caso la richiesta dei vari documenti genera una coda di messaggi in arrivo che termina dopo la ricezione dell'ultima news.

Oltre a ricevere le news, è possibile inviare news specificando il gruppo di discussione che interessa, è possibile inviare posta elettronica sia ad un utente qualsiasi che, ad esempio, in risposta a colui che ha pubblicato una news (nel caso in cui si voglia rispondere privatamente e non pubblicamente).

Con un programmi di Newsgroup non è possibile ricevere posta elettronica.

La procedura di configurazione di un programma di Newsgroup prevede che si specifichi il proprio indirizzo di posta elettronica, i nominativi del server di News e di e-mail ed una serie di altre informazioni relative alla presentazione e prestazioni del programma. Di solito le scelte di default sono ottimali. Si riportano in tabella 1 gli indirizzi di alcuni server di news con l'avvertenza che, spesso, essi rispondono solo se siamo collegati ad internet attraverso il relativo provider.

Tabella 1. – indirizzi di alcuni server di news

Provider	Indirizzo newsgroup
Tin	news.tin.it
Libero	powernews.libero.it
Tiscali	news.tiscali.it
Supereva	news.supereva.it
Infinito	news.albacom.it
Mclink	news.mclink.it
Galactica	news.galactica.it

Outlook Express permette di gestire le news di Usenet. L'impostazione di un server di news segue le specifiche espresse nel precedente paragrafo relativo alla posta elettronica a proposito della creazione di un account.

Subito dopo aver definito il server di news al quale collegarsi, Outlook Express chiede se si desidera scaricare la lista dei newsgroup, operazione che richiede qualche minuto poiché i newsgroup disponibili sono decine di migliaia.

Si seleziona il newsgroup e successivamente di fa doppio clic per accedere ai titoli delle ultime news pubblicate dagli utenti.

³ Fuori linea, cioè a modem spento. Le news sono lette dal disco rigido sul quale sono state precedentemente salvate.

Si seleziona un titolo e si fa doppio clic per poter leggere la relativa news.

Si può comporre una news per poi poterla pubblicare sul newsgroup scelto e si può rispondere ad una news di un altro utente. In tal caso le varie news di un dato newsgroup che hanno stesso oggetto vengono raggruppate per poter meglio seguire il dibattito che si viene così a determinare tra i vari utenti. È possibile, inoltre, rispondere privatamente al mittente via posta elettronica.

2.4. FTP

FTP (File Transfer Protocol) è stato il primo protocollo per trasferire files tra diversi sistemi. Ancor oggi rappresenta un valido sistema per trasferire immagini, testo e programmi eseguibili localizzati in computer remoti e salvarli sul proprio hard-disk o, viceversa, per trasmettere un proprio file ad un computer remoto.

Il software che gestisce il protocollo FTP può avere una interfaccia di tipo testo e, in tal caso, l'utente deve conoscere la sintassi dei comandi tipici di tale protocollo.

Attualmente sono disponibili dei programmi ad interfaccia grafica che consentono le varie attività dell'FTP semplicemente cliccando su dei pulsanti.

Il protocollo FTP può essere utilizzato in modo anonimo o con chiave di accesso.

Nel primo caso l'accesso al server FTP remoto è consentito rispondendo "anonymous" alla richiesta "User ID" ed inserendo il proprio indirizzo di e-mail nel campo "password"; nel secondo caso si devono inserire i dati personalizzati di User ID e di password.

I browser Web come NETSCAPE ed EXPLORER consentono di attivare l'FTP ma, ovviamente, con il software adatto è possibile ottenere prestazioni più spinte.

Alcuni di questi sono WS_FTP, Filezilla, ecc.

I programmi si presentano col monitor diviso in due parti: nella parte sinistra è presente una struttura del tutto simile a "Risorse del computer" che fornisce le informazioni del proprio computer (Sito Locale) e nella parte destra quelle del computer remoto al quale ci si collega (Sito Remoto).

Per entrambi i computer le informazioni sono costituite dall'elenco dei drive, dalle directory di ciascun drive e dall'elenco dei file contenuti nella directory selezionata.

Le attività possibili, mediante click del mouse su relativi pulsanti sono:

- Cambia Directory,
- Crea Directory,
- Rimuovi Directory,
- Visualizzazione del file,
- Esecuzione del file,
- Ridenominazione del file,
- Cancellazione del file,
- Trasferimento da locale a remoto o da remoto a locale.

Ovviamente, alcune di queste funzioni potrebbero non essere possibili sul computer remoto, specialmente se l'accesso è anonimo.

Per la connessione al computer remoto si deve attivare il relativo pulsante che ci mostra una finestra di dialogo in cui inserire l'indirizzo FTP dell'host, i propri "User ID" e "password" e la sottodirectory di interesse del computer remoto.

Il comando più utilizzato è il trasferimento di un file dal computer locale a quello remoto e viceversa, tipiche azioni di coloro che aggiornano un sito web.

Durante il trasferimento del file appaiono dei messaggi con un istogramma che ci informano sulla lunghezza del file, sulla quantità di byte ancora da trasferire e sulla durata presunta del trasferimento che va, via via, riducendosi.

In genere i programmi trasferiti tramite FTP sono compressi in formato ZIP per ridurre il tempo di trasferimento dei dati.

2.5. TELNET

È un programma che possiede una interfaccia di tipo testo ed è impiegato per il collegamento a sistemi remoti: è possibile trasferire file, leggere directory eseguire a distanza programmi inseriti nell'host computer al quale ci siamo collegati purché, ovviamente, si abbia un 'account' su quel computer. Può essere utilizzato per collegarsi alle BBS inserite in internet al costo di una chiamata urbana. Occorre conoscere la sintassi dei comandi da impartire.

2.6. IRC (*internet Relay Chat*)

Consente di utilizzare la tastiera e di comunicare con chiunque in tempo reale. È possibile, ovviamente, anche ricevere messaggi da chiunque. L'utente sceglie un canale sul quale desidera avviare la conversazione. Le persone coinvolte nella conversazione sono molte e sullo schermo vengono visualizzate righe distinte nell'ordine in cui vengono trasmesse ed hanno come prefisso il nome dell'utente che le ha digitate.

Si ha, così, il 'salotto virtuale'. È possibile definire il nome di un nuovo canale al quale si possono collegare altri utenti.

È, inoltre, possibile inserire una password per consentire "la conversazione" ad un gruppo limitato di utenti (forum liberi, moderati, ecc.).

Nelle chat libere il livello della conversazione è di solito molto basso e i messaggi dei vari partecipanti arrivano accavallati e con un certo ritardo per cui spesso si perde il filo del discorso e ci si annoia quasi subito.

I programmi che consentono l'IRC sono WSIRC, MIRC, ecc.

Alcuni programmi, come ad esempio Windows Messenger, aggiungono alla chat strumenti multimediali: lavagna virtuale su cui disegnare condivisa con gli interlocutori, audio e video; queste ultime sono condivise con un solo interlocutore.

3. Collegamento ad internet

Molte Università e molte aziende hanno un collegamento diretto ad internet.

Procurandosi un *account*, richiedendolo all'amministratore di rete, è possibile accedere alla rete sfruttando l'elevata velocità del collegamento.

Il metodo più semplice ed economico per un utente privato che desidera collegarsi ad internet, invece, è quello di utilizzare la rete telefonica commutata. In particolare si inserisce un modem V90 o V92 funzionante a 56Kbps in download tra l'uscita USB del PC e la presa telefonica di casa. Spesso si utilizza il modem interno già integrato sulla scheda madre del computer.

Attualmente è possibile sfruttare la larga banda utilizzando un adattatore ADSL da inserire tra la linea telefonica e l'interfaccia USB del computer oppure tra la linea telefonica ed il connettore RJ45 della scheda di rete inserita nel proprio PC.

L'adattatore ADSL può essere fornito in comodato d'uso dal fornitore d'accesso della ADSL oppure lo si può acquistare personalmente. Il servizio ADSL di base, come è noto, consente un funzionamento asimmetrico con velocità di punta in download pari a 640Kbps corrispondente ad 80Kbyte al secondo. La velocità di punta in upload,

invece, è di 256Kbps corrispondente a 32Kbyte al secondo. Altri tipi di contratto consentono un funzionamento a 1280Kbps fino ad un massimo di 8Mbps.

Negli anni dell'avvento di internet in Italia (1993-1995), i modem più veloci erano in grado di funzionare a 14400bps o, al massimo, a 28800bps. Si doveva, inoltre, fare i conti con i disturbi della linea telefonica analogica che riduceva drasticamente l'efficienza di trasmissione. Oggi, invece, con il miglioramento della qualità delle linee e con la disponibilità di modem V90 – V92 a 56Kbps ed adattatori ADSL a 640Kbps, aventi circuiti per la compressione dei dati e la correzione automatica degli errori, è possibile comunicare alla velocità massima corrispondente a 7Kbyte al secondo (V90 – V92) e 80Kbyte al secondo (ADSL) se il traffico dati nella rete ce lo consente.

Ci si deve collegare, in pratica, ad un computer *server* (nodo) che a sua volta è collegato ad internet; il nostro è il computer *client*.

