

Modulo 2 – Online Essentials

Lezione 1 - Concetti di navigazione in rete

*In questa lezione si impareranno i **Concetti fondamentali (1.1)**, cioè a comprendere i termini: Internet, World Wide Web (WWW), Uniform Resource Locator (URL), collegamento ipertestuale (hyperlink) (1.1.1), ad identificare diversi tipi di servizi e di utilizzi dell'ICT, quali servizi Internet, tecnologie mobili, applicazioni di produttività di ufficio (1.1.2), a capire cosa è un browser e saper indicare il nome dei browser più comuni (1.1.3), ad identificare diverse attività su Internet, quali ricerca di informazioni, acquisti, formazione, pubblicazione, e-banking, servizi della pubblica amministrazione, intrattenimento, comunicazione (1.1.4), a conoscere la **Sicurezza (1.2)**, cioè a conoscere le diverse modalità per proteggersi quando si è online: effettuare acquisti da siti web noti e di buona reputazione, evitare la comunicazione non necessaria di informazioni personali e finanziarie, scollegarsi dai siti web (1.2.1), a definire il termine "crittografia" (1.2.2), a saper identificare un sito web sicuro: https, simbolo del lucchetto (1.2.3), a definire il termine "certificato digitale" (1.2.4), ad identificare le possibilità di controllo dell'uso di Internet, quali supervisione, limitazioni alla navigazione sul web, limitazioni agli scaricamenti (1.2.5).*

1.1 Concetti fondamentali

1.1.1 Comprendere i termini: Internet, World Wide Web (WWW), Uniform Resource Locator (URL), collegamento ipertestuale (hyperlink).

Nel modulo precedente abbiamo già parlato di Internet e dei suoi principali servizi, in questa lezione approfondiremo questi temi.

Il termine Internet deriva da INTERconnected NETwork, cioè Reti Interconnesse oppure Rete di Reti.

Infatti la struttura di Internet si basa su un insieme di reti locali, collegate a reti più ampie di tipo geografico; il sistema è completato da dorsali che non sono altro che linee di collegamento ad alta velocità, che rendono possibile la comunicazione rapida a livello mondiale.

Una delle caratteristiche principali di Internet è di non avere una gerarchia, cioè di non avere un Centro di Controllo e neppure nodi centrali; infatti una delle sue prime specifiche progettuali fu appunto quella di creare una rete in cui la messa fuori uso di alcuni nodi o di alcune connessioni non potesse interrompere le comunicazioni della rete. La struttura delle connessioni è a maglia; esistono infatti più percorsi alternativi per connettere due poli.

L'analogia che può essere fatta è quella della rete stradale. Anche in questa struttura esistono percorsi alternativi per collegare due località, e i tratti a maggiore traffico sono serviti da autostrade, che hanno il ruolo che in Internet è assegnato alle dorsali. Non a caso a queste linee telematiche, ad alta velocità e accessibili al pubblico, è stato dato il nome di autostrade dell'informazione.

Internet è una rete globale, a livello mondiale, dove tutte le risorse informatiche riescono a comunicare tra di loro grazie ad un protocollo di trasmissione comune, il TCP/IP (Transmission Control Protocol / Internet Protocol). Il protocollo di trasmissione è un insieme di regole che debbono essere seguite nelle varie operazioni necessarie per il trasferimento di dati. Il protocollo di comunicazione dovrà stabilire il destinatario ed il mittente del messaggio, che tipo di controllo degli errori utilizzare, quale sistema di compressione dati applicare, come si deve indicare la fine dell'invio di un messaggio, come il computer che riceve i dati deve segnalare l'avvenuta ricezione, ecc.

A Internet sono connessi dispositivi di comunicazione come computer, tablet, smartphone, telefoni cellulari, e le reti telematiche sfruttano una vasta gamma di tecnologie, quali doppiini telefonici, fibre ottiche, canali radio o a microonde, collegamenti satellitari.

Internet usa un tipo di comunicazione "a pacchetto". Questo significa che ogni messaggio viene suddiviso in tanti "pacchetti" di dati contenenti ciascuno il mittente, il destinatario, i dati, un numero progressivo ed un algoritmo che consente al ricevente di controllare che i dati siano arrivati senza errori.