Il collegamento ad internet, come è noto, segue la filosofia client-server.

Il computer server è quello del fornitore di servizi (*provider*) che risulta collegato ad internet attraverso una linea telefonica dedicata ad alta velocità. Il provider, pertanto, paga al gestore telefonico il canone della linea dedicata ad alta velocità e una quota di affitto alla compagnia che gli fornisce, a sua volta, l'accesso ad internet (una specie di provider di livello superiore).

Più alta è la velocità della linea dedicata, più elevato è il numero di utenti che il provider può gestire senza provocare intasamenti nelle linee telefoniche.

All'aumentare, però, del numero di utenti collegati, diminuisce la velocità di comunicazione. La motivazione è alquanto semplice: una stessa banda di frequenza viene suddivisa tra più utenti per cui a ciascuno di essi è destinata una banda inferiore.

Il collegamento al provider dell'utente remoto tramite rete telefonica commutata (RTC) (connessione dial-up) avviene mediante il protocollo PPP (Point to Point Protocol).

Internet, come è noto, è una rete a *commutazione di pacchetto* con servizio a *datagramma* per cui i singoli pacchetti, lanciati nella rete, ricercano il percorso da un nodo all'altro fino a giungere a destinazione. Data la grande diversità delle varie reti a cui appartengono i nodi, i vari pacchetti devono essere "incapsulati", cioè rivestiti con informazioni supplementari che possono essere interpretati da tutti i computer.

Questi protocolli, numerosissimi, costituiscono il noto **TCP/IP** (*Transmission Control Protocol/internet Protocol*).

I protocolli TCP/IP sono attivati dal relativo software. Uno di questi software funzionante in ambiente Windows è il WINSOCK.DLL, una libreria dinamica che consente la comunicazione in internet. Per attivare questa libreria si deve mettere a punto un opportuno programma di accesso remoto. Un programma che utilizza la propria libreria WINSOCK.DLL è *Connessione Remota* del sistema operativo Windows.

Per attivare il collegamento in internet si devono inserire delle informazioni fornite dal provider circa il nome, il codice del server e il tipo di collegamento se SLIP o PPP, a quale porta seriale ci si connette, a quale velocità va impostato il modem o l'adattatore ADSL. Dopo aver acceso il modem ed eseguito il login con *Connessione Remota* si stabilisce la comunicazione tra il nostro computer e quello del provider.

Tale comunicazione prevede la chiamata telefonica, la fornitura, da parte del chiamante, dell'identificativo dell'utente e della password. Se tutto è corretto il modem dell'utente e quello del provider iniziano a negoziare la velocità di comunicazione ed altro. Tutto questo avviene automaticamente in modo trasparente per l'utente.

Quest'ultimo, se vuole, può attivare manualmente la procedura di collegamento, cosa che conviene fare solo se si è esperti e si desidera attivare la comunicazione con

caratteristiche diverse da quelle inserite in un file fornito dal provider noto come *script di login*.

Per accedere al mondo internet WWW occorre eseguire un programma browser del tipo Internet Explorer o Netscape Navigator precedentemente installato.

Per attivare gli altri servizi forniti da internet senza usufruirne dal programma browser, si deve avere a disposizione una serie di programmi del tipo descritti nel paragrafo 2.

L'abbattimento della comunicazione avviene attivando il comando disconnetti dopo aver richiamato il programma di Connessione Remota. In caso di imprevisti è sufficiente spegnere il modem o l'adattatore ADSL (per chi ha il modem interno al computer si consiglia di staccare la spina telefonica).

3.1. I costi

Le spese da sostenere per il collegamento ad internet con modem tramite accesso fornito da un *provider*, supponendo di disporre già di una comune linea telefonica commutata, di un PC con porta seriale o con interfaccia USB e di un modem, consistono nel contratto stipulato con il provider e nel consumo telefonico effettuato che causeranno un aumento dell'importo della bolletta telefonica bimestrale.

Il contratto con il provider può essere stipulato a tempo (ad esempio 100 ore), in fasce di orario (ad esempio dalle 17.00 alle 24.00) o senza limitazioni di tempo o orario; può dipendere dai servizi richiesti: *full-internet* (www, e-mail, news, chat, ftp, telnet, ecc.), controllo *antivirus* e *antispam* della casella postale, dimensione in Mbyte di quest'ultima, numero di caselle postali, invio di sms e di mms, ecc.; affitto dello spazio web sul server, in altre parole la produzione da parte nostra di pagine web, disponibili in internet, ma memorizzate nel server del provider.

La spesa dipende dallo spazio e dal tempo impegnato (ad esempio 100Mbyte per un anno).

Al giorno d'oggi, i maggiori introiti dei provider derivano dallo spazio web affittato alle imprese commerciali che pubblicizzano e commercializzano i loro prodotti sulla rete, dalla produzione delle stesse pagine web ed ai servizi di sicurezza.

Poiché i maggiori destinatari dei messaggi pubblicitari e delle informazioni in genere è l'utente privato, esiste la tendenza, già consolidata peraltro negli Stati Uniti e in alcuni Paesi Europei, a non far pagare all'utente privato il canone d'accesso alla rete.

I provider, inoltre, condividono con le compagnie telefoniche gli introiti derivanti dalle spese di collegamento telefonico per la connessione ad internet da parte degli utenti.

La seconda spesa è quella che si sostiene a beneficio del gestore telefonico.

Attualmente per l'utente privato sono possibili tre scelte:

1. connettersi alla rete telefonica commutata (RTC) poiché è la più economica;
2. connettersi ad ISDN, lievemente più costosa, ma decisamente più veloce (da 64Kbps a 128Kbps);
3. collegamento ad internet in ADSL.

La tipica tariffazione della RTC, salvo diverso contratto con gestori diversi di servizi telefonici, è a tempo ed è suddivisa in due fasce orarie:

- tariffa ordinaria dalle 08.00 alle 18.30;
- tariffa serale e notturna dalle 18.30 alle 08.00 del giorno successivo;

Per le domeniche e i giorni festivi vige una sola tariffa: quella festiva che coincide con quella serale e notturna. Essa va in vigore dalle ore 13.00 del sabato o del giorno prefestivo fino alle ore 08.00 del lunedì o del giorno post-festivo.

Il costo della telefonata dipende anche dal tipo di collegamento:

- urbano
- interurbano

L'elevato costo dell'uso del mezzo fisico di trasmissione dati ha frenato, in Italia, lo sviluppo di internet che, tuttavia, è cresciuto a ritmi vertiginosi.

Se si ha il collegamento ADSL l'utente paga il servizio secondo il contratto stipulato che può essere a tempo o fisso per una durata parziale durante la giornata o 24 ore su 24. Il collegamento ADSL non incide sulla bolletta telefonica convenzionale, anzi l'utente può usufruire del collegamento ad internet e nel contempo eseguire una telefonata convenzionale.

Per minimizzare le spese per il collegamento ad internet conviene:

1. rivolgersi ad un provider che, a parità di servizi, larghezza di banda e importo del contratto, risiede o ha un POP (Point Of Presence) nella nostra città;
2. effettuare i collegamenti nelle ore ricadenti nella fascia serale o durante le giornate festive e, comunque, nello ore di scarso traffico;
3. effettuare brevi e mirati collegamenti;
4. effettuare collegamenti con Paesi aventi fuso orario tale da ricevere le nostre chiamate durante le loro ore notturne.

A titolo d'esempio l'orario per effettuare il migliore collegamento con siti americani sotto il profilo della velocità e della spesa degli scatti telefonici è quello compreso tra le 07.00 e le 08.00 del mattino durante il quale è scarso il traffico telematico italiano mentre in america è notte.

3.2. Indirizzi Web utili di carattere elettronico

Si riportano di seguito alcuni indirizzi Web di carattere elettronico con l'avvertenza che alcuni di questi potrebbero, col tempo, essere modificati per cui non è garantito con certezza il *link* a tali siti.

http://www.intel.com	Intel (MP, adattatori di rete, ecc.)
http://www.microsoft.com	Microsoft
http://www.compaq.com	Compaq (computers, adattatori di rete)
http://www.3com.com	3Com (adattatori di rete, ecc.)
http://www.ti.com	Texas Instrument
http://www.national.com	National Semiconductor
http://www.moto.com	Motorola
http://www.philips.com	Philips
http://www.orcad.com	Orcad (Software circuiti elettronici)
http://www.protel.com	Protel (Software circuiti elettronici)
http://www.hp.com	Hewlett-Packard
http://www.hayes.com	Hayes (modem)

4. Linguaggio HTML

Col termine HTML (Hyper Text Markup Language) si intende un semplice linguaggio in grado di impartire dei comandi attraverso un sistema di etichettatura

(tagging scheme); esso rappresenta un sottoinsieme del più complesso linguaggio SGML (Structured Generalized Markup Language).

Un documento HTML è un file di testo in cui alcuni caratteri rappresentano dei comandi che consentono di strutturare a nostro piacimento il documento comprensivo di immagini e link.

Attualmente è in uso la versione 4.0; le versioni aggiornate introducono nuovi comandi e dichiarano obsoleti alcuni altri che continuano, comunque, a funzionare o a non funzionare per nulla a seconda del browser utilizzato.

I comandi che non funzionano vengono semplicemente ignorati.

La maggior parte dei comandi ha una etichetta (tag) iniziale che l'attiva e una etichetta finale che la disattiva.

Vi sono, inoltre, dei comandi che, per loro natura, non hanno bisogno del tag di disattivazione.

Un tag è compreso tra due parentesi angolari (i segni di minore e maggiore), ad esempio <H1> (formato di intestazione di dimensione 1, la più grande).

Un tag di disattivazione ha la stessa struttura del tag di attivazione ma inizia con la parentesi angolare aperta seguita dal segno di diviso, ad esempio </H1>.

La sintassi del tag può indifferentemente essere scritta in caratteri minuscoli o maiuscoli.

Una particolare caratteristica è la seguente: l'inserimento di due o più spazi tra parole in un documento HTML viene considerato come unico spazio e i ritorni a capo vengono ignorati. Esiste un apposito comando per l'inserimento di un ritorno a capo
 che significa "break".

Uno spazio vuoto supplementare è considerato un carattere speciale dal codice "nbsp"; un carattere speciale inizia con una "e commerciale" e termina con un "punto e virgola" per cui per ottenere uno spazio supplementare nel browser si deve inserire, in HTML, il codice: " ".

La struttura di un documento HTML è costituita da due parti: l'intestazione (header) e corpo (body).

Nell'intestazione si inseriscono delle informazioni di servizio e il titolo del documento che apparirà nella barra del titolo del browser. I due tag che identificano l'inizio e la fine dell'intestazione sono: <header> e </header>.

Nel body si scrive l'effettivo documento utilizzando i vari codici HTML. I due tag che identificano l'inizio e la fine del body sono: <body> e </body>.

Un documento HTML deve iniziare col tag <html> e terminare con </html>.

A titolo di esempio si scrive, in formato HTML, il codice per ottenere la schermata mostrata in fig.8 utilizzando un qualsiasi browser di pagine Web:

```
<html>
  <head>
    <title>Home Page</title>
  </head>

  <body>
    <p align="center"><b>Linguaggio HTML</b></p>
    <p>Col termine HTML (Hyper Text
    Markup Language) si intende un semplice linguaggio in grado di impartire dei
    comandi attraverso un sistema di etichettatura (tagging scheme); esso
    rappresenta un sottoinsieme del più complesso linguaggio SGML (Structured
    Generalized Markup Language).</p>
    <p>Un documento HTML è un file di testo in cui
    alcuni caratteri rappresentano dei comandi che consentono di strutturare a
    nostro piacimento il documento comprensivo di immagini e link.</p>
  </body>
</html>
```



Fig.8. – Visualizzazione del precedente documento HTML.

Commento:

```

<html> è il tag di apertura di un documento HTML;
<header> è il tag di apertura dell'intestazione;
<title> è il tag di apertura del titolo che va nell'intestazione;
</header> è il tag di chiusura dell'intestazione;
<body> è il tag di apertura del corpo del documento;
<p> è il tag di inizio paragrafo;
align="center" è l'attributo di allineamento centrato del paragrafo;
<b> è il tag del grassetto (bold);
</b> è il tag di chiusura del grassetto;
</p> è il tag di chiusura del paragrafo;
</body> è il tag di chiusura del body;
</html> è il tag di chiusura del codice HTML.
  
```

Un documento HTML può essere composto utilizzando un qualsiasi editor di testo come blocco note, wordpad di Windows, Word per DOS o per Windows, ecc., purché si salvi il documento in formato testo attribuendo un nome a piacere con estensione htm o html.

La funzionalità del codice html inserito, però, è a totale carico dell'utente che deve ricordare a memoria i vari tag e la relativa sintassi, pena la non corretta visualizzazione del documento quando si impiega un browser.

Esistono, tuttavia, numerosi programmi editori di documenti HTML funzionanti sotto Windows ed altri sistemi operativi che presentano una interfaccia grafica ed una struttura a menù che consentono di inserire velocemente i più importanti tag HTML semplicemente prelevandoli da opportune barre degli strumenti o dai menù.

Si elencano alcuni di questi programmi: Html editor, W3E, Hot dog, ecc.

Altri programmi, come Microsoft Front Page, Macromedia Dreamweaver, ecc. compongono pagine HTML senza dover scrivere neanche un tag.

È possibile l'inserimento di liste, tabelle, immagini, collegamenti e quant'altro prelevandoli dalle barre degli strumenti o dai menù. È, inoltre, possibile visualizzare il corrispondente codice html per poterlo, all'occorrenza, modificare manualmente al fine

di ottimizzare il documento sotto il profilo delle dimensioni del file o perché quel particolare tag non è previsto dal programma.

Attualmente, all'interno di pagine html, è possibile inserire codice di veri e propri linguaggi di programmazione eseguiti sul server (PHP, ASP) o sul client (JAVA, Javascript).

Si elencano di seguito, a beneficio dei programmatori di pagine Web, i fondamentali tag del formato HTML senza fornire un commento approfondito poiché l'argomento esula dagli obiettivi del testo.

GENERALI (tutti i documenti HTML dovrebbero contenere questi comandi)	
Tipo	<HTML></HTML> (inizio e fine del file)
Titolo	<TITLE></TITLE> (nome del documento; deve essere nella testata)
Testata	<HEAD></HEAD> (informazioni descrittive; come il titolo)
Corpo	<BODY></BODY> (contenuto della pagina)

DEFINIZIONE DI STRUTTURA (sostituire ? con un numero da 1 a 6)	
Intestazioni (Headings)	<H?></H?>; (sono definiti 6 livelli)
Allineamento	<H? ALIGN=LEFT CENTER RIGHT></H?>
Blocchi divisi	<DIV></DIV>
Allineamento	<DIV ALIGN=LEFT RIGHT CENTER JUSTIFY></DIV>
Codice	<CODE></CODE> (per listati di programmi)
Il font più grande	<BIG></BIG>
Il font più piccolo	<SMALL></SMALL>

FORMATTAZIONE DI PRESENTAZIONE (Modalità di visualizzazione del testo)	
Neretto (Bold)	
Corsivo (Italic)	<I></I>
Deponente	
Esponente	
Macchina da scrivere	<TT></TT> (visualizzato a spaziatura fissa)
Preformattato	<PRE></PRE> (visualizzato tale e quale)
Larghezza	<PRE WIDTH=?></PRE> (in caratteri)
Centrato	<CENTER></CENTER> (sia per testo che immagini)
Lampeggiante	<BLINK></BLINK> (Blinking)
Grandezza del Font	 (valori da 1 a 7)
Cambio grandezza font	
Grandezza font di base	<BASEFONT SIZE=?> (da 1 a 7; default 3)
Colore del Font	 (\$= valore esadecimale)

COLLEGAMENTI E GRAFICI	
Collegamento	
ad un punto(target)	 (in un altro documento)
	 (nello stesso documento)
ad una finestra	 (nello stesso documento)
Definizione del punto	
Visualizzazione immagine	
Allineamento	
Allineamento	
testo alternativo	 (quando non viene visualizzata l'immagine)
Mappa navigabile	 (richiede uno script)
Mappa navigabile locale	
Descrizione mappa	<MAP NAME="***";></MAP> (descrive la mappa)
Sezione mappa	<AREA SHAPE="RECT CIRCLE POLYGON" COORDS=",,,," HREF="URL" NOHREF>
Dimensioni	 (in pixel)
Bordi	 (in pixel)
Spazio circostante	 (in pixel)
Bassa risoluzione	

Metodo "Client Pull" <META HTTP-EQUIV="Refresh" CONTENT="?"; URL=URL">
 Incorpora oggetti <EMBED SRC="URL"> (inserimento oggetto nella pagina)
 Grandezza oggetti <EMBED SRC="URL" WIDTH="?" HEIGHT="?">

DIVISORI

Paragrafo <P> (di solito esegue un doppio ritorno a capo)
 Paragrafo <P></P> (ridefinito come comando pieno)
 Allineamento <P ALIGN=LEFT|CENTER|RIGHT></P>
 Interruzione riga
 (ritorno a capo singolo)
 Pulizia margini <BR CLEAR=LEFT|RIGHT|ALL>
 Riga orizzontale <HR>
 Allineamento <HR ALIGN=LEFT|RIGHT|CENTER>
 Spessore <HR SIZE=?> (in pixel)
 Larghezza <HR WIDTH=?> (in pixel)
 Larghezza in % <HR WIDTH=%> percentuale della larghezza di pagina
 Riga piena <HR NOSHADE> (senza l'effetto 3D)

SFONDO E COLORI (\$ = Valore esadecimale)

Immagine di sfondo <BODY BACKGROUND="URL">
 Colore di sfondo <BODY BGCOLOR="#\$\$\$\$\$\$"> (RGB)
 Colore del testo <BODY TEXT="#\$\$\$\$\$\$">
 Colore dei collegamenti <BODY LINK="#\$\$\$\$\$\$">
 Colore dei collegamenti visitati <BODY VLINK="#\$\$\$\$\$\$">
 colore del collegamento in corso <BODY ALINK="#\$\$\$\$\$\$">