Ciò permette di "instradare" i diversi pacchetti anche per vie diverse, a seconda del traffico o anche di eventuali interruzioni di linee. Inoltre questo sistema ottimizza l'uso delle linee poiché nessuno ne monopolizza una (come accade nelle comunicazioni telefoniche sulle linee tradizionali, nelle quali durante una conversazione le pause non possono essere utilizzate per trasmettere altri dati).

L'obiettivo di Internet è quello di mettere a disposizione una struttura a basso costo, ma in grado di fornire una vasta gamma di servizi, tuttora in fase di espansione. Ogni utente ha la possibilità di essere fruitore e fornitore di servizi.

La semplicità, i costi contenuti, la grande quantità di informazioni e servizi disponibili, la capillarità e globalità di diffusione sono i fattori che hanno determinato il grande successo di Internet.

Uno dei servizi più diffusi è certamente il World Wide Web, spesso abbreviato semplicemente in " Web" o anche indicato come "Navigazione in Internet". Proprio questo ultimo termine spesso genera confusione nell'uso dei termini Internet e Navigazione in Internet. Può, quindi, essere utile precisare, ancora una volta, che Internet è la struttura informatica e telematica che garantisce la trasmissione, mentre la navigazione in Internet è un servizio, di cui adesso analizzeremo le caratteristiche.

Le banche dati disponibili nella rete costituiscono il più cospicuo patrimonio di Internet. Le informazioni sono disponibili in formato multimediale (testo, immagini, filmati, audio) e ipertestuale, ossia alcuni termini sono associati ad altri attraverso collegamenti fisici, che riflettono collegamenti logici ad argomenti correlati. Grazie a questi collegamenti (in inglese link) ogni utente può liberamente muoversi tra le informazioni seguendo percorsi non prefissati ma decisi dall'utente stesso. Da qui deriva il termine di navigazione.

Questo è possibile grazie all'adozione di una interfaccia standardizzata per cui l'accesso è garantito in quanto tutti i siti sono interfacciabili mediante gli stessi programmi di interrogazione.

Il progetto Word Wide Web è nato nel 1990 dal gruppo di lavoro di Tim Berners-Lee, presso i laboratori del CERN (Centro Europeo per la Ricerca Nucleare) di Ginevra, ed inizialmente si proponeva di costituire un mezzo veloce per lo scambio di dati fra gruppi di scienziati sparsi in tutto il mondo.

L'introduzione del servizio WWW ha reso l'accesso alla rete facile e orientato ad utenti finali con limitate competenze informatiche, grazie all'adozione di un linguaggio comune per la definizione delle pagine che vengono visualizzate dagli utenti.

Il linguaggio utilizzato è l'HTML (HyperText Markup Language), che viene interpretato da appositi programmi che forniscono le funzioni per visualizzare le informazioni in modo comprensibile, e per utilizzare i collegamenti ipertestuali.

Dal momento che il World Wide Web può essere considerato un'enorme banca di dati multimediali, distribuita in un elevato numero di sistemi informatici, sparsi in tutto il mondo, per poter avere l'accesso al sistema che ci interessa occorre conoscerne l'indirizzo, ma anche la risposta deve essere instradata al computer dell'utente che ha effettuato la richiesta.

E' quindi evidente la necessità di un sistema di indirizzi che identifichi ogni risorsa collegata ad Internet.

Un indirizzo IP è un codice numerico che identifica univocamente un dispositivo collegato alla rete Internet, fornisce il percorso per raggiungerlo in una comunicazione a pacchetto. Ad alcuni dispositivi, come i nodi della rete, possono essere associati più indirizzi.

Gli indirizzi sono facilmente gestiti dalle risorse informatiche della rete, ma, dato l'elevato numero di cifre che li compongono, non sono facilmente utilizzabili direttamente dagli utenti della rete.

La soluzione del problema consiste nel dare agli utenti la possibilità di utilizzare nomi simbolici, di tipo mnemonico e quindi facili da ricordare. L'indirizzo espresso in questa forma prende il nome di Uniform Resource Locator (URL). Questo argomento verrà trattato in modo più dettagliato nel prossimo punto. La trasformazione dell'indirizzo simbolico nell'indirizzo fisico corrispondente viene effettuata dal Domain Name Server (DNS), un servizio, distribuito su più elaboratori, che gestisce le tabelle che permettono la traduzione da URL a IP Number.

Abbiamo già detto che una delle caratteristiche più interessanti del World Wide Web è la possibilità di navigare, cioè di saltare da un documento ad