LISTE (le liste possono essere annidate)

Liste senza ordine (prima di ogni elemento)
 Tipo di bullet <UL TYPE=DISC|CIRCLE|SQUARE> (per tutta la lista)
 <LI TYPE=DISC|CIRCLE|SQUARE> (questo e successivi)
 Liste numerate (prima di ogni elemento)
 Tipo di numero <OL TYPE=A|a|I|i|1> (per tutta la lista)
 <LI TYPE=A|a|I|i|1> (questo e successivi)
 Numero di partenza <OL VALUE=?> (per tutta la lista)
 <LI VALUE=?> (questo e successivi)
 Lista di definizioni <DL><DT><DD></DL> (<DT>=termine, <DD>=definizione)
 Lista tipo Menu <MENU></MENU> (prima di ogni elemento)
 Lista tipo Directory <DIR></DIR> (prima di ogni elemento)

CARATTERI SPECIALI (devono essere digitati in minuscolo)

Carattere speciale (il numero dopo &# indica il codice ISO 8859-1)

<	<
>	>
&	&
"	"
Registered TM	®
Registered TM	®
Copyright	©
Copyright	©
à	à
é	é
è	è
ì	ì
ò	ò
ù	ù

MODULI (generalmente richiedono uno script sul server)

Definizione <FORM ACTION="URL" METHOD=GET|POST></FORM>
 Upload di file <FORM ENCTYPE="multipart/form-data"></FORM>
 Campo di immissione <INPUT TYPE="TEXT|PASSWORD|CHECKBOX|RADIO|

Nome del campo	<INPUT NAME="***">	IMAGE HIDDEN SUBMIT RESET">
Valore del campo	<INPUT VALUE="***">	
Barrato?	<INPUT CHECKED>	(checkbox e radio)
Grandezza	<INPUT SIZE=?>	(in caratteri)
Lunghezza massima	<INPUT MAXLENGTH=?>	(in caratteri)
Lista di selezione	<SELECT></SELECT>	
Nome del campo	<SELECT NAME="***"></SELECT>	
Numero di opzioni	<SELECT SIZE=?></SELECT>	
Scelta multipla	<SELECT MULTIPLE>	(per selezionare più di 1 elemento)
Opzioni	<OPTION>	(Elementi che possono essere selezionati)
Opzione proposta	<OPTION SELECTED>	
Finestra di immissione	<TEXTAREA ROWS=? COLS=?></TEXTAREA>	
Nome del campo	<TEXTAREA NAME="***"></TEXTAREA>	
Divisione del testo	<TEXTAREA WRAP=OFF VIRTUAL PHYSICAL></TEXTAREA>	

TABELLE		
Definizione tabella	<TABLE></TABLE>	
Bordo	<TABLE BORDER></TABLE>	(per visualizzare il bordo)
Table Border	<TABLE BORDER=?></TABLE>	(per indicare lo spessore)
Spazio tra celle	<TABLE CELLSPACING=?>	
Spazio all'interno	<TABLE CELLPADDING=?>	
Larghezza desiderata	<TABLE WIDTH=?>	(in pixel)
Larghezza in %	<TABLE WIDTH=%>	(percentuale della pagina)
Riga	<TR></TR>	
Allineamento	<TR ALIGN=LEFT RIGHT CENTER VALIGN=TOP MIDDLE BOTTOM>	
Cella	<TD></TD>	(deve essere all'interno di una riga)
Allineamento	<TD ALIGN=LEFT RIGHT CENTER VALIGN=TOP MIDDLE BOTTOM>	
Senza interruzione	<TD NOWRAP>	
Colonne da occupare	<TD COLSPAN=?>	
Righe da occupare	<TD ROWSPAN=?>	
Larghezza desiderata	<TD WIDTH=?>	(in pixel)
Largh.desiderata in %	<TD WIDTH=%>	(percentuale della tabella)
Intestazione	<TH></TH>	(come <TD>, ma in neretto e centrata)
Allineamento	<TH ALIGN=LEFT RIGHT CENTER VALIGN=TOP MIDDLE BOTTOM>	
Senza interruzione	<TH NOWRAP>	
Colonne da occupare	<TH COLSPAN=?>	
Righe da occupare	<TH ROWSPAN=?>	
Larghezza desiderata	<TH WIDTH=?>	(in pixel)
Largh.desiderata in %	<TH WIDTH=%>	(percentuale della tabella)
Legenda della tabella	<CAPTION></CAPTION>	
Allineamento	<CAPTION ALIGN=TOP BOTTOM>	(sopra o sotto la tabella)

FRAME (definizione e gestione di specifiche parti dello schermo)		
Documento	FRAME <FRAMESET></FRAMESET>	(al posto di <BODY>)
Altezza in righe	<FRAMESET ROWS=,,,></FRAMESET>	(pixel o %)
Altezza in righe	<FRAMESET ROWS=*></FRAMESET>	(* = misura relativa)
Larghezza in colonne	<FRAMESET COLS=,,,></FRAMESET>	(pixel o %)
larghezza in colonne	<FRAMESET COLS=*></FRAMESET>	(* = misura relativa)
Defizione	<FRAME>	(contenuto di ogni singolo quadro)
Visualizza documento	<FRAME SRC="URL">	
Nome del frame	<FRAME NAME="***" _blank _self _parent _top>	
Larghezza	<FRAME MARGINWIDTH=?>	(margine destro e sinistro)
Altezza margine	<FRAME MARGINHEIGHT=?>	(margine alto e basso)
Barra di scorrimento?	<FRAME SCROLLING="YES NO AUTO">	
Misure non modificabili	<FRAME NORESIZE>	
Contenuto in assenza di frame	<NOFRAMES></NOFRAMES>	(per i browser che non supportano FRAME)

Al giorno d'oggi le pagine web che si sfogliano col browser non contengono solo codice HTML.

Per arricchire i documenti con altre funzionalità multimediali, stilistiche e di maggior interazione, si utilizzano veri e propri linguaggi di programmazione che eseguono dei codici specifici.

Alcuni di questi linguaggi, ad esempio JAVA o Javascript, risiedono nel browser ed in tal caso il programma da eseguire è inserito nel file HTML.

Altri linguaggi specifici, ad esempio PHP e ASP, risiedono nel server per cui la pagina web trasferita sul browser è il risultato dell'elaborazione avvenuta sul server.

Le applicazioni scritte in Java, ad esempio, importabili via internet ed eseguibili dai browser, sono note come *applets* (applicazioncine); queste sono dei veri e propri programmi che si possono lanciare e con i quali è possibile interagire.

Si realizzano applicazioni in Java per ottenere testi ed immagini in animazione, videogiochi interattivi, programmi per l'insegnamento della fisica, chimica, meccanica, elettrotecnica, elettronica, matematica, medicina, ecc.

L'utente può inserire dei valori da tastiera o attivare degli eventi con il mouse e l'applicazione si adegua ai valori introdotti.

Si riportano alcuni indirizzi dei siti Web da cui prelevare informazioni ed applets in linguaggio Java: <http://java.sun.com> <http://www.gamelan.com>

5. Sicurezza informatica

La sicurezza dei sistemi informatici è un problema che riguarda sia gli aspetti hardware che software di computer singoli, in rete locale e collegati ad internet.

I problemi hardware sono collegati ai guasti delle parti fisiche del computer come, ad esempio, l'hard-disk, la memoria centrale, la scheda madre, la scheda grafica, ecc.

I problemi software sono quelli dovuti ai malfunzionamenti per incompatibilità con altri software installati, presenza di virus, cancellazione involontaria di programmi.

Quando uno o più computer sono collegati ad internet o in rete locale uno dei problemi più sentiti riguarda l'accesso ai dati da parte di utenti non autorizzati.

La sicurezza informatica ha, come obiettivo principale, quello di garantire un adeguato grado di protezione dei beni, cioè dell'hardware, del software e dei dati, mediante l'attuazione di un progetto di sicurezza globale che, partendo dalla definizione di una politica di sicurezza, tenga conto di tutti gli aspetti del problema e giunga ad un livello di protezione, informatico ed organizzativo, che possa essere controllato nel tempo.

Occorre, pertanto, garantire che il bene mantenga inalterate nel tempo queste proprietà:

- Sicurezza/riservatezza (Confidentiality);
- Integrità (Integrity);
- Disponibilità (Availability);
- Autenticazione;
- Non ripudio.

5.1. Sicurezza di un computer

La sicurezza di un singolo computer è legata alla capacità di un PC di funzionare correttamente senza guasti hardware né problemi nel software.

I dati importanti subiscono periodicamente un processo di backup (duplicazione del salvataggio) che l'utente sceglie fra i tanti disponibili.

5.1.1. Guasti hardware

Uno dei più gravi guasti hardware è la rottura dell'hard-disk. Su di esso, come è noto, risiedono, programmi, documenti e dati dell'azienda, del personale, dei clienti, ecc.

Se l'attività deve funzionare continuamente, come nella produzione di un articolo, in una banca o in un supermercato, anche in presenza di guasto dell'hard-disk, si deve prevedere un sistema in cui i dati sono registrati su due hard-disk: il primo è quello correntemente utilizzato, il secondo è l'esatta replica del primo. In caso di guasto di una delle due memorie di massa, va in funzione automaticamente l'altra.

5.1.2. Calamità naturali

Per evitare che le calamità naturali come terremoti, alluvioni, esplosioni per perdita di gas, incendi, possano minare il funzionamento delle apparecchiature, si ricorre a varie soluzioni come edifici costruiti con norme antisismiche, pavimento sopraelevato, sensori di fumi e di gas collegati a sistemi di teleallarmi.

In caso di black-out elettrico entrano in funzione i gruppi di continuità (UPS *Uninterruptible Power Supply*) che assicurano una certa autonomia di funzionamento per un tempo sufficiente a salvare i dati transitori ed a chiudere correttamente le varie applicazioni software.

Se si teme che il computer, comunque, possa subire danni si deve prevedere un backup periodico di tutti i dati ed un backup giornaliero dei dati più importanti.

La successiva operazione di ripristino dei dati (restore) sulla macchina riparata o su un'altra su cui è montato lo stesso software consentirà di recuperare i dati persi fino al momento dell'ultimo backup.

Vi sono varie tecniche di backup: duplicazioni di un hard-disk su un secondo hard-disk (mirroring); uso di nastri magnetici e software in grado di eseguire il backup incrementale (ogni giorno vengono aggiunti sul nastro i nuovi dati o le modifiche dei dati precedenti); masterizzazione di uno o più CD-ROM o DVD meglio se riscrivibili.

5.1.3. Virus

Programmi o documenti non controllati possono contenere virus che rappresentano una minaccia per il funzionamento del computer.

Un virus è un programma realizzato con lo scopo di deteriorare, modificare o addirittura impedire il funzionamento di uno o più programmi, anche del sistema operativo. Alcuni virus sono dei file che si autoriproducono occupando spazio che di norma è impegnato da dati e programmi.

Un virus appartiene alla famiglia dei *Malicious Software* (malware) che si diffondono da computer a computer per provocare danni ai sistemi.

I virus si possono classificare in base a diverse caratteristiche, tra cui la più significativa è l'ambiente attraverso cui si propaga l'infezione e si sviluppa il virus:

- i *boot virus*, che infettano il Boot Sector o il Master Boot Record dei dischi in modo da essere caricati all'avvio del sistema;
- i *file virus*, che infettano, con varie modalità, i file eseguibili e utilizzano lo scambio di questi ultimi per propagare l'infezione;

- i *macrovirus*, che sono realizzati in VBA (Visual Basic for Application), presenti nei documenti degli applicativi di Office;
- i *network virus*, che si diffondono sfruttando le vulnerabilità dei protocolli di internet.

Per evitare problemi causati dai virus si installa nel computer un programma antivirus col compito di individuare e distruggere virus residenti nella memoria centrale o nell'hard-disk. Un altro compito dell'antivirus è quello dello scudo (shield) come prevenzione: se un virus sta per transitare nel sistema attraverso un documento o un programma residente su dischetto, CD-ROM, rete locale, internet, ecc. l'antivirus se ne accorge e chiede all'utente quale operazione intraprendere: può impedirne l'accesso o, se può, debella il virus "guarendo" il file incriminato, cancella il file, ecc.

In realtà non sempre l'antivirus è in grado di riconoscere la presenza di un virus.

Occorre, quindi, dotarsi di un serio programma antivirus ampiamente collaudato e, soprattutto, occorre aggiornare periodicamente il database dei virus conosciuti perché, come è noto, ogni giorno ne vengono creati di nuovi.

5.1.4. Errori degli utenti

Errori banali, alle volte, commessi da utenti o da programmatori, possono produrre dei veri e propri disastri.

La cancellazione definitiva accidentale di file vitali o di intere cartelle è senza dubbio uno degli errori più banali e più frequenti.

Si ricordi che la cancellazione di file non corrisponde alla smagnetizzazione ma nella cancellazione di un riferimento nella FAT (File Allocation Table = Tabella di Allocazione dei File): i settori impegnati dal file cancellato sono ora disponibili per la sovrascrittura di un altro file.

Esistono in commercio degli appositi programmi in grado di recuperare i dati che si ritengono cancellati definitivamente. Questi programmi eseguono una operazione di *undelete* che, come si intuisce dal termine, permette di "resuscitare" i dati cancellati.

La procedura di recupero ha un elevato tasso di successo purché avvenga immediatamente dopo la cancellazione accidentale. Infatti, se dopo l'errore commesso si effettuano operazioni che costringono l'hard-disk alla scrittura, ciò può verosimilmente avvenire negli stessi settori del file cancellato.

5.2. Sicurezza nelle reti di computer

Oltre ai problemi prima citati che possono affliggere un PC vi sono altri problemi che si aggiungono quando il computer è collegato in una rete locale o ad internet.

5.2.1. Hacker

Un hacker è un programmatore particolarmente esperto delle problematiche di rete che riesce, con stratagemmi, tecniche particolari ed opportuni software, ad introdursi in una rete locale o in un PC collegato ad internet senza avere l'autorizzazione all'accesso.

Spesso il controllo dell'accesso è protetto da password. L'inserimento di password banali e prevedibili, come la data di nascita o il proprio nome di battesimo, è causa di accessi frequenti da parte di hacker che possono, violando la privacy, visualizzare i file residenti sull'hard disk, modificandoli o cancellandoli provocando, di conseguenza, grave danno.

Occorre precisare, tuttavia, che non tutti gli hacker hanno comportamenti illegali e dannosi; alle volte forniscono consulenze per aumentare la protezione di un sistema informatico o per risolvere qualche problema causato da “colleghi” malintenzionati.

5.2.2. Trojan, spyware

Un cavallo di Troia è un programma apparentemente innocuo che effettua operazioni diverse e dannose da quelle previste dall'utente.

Un esempio di cavallo di troia molto semplice è la creazione di una finestra di *login* identica a quella del sistema ma finta, che invia *password* e altre informazioni riservate all'autore del *software* doloso.

Spesso quando un sistema viene compromesso l'intruso inserisce cavalli di troia con lo scopo di mascherare l'attacco, procurarsi informazioni aggiuntive e creare un accesso (*backdoor* = *porta di servizio*) da sfruttare successivamente.

Gli spyware sono piccoli programmi che spiano i dati che riguardano l'utente; possono entrare nel computer attraverso l'installazione di programmi gratuiti se accettiamo di visualizzare banners pubblicitari (*adware*).

All'installazione di questi programmi seguono alcuni comportamenti molto strani del computer: pop-up pubblicitari che si aprono apparentemente senza motivo, rallentamenti del browser e del sistema operativo, comparsa di file e cartelle mai visti prima.

I dati che vengono raccolti possono riguardare la nostra e-mail, i prodotti acquistati con la carta di credito, i siti che visitiamo più spesso, tutte le nostre abitudini di navigazione.

Queste informazioni vengono trasmesse a chi ha creato lo spyware che potrà rivenderle ad aziende interessate per ricerche di mercato oppure per inviarci *spam*, ovvero la pubblicità non desiderata.

5.2.3. Sniffing, Spoofing e DoS

Si intende per *Sniffing* il comportamento di un malintenzionato che si inserisce in una tratta che collega due PC di una rete locale o di internet con lo scopo di intercettare le informazioni relative all'autenticazione dell'utente.



Fig.9. – Schema di principio dello sniffing.

Per questo motivo le password, il numero di carta di credito ed altre informazioni riservate non devono essere trasmesse in chiaro ma devono subire un processo di codifica detta crittografia.

Lo sniffing viene realizzato con appositi software che tentano di convertire i pacchetti in transito in forma leggibile concentrando il proprio interesse all'intercettazione di userid e password.

Lo *Spoofing* ha come obiettivo la sostituzione. Vi sono vari tipi di spoofing:

- *user account spoofing* quando avviene la sostituzione di un utente senza averne diritto, ovvero se si utilizza una qualche forma di abuso dell'identità elettronica;
- *data spoofing* quando si prende il controllo di un canale di comunicazione e si modificano i contenuti dei pacchetti in transito;

- *IP spoofing* quando si manipola l'indirizzo IP da cui parte una certa connessione in modo da far credere di essere un sistema sorgente differente.

Tra questi tipi di attacchi, l'*IP spoofing* è il più noto e diffuso, e ha come obiettivo quello di aggirare i principali controlli attivi effettuati per garantire la sicurezza, che sono basati sul monitoraggio dei numeri IP.

Il DoS (*Denial of Service* = Negazione del servizio) è un tipo di attacco che ha lo scopo di impedire l'accesso alle informazioni di un computer anche se autorizzato.

Due forme molto semplici e diffuse di Denial of Service sono:

- il *mail bombing*, che è realizzato inviando a un utente una quantità di posta sufficiente a riempire lo spazio disponibile e dunque bloccare il suo servizio di ricezione.
- la *bandwidth consumption*, che consiste nel generare una quantità elevatissima di traffico verso una certa destinazione, occupando tutta la larghezza di banda disponibile ed impedendo così ad altri di usufruire dei servizi messi a disposizione.

5.3. Sistemi di sicurezza

I sistemi di sicurezza per la protezione dei dati importanti in transito e per l'integrità dei PC della rete locale si basano sulle seguenti soluzioni:

- la *crittografia* che permette di far transitare sulla rete messaggi cifrati nascondendo il contenuto e offre, inoltre, supporto di base alla certificazione e alla firma digitale;
- *gli antivirus* che consentono l'intercettazione e la rimozione dei virus;
- *i firewall* che sono dei programmi in grado di creare una barriera difensiva perimetrale, ovvero di rendere più difficili gli attacchi ai sistemi di una LAN prevenendo gli accessi non autorizzati.

5.3.1. Crittografia

Quando si eseguono delle transazioni, i siti commerciali richiedono informazioni riservate come il numero di carta di credito; quando si scarica la posta elettronica utilizzando il browser web tipo Internet Explorer, si inserisce, insieme alla "user-id", la password che verrà trasmessa in chiaro.

Queste informazioni, per raggiungere la destinazione, transitano di nodo in nodo.

Un malintenzionato collegato ad uno di questi nodi può, con l'uso di particolari software di rete, intercettare le nostre informazioni e può, se vuole, arrecarci danno.

Una soluzione per impedire la leggibilità è quella di crittografare il messaggio.

In pratica si utilizza un codice che, agendo, sul messaggio, ne genera un altro assolutamente incomprensibile. Il vero destinatario è in possesso dello stesso codice per cui, attraverso un procedimento inverso, può risalire al messaggio originale.

Per evitare che il malintenzionato, venuto in possesso del codice che si sta utilizzando, possa decodificare il messaggio, si utilizzano, di volta in volta, codici diversi con metodiche differenti che il trasmettitore ed il ricevitore hanno precedentemente concordato.

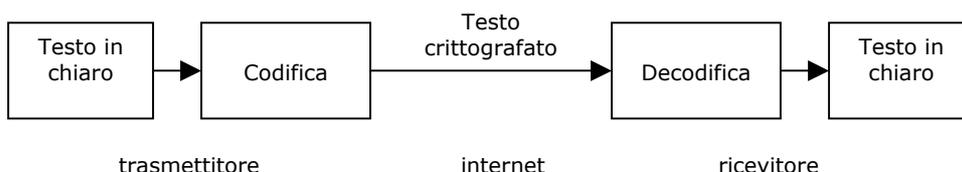


Fig.10. – Schema di principio della crittografia.

La codifica può essere una legge matematica che applicata su un carattere delle parole di un messaggio, ne genera un altro.

Ad esempio se si decide di trasmettere al posto di un dato carattere quello successivo in ordine alfabetico crescente, si ha che la lettera “a” è sostituita da “b”, la “b” da “c” e così via.

La parola “elettronica” diventa “fmfuuspojdb”.

Una variante è la codifica con la lettera precedente o con una lettera che dista da quella data di n posizioni in avanti o indietro. È necessario che il ricevitore conosca tale legge (algoritmo crittografico).

Gli esempi menzionati sono molto banali in quanto un qualsiasi software che tenta la decodifica riesce abbastanza presto a risalire alla legge applicata e quindi alla decodifica del messaggio.

Un'altra tecnica più convincente si basa sull'uso di una parola binaria abbastanza lunga (*chiave*) che, insieme ad un algoritmo crittografico, concorre alla codifica del messaggio.

Il malintenzionato, per risalire all'informazione in chiaro, deve scoprire sia l'algoritmo crittografico e, soprattutto, deve “inventarsi” la chiave, nota solo al mittente ed al destinatario del messaggio.

5.3.2. Crittografia a chiave simmetrica e asimmetrica

Un sistema crittografico si dice a *chiave simmetrica* se questa è la stessa sia per codificare che per decodificare il messaggio. In altre parole la chiave che il mittente utilizza per crittografare il messaggio è la stessa usata dal destinatario per il decriptaggio.

La chiave si dice *privata* poiché è nota solo al mittente e al destinatario del messaggio.

La difficoltà cui va incontro il malintenzionato aumenta esponenzialmente all'aumentare del numero di bit che costituiscono la chiave.

Con 64 bit, ad esempio, si hanno 2^{64} combinazioni binarie: il numero di tentativi, prima di approdare eventualmente alla soluzione del caso, è enormemente elevato e richiederebbe anni di continua elaborazione da parte del PC che si cimenta alla decodifica.

Una chiave a 128 bit è ritenuta molto sicura. Un punto delicato di tutto il meccanismo è la trasmissione della chiave tra i due interlocutori: se il malintenzionato intercetta la chiave durante tale trasmissione, è in grado di decodificare facilmente i successivi messaggi.

Per rendere sicura la distribuzione delle chiavi è stata messa a punto la tecnica della crittografia a *chiave asimmetrica*.

Il nome deriva dal fatto che si utilizzano due chiavi diverse:

- *chiave pubblica* per l'operazione di codifica;
- *chiave privata* per l'operazione di decodifica.

Per chiave pubblica si intende una sequenza di caratteri, di lunghezza arbitraria, utilizzata in coppia con la chiave privata nella crittografia a chiave pubblica. Deve essere resa pubblica.

Per chiave privata, invece, si intende una sequenza di caratteri, di lunghezza arbitraria, utilizzata in coppia con la chiave pubblica nella crittografia a chiave pubblica. Deve essere conosciuta solo dal proprietario.

Ciascun utente deve quindi possedere due chiavi, una privata che conosce solo lui e una pubblica che rende nota a tutti.

Esiste ovviamente una correlazione matematica tra chiave pubblica e chiave privata che deve rendere semplice calcolare la chiave pubblica a partire da quella privata ed estremamente impegnativo calcolare la chiave privata a partire da quella pubblica.

La sicurezza di un algoritmo asimmetrico risiede proprio nella difficoltà a individuare la chiave privata quando si è in possesso di quella pubblica.

Facendo riferimento alla fig.11, se A vuole inviare un messaggio riservato a B, deve possedere la chiave pubblica di B (che è disponibile a tutti) e utilizzarla per criptare il messaggio. B sarà l'unico a riuscire a decrittare il messaggio poiché è l'unico in possesso della chiave privata.

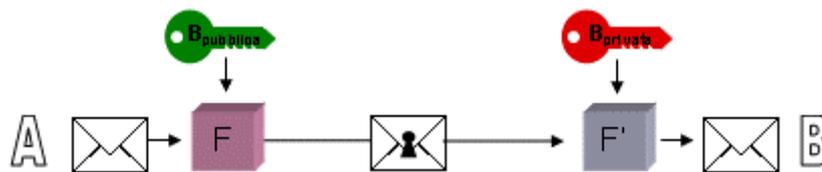


Fig. 11. – Schema della trasmissione di un messaggio con sistema crittografico a chiave asimmetrica.

Un software molto noto per la crittografia a chiave asimmetrica è **PGP** (Pretty Good Privacy).

Fra i vari algoritmi crittografici a chiave asimmetrica si ricorda **RSA** (acronimo dei cognomi degli ideatori: Rivest, Shamir, Adleman).

Con l'algoritmo RSA si genera la chiave pubblica, da fornire a tutti, costituita da una coppia di numeri (p,n) e la chiave privata, da custodire gelosamente, costituita dalla coppia (q,n).

Il metodo consiste nel codificare il messaggio M in chiaro, costituito da un blocco di caratteri, utilizzando la chiave pubblica in modo da generare il messaggio cifrato C utilizzando la funzione:

$$C = M^p \bmod n$$

La funzione C, in pratica, è il resto della divisione tra M^p ed n.

Il ricevitore decodifica il messaggio cifrato C ricevuto e genera il messaggio in chiaro M con la seguente funzione:

$$M = C^q \bmod n$$

La funzione M, in pratica, è il resto della divisione tra C^q ed n.

Affinché si ottenga il corretto messaggio M, ovviamente, p e q devono essere opportunamente correlati tra di loro.

Tralasciando la dimostrazione che porta alla corretta decodifica, ci limitiamo a dire che la chiave pubblica (p,n) e privata (q,n) si determinano a partire da due numeri primi molto grandi costituiti da centinaia di cifre.

5.3.3. Firma digitale

La firma digitale è una tecnica che ha lo scopo di assicurare l'autenticazione e l'integrità dei documenti elettronici.

Per autenticazione si intende la certezza dell'identità di un utente.

Per integrità dei documenti si intende la certezza che il documento ricevuto non ha subito alcuna modifica rispetto a quello che ci si aspettava di ricevere.

La firma digitale si ottiene con la tecnica della crittografia a chiave asimmetrica scambiando i ruoli delle chiavi pubblica e privata, cioè la persona che firma un documento usa la sua chiave privata e il destinatario che vuole assicurarsi dell'autenticità utilizza la chiave pubblica.

Dal documento che si intende trasmettere si ricava, con opportune tecniche, un sottoinsieme di caratteri di lunghezza fissa pari a 128 o 160 caratteri che prende il nome di *impronta*.

Due documenti diversi danno origine a due impronte diverse grazie all'utilizzo di una particolare funzione, detta *funzione di hash*.

La firma digitale è il risultato della codifica dell'impronta con la chiave privata.

Il ricevitore, per controllare l'identità del mittente e l'integrità del documento, utilizza la funzione di hash che applica al testo in chiaro ricevuto insieme alla firma digitale per calcolare l'impronta. Successivamente applica la chiave pubblica alla firma digitale per determinare l'impronta: se questa coincide con quella determinata dal messaggio si ha la conferma dell'identità del mittente e l'originalità del documento ricevuto.

Se il mittente apporta una modifica al documento, anche la nuova firma digitale risulterà diversa.

La Pubblica Amministrazione incomincia ad utilizzare la firma digitale nei documenti elettronici sia per il riconoscimento del mittente sia per la garanzia dell'autenticità del documento.

Il documento con firma digitale assume lo stesso significato di un documento cartaceo firmato.

In quest'ultimo caso la firma sul foglio garantisce le generalità del mittente e l'autenticità del documento.

5.3.4. Firewall, antivirus, antispyware, wardriving

Per difendersi dagli attacchi di malintenzionati, sempre in agguato sulla rete, si possono utilizzare programmi firewall (muro di fuoco), antivirus e antispyware.

Un *firewall* è un programma che consente di controllare il traffico in uscita ed in entrata nel singolo computer (personal firewall) e nell'intera rete locale (network firewall).

Nel caso di un network firewall è possibile condividere con altri computer il collegamento ad internet sia di tipo dial-up che ADSL, wireless o satellitare.

Per la condivisione si può utilizzare il NAT (Network Address Translation) o il Proxy Server.

Con un programma firewall si definiscono le politiche di sicurezza individuando le applicazioni o i protocolli che possono avere accesso ad internet. Le impostazioni predefinite possono essere modificate manualmente consentendo o proibendo a determinate applicazioni l'accesso ad internet specificando, anche, l'intervallo degli indirizzi IP locali che hanno l'accesso o meno.

È possibile, inoltre, filtrare i siti bloccando le pagine con banner o script o che contengano termini proibiti e impedendo il collegamento P2P (Peer to Peer).

Un firewall è in grado di bloccare i tentativi di intrusione comunicando tutti gli interventi effettuati. Se l'accesso al computer da parte di un utente remoto è un evento che desideriamo accettare (software didattico in una rete, gestione, manutenzione ed amministrazione remota, ecc.) è possibile consentire selettivamente il permesso d'accesso oppure è possibile abbassare il livello di protezione.

Programmi firewall molto noti sono ZoneAlarm e Kerio.

I programmi *antivirus* intercettano il transito di un virus, se riconosciuto, che tenta di entrare nel nostro computer attraverso CD, dischetti e, soprattutto, internet.

In genere l'antivirus, oltre al riconoscimento, è in grado di eliminare il virus.

La classificazione dei virus e le principali azioni svolte dagli antivirus sono stati descritti nel precedente paragrafo 5.1.3.

Gli antivirus più noti sono McAfee VirusScan, Norton AntiVirus (NAV), AntiVirus Grisoft (AVG), ecc.

Alcuni di questi, in versione ridotta, sono gratuiti.

Alcuni antivirus in versione completa detengono anche le funzioni di firewall e antispyware.

Uno *spyware*, come si è detto nel paragrafo 5.2.2. è un programma di piccole dimensioni il cui unico scopo è spiare e raccogliere informazioni contenute nel PC.

In alcuni casi gli utenti non sono informati dell'installazione di questi "programmi aggiuntivi" che rimangono anche dopo la disinstallazione dell'applicazione adware.

Esistono specifici software denominati "lavasoftware" o antispyware che hanno lo scopo di esaminare l'intero computer alla caccia delle applicazioni spyware da eliminare.

La funzione di messa in quarantena trasferisce il sospetto spyware in una zona sotto il controllo dell'antispyware consentendo di ripristinare il file eliminato qualora ci si accorge che l'antispyware ha preso un abbaglio, cioè ha considerato spyware un file innocuo di nostro interesse. Questa necessità, per fortuna, si manifesta con scarsa frequenza.

Gli antispyware più noti sono Ad-Aware della Lavasoft Sweden, Spybot - Search & Destroy, Spyware Stormer, ecc.

Anche gli antispyware sono disponibili in versione free dalle prestazioni ridotte rispetto a quelle a pagamento.

Per *wardriving* si intende una tecnica volta ad intercettare una rete wireless attraverso l'uso di un PC portatile dotato di adattatore wireless con lo scopo di accedere ai dati della rete locale o di sfruttare gratuitamente l'accesso ad Internet.

La tecnica consiste nell'utilizzo di potenti antenne direttive che consentono di intercettare la rete mantenendosi a sufficiente distanza onde non farsi scoprire e registrare le coordinate spaziali utilizzando un sistema GPS.

Per evitare gli effetti di queste illecite manovre da parte di malintenzionati è necessario proteggere a dovere la propria rete.

Il malintenzionato può configurare il suo adattatore wireless in modo da rilevare passivamente il traffico dati delle altre reti wireless senza inviare nulla di suo.

Un'altra tecnica consiste nel provocare dei disturbi elettromagnetici con particolari apparecchiature dette *Jammer*. In presenza di trasmissione disturbata la comunicazione è dirottata su un altro Access Point che potrebbe essere simulato da un software montato sul portatile del malintenzionato.

Il dirottamento su un altro Access Point può avvenire anche provocando un intasamento di dati (tecnica DoS = Denial of Service) sull'Access Point della rete wireless.

I malintenzionati esperti dotati di opportuni software sono in grado di leggere facilmente l'identificativo SSID dell'Access Point, sono in grado di sfruttare il punto debole del sistema di crittografia WEP (parte della chiave segreta viaggia in chiaro in un pacchetto), possono modificare il MAC address del proprio adattatore wireless in modo da essere riconosciuto dall'Access Point come appartenente alla rete.

Per minimizzare il rischio di essere intercettati è bene controllare che l'Access Point propaghi le onde radio fuori dall'edificio con intensità nulla o trascurabile e cambiare frequentemente le chiavi condivise del sistema crittografico per rendere inutilizzabili quelle precedentemente trafugate dal malintenzionato.

6. Trattamento dei dati personali

Per privacy si intende il diritto alla protezione dei dati personali. Erroneamente qualcuno crede che la privacy sia il diritto all'anonimato.

Il provvedimento che disciplina il trattamento dei dati personali è il Decreto legislativo 30 giugno 2003, n.196 costituito da 186 articoli per un totale di oltre 50 pagine, che sostituisce la legge 675 del 1996.

L'articolo 1, appunto, recita: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano".

L'articolo 4, che di seguito si riporta, fornisce le definizioni dei termini usati in ambito al trattamento dei dati personali e consta di 4 commi.

Art.4 – Definizioni

1. Ai fini del presente codice si intende per:

- a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
- d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

- l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

- a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- b) "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- c) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- d) "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- f) "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

- a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

- e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- f) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- g) "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

- a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

6.1. Anonimato in rete

Senza particolari accorgimenti, sul web non esiste alcuna privacy: l'intero traffico dati è registrato in file conservati sui server.

Collegandosi al sito www.notrace.it/spy.asp è possibile rendersi conto di ciò: si possono avere informazioni da dove ci stiamo collegando, con quale computer, quale sistema operativo e molto altro ancora.

Questa problematica è legata agli spyware ed allo sniffing che minano la privacy e la sicurezza del proprio computer o della rete locale.

Ogni PC collegato ad internet, come è noto, possiede un indirizzo IP a 32 bit che lascia traccia del passaggio e delle operazioni ovunque, a meno che non lo si "nasconde" adeguatamente.

Chiunque, leggendo l'indirizzo IP, può risalire al computer dal quale ci stiamo collegando senza troppi problemi.

L'anonimato in rete è quindi legato all'abilità di "mascherare" il nostro indirizzo IP.

Una soluzione che garantisca l'anonimato durante la navigazione è l'utilizzo di proxy server gratuiti o a pagamento disponibili in rete. I server proxy filtrano l'indirizzo IP inserendo al loro posto quello del server.

Per assicurare l'anonimato delle e-mail si utilizzano particolari server denominati "remailer anonimi".

Un remailer anonimo è un servizio e-mail configurato in modo da eliminare ogni traccia riguardante il mittente del messaggio.

A differenza della maggior parte dei server e-mail, un remailer non mantiene nessun tipo di registro (file log), né aggiunge informazioni per il tracciamento del messaggio, assicurandosi che ogni messaggio in uscita sia privo di ogni tipo di informazione utile al rintracciamento del mittente. L'unica traccia è l'indirizzo IP del computer del remailer.

I remailer proteggono la privacy e la libertà di parola in rete, visto che esistono svariati strumenti di controllo, da quelli di marketing a quelli militari.

I messaggi di posta, tuttavia, viaggiando in chiaro, potrebbero consentire ai malintenzionati di risalire al mittente. Per questo motivo, oltre all'uso dei remailer anonimi, è necessario crittografare anche il messaggio utilizzando, ad esempio, il programma PGP.

Anche il "file sharing" (scambio di file tra utenti secondo la filosofia client-client e non client-server) può essere anonimo grazie all'impiego di specifici software in grado di non mostrare agli utenti il nome e l'indirizzo IP di colui che condivide file sulla rete, sia programmi che musica mp3 o video.

7. Diritti d'autore

Con l'avvento delle nuove tecnologie è divenuto facile duplicare opere d'ingegno ed artistiche: fotocopie di libri, duplicazioni su supporti magnetici ed ottici di documenti elettronici di particolare pregio, programmi per computer, musica e video, acquisizione delle stesse opere da internet.

Se da un lato ciò favorisce la divulgazione del sapere, dall'altro questo comporta un mancato guadagno per l'autore e tutti coloro che hanno contribuito alla realizzazione dell'opera e che si sono impegnati investendo tempo, denaro e messo a disposizione le proprie capacità artistiche, culturali, tecniche ed organizzative.

Il mancato guadagno, in prospettiva, scoraggia l'impegno degli autori con conseguente inaridimento della produzione di opere.

La disposizione legislativa che tutela il diritto d'autore è la legge 633 del 1941 che, evidentemente, non prevede la duplicazione delle opere artistiche e d'ingegno con l'ausilio di computer.

Le principali integrazioni alla legge 633/41 sono costituite dal decreto legislativo n. 518 del 29/12/1992 e dalla legge n. 248 del 18/08/2000.

Oggetto di tutela del diritto d'autore, nel caso di programmi per computer, è soltanto la forma espressiva del programma, non l'idea in esso contenuta.

Questa tutela limitata corrisponde ad una precisa scelta con la quale si è ritenuto di non arrestare il progresso tecnologico e scientifico, consentendo la diffusione di algoritmi e principi, ma si è altresì ritenuto di proteggere il singolo programma creato sulla base di quei principi.

Secondo il decreto legislativo 518/92, le disposizioni dello stesso decreto si applicano anche ai programmi creati prima della sua entrata in vigore.

La durata della tutela è di tutta la vita dell'autore e di 70 anni dalla sua morte.

Se il programma è un'opera collettiva, la durata della tutela è di 70 anni dalla prima pubblicazione.

Se il software è creato e pubblicato dalla Amministrazione dello Stato la durata è ridotta a 20 anni dalla data di pubblicazione.

La prova del diritto, cioè la prova che il programma è stato sviluppato da un soggetto, piuttosto che da un altro, può essere fornita mediante il deposito del programma presso l'apposito registro pubblico speciale per i programmi per elaboratore, costituito presso la SIAE.

Il legittimo acquirente può riprodurre il programma e tradurre, adattare o trasformare il programma solo se tali attività sono necessarie per l'uso del programma conformemente alla sua destinazione, inclusa la correzione degli errori; può, inoltre, effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso.

Chiunque abusivamente duplica per trarne profitto programmi per elaboratore, o, ai medesimi fini, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione programmi non contrassegnati dalla SIAE è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da € 2.500 a € 15.000.

Nel 2004, per far fronte al crescente fenomeno della pirateria informatica consistente nell'importazione da internet di programmi, musica e video in formato elettronico, è entrata in vigore in Italia una legge, nota come Legge Urbani, sulla pirateria informatica e sulla tutela della proprietà intellettuale.

La legge si scaglia soprattutto contro coloro che condividono su internet musica e video attraverso la tecnica peer-to-peer.

Introduce, inoltre, una tassa sensibile sull'acquisto di supporti di memoria sia ottici che magnetici, cioè su CD-ROM e DVD registrabili, su hard-disk e lettori di MP3: € 0,36 per ogni gigabyte.

Impone, inoltre, la tassa del 3% sull'acquisto di software per la masterizzazione e sugli stessi masterizzatori di CD-ROM e DVD.

La legge prevede, inoltre, forti sanzioni anche nei confronti dei provider che non denunciano all'autorità di polizia i clienti dediti al peer-to-peer.

Questionari

Quesiti a risposta singola

Rispondere a ciascuna domanda in 10 righe al massimo.

1. Che cosa si intende per internet?
2. Perché lo sviluppo di internet si è avuto dopo l'introduzione del www da parte del CERN di Ginevra?
3. Quali sono le principali attività che un programma browser di pagine web consente di effettuare?
4. Descrivi la procedura per la composizione e l'invio di un messaggio di posta elettronica.
5. Esprimi le principali differenze tra una mailing list ed un newsgroup.
6. Descrivi la procedura per definire un nuovo account di posta elettronica col programma Outlook Express.
7. Descrivi le principali funzioni consentite da un programma ad interfaccia grafica che permette di gestire il protocollo FTP.
8. Quali sono le principali modalità di collegamento ad internet a disposizione di un utente privato?
9. Fornisci qualche breve caratteristica dei comandi HTML con i quali è possibile comporre pagine web.
10. Quali sono le principali cause che minano la sicurezza informatica?
11. Dopo aver fornito il concetto di virus indica le azioni che un software antivirus è in grado di eseguire.
12. Descrivi una delle seguenti tecniche utilizzate da malintenzionati per minare la sicurezza informatica di una rete di PC: sniffing, spoofing, DoS.
13. Descrivi il principio di funzionamento della crittografia.
14. Cosa si intende per crittografia a chiave simmetrica e asimmetrica?
15. La firma digitale: descrivi la tecnica realizzativa e l'aspetto legale su un documento elettronico.
16. Che cosa si intende per wardriving?
17. La legge sulla privacy è garantita da una recente legge. Quale? Cosa recita l'art.1? Quale legge sostituisce?
18. L'art.4 della recente legge sulla privacy fornisce una serie di definizioni di termini. In particolare cosa si intende per "dati sensibili"?
19. L'art.4 della recente legge sulla privacy fornisce una serie di definizioni di termini. In particolare cosa si intende per "reti di comunicazione elettronica"?
20. Un server proxy consente la garanzia dell'anonimato durante la navigazione in internet. Come è possibile ciò?
21. Quanto tempo dura la tutela dei diritti d'autore di un singolo autore, di un'opera collettiva e dal software creato dalla Amministrazione dello Stato?
22. Le principali azioni della Legge Urbani contro la pirateria informatica.

Quesiti a risposta vero/falso

Barrare la casella relativa alla risposta che si ritiene esatta.

1. Il programma di posta elettronica Outlook Express scarica i messaggi solo all'avvio.
2. Preferiti è l'elenco degli indirizzi Internet che visiti più frequentemente.
3. Per aprire un sito di cui non si conosce l'indirizzo si utilizza un motore di ricerca.
4. Inoltrare un messaggio vuol dire inviare un messaggio ricevuto a un altro destinatario.
5. Per inviare più messaggi di posta a uno stesso gruppo di persone si crea una lista di distribuzione (mailing list).
6. Per attivare il controllo ortografico di un messaggio si attiva il menù Strumenti.
7. Il seguente indirizzo Web è corretto? <http://www.regione.puglia>
8. L'URL è l'indirizzo di una pagina Web.
9. Se ad un messaggio si assegna una priorità alta il messaggio viene inviato più velocemente.
10. Nella Rubrica di Outlook puoi inserire i nomi, gli indirizzi e-mail e altre utili informazioni sulle persone con le quali scambi messaggi di posta.
11. Per impostare i margini di una pagina Web che si desidera stampare si apre la finestra di dialogo Anteprima di Stampa.
12. Una pagina Web può essere salvata nel formato gif.
13. Per impostare la pagina iniziale di navigazione si apre il menu File e si seleziona il comando Salva con nome.
14. Per rendere più veloce il caricamento delle pagine Web si può visualizzare solo il testo delle pagine Web.
15. Il comando Opzioni Internet si trova nel menu Modifica.
16. Quando rispondi a un messaggio ricevuto, nel campo Oggetto del messaggio di risposta compare la sigla Re:
17. In Internet Explorer il menu che si deve aprire per personalizzare le Barre degli strumenti è il menu Strumenti.
18. Un link può essere rappresentato da immagini e parti di testo.

-
19. Outlook inserisce automaticamente nella Rubrica i nominativi di coloro che ti inviano un messaggio di posta elettronica.
 20. I messaggi di posta spostati nella cartella Posta Eliminata di Outlook sono eliminati definitivamente.
 21. Un documento html ha il titolo nel blocco di intestazione.
 22. L'obiettivo della sicurezza informatica è quello di garantire un adeguato grado di protezione dei beni.
 23. Un virus si può diffondere sfruttando la vulnerabilità dei protocolli di internet.
 24. Un hacker è un malintenzionato che diffonde virus.
 25. Lo spoofing è una tecnica che consiste nell'inviare ad un utente una ingente quantità di messaggi.
 26. La crittografia permette di trasmettere messaggi in chiaro.
 27. La chiave pubblica si utilizza nella crittografia a chiave asimmetrica.
 28. L'impronta è un sottoinsieme di caratteri di un documento lungo 1024 caratteri.
 29. Il wardriving è una tecnica con la quale si intercetta una rete wireless allo scopo di accedere alle risorse della rete locale e di sfruttare l'accesso ad internet.
 30. L'articolo 1 della legge 196/2003 sulla privacy afferma: Chiunque ha diritto alla protezione dei dati personali che lo riguardano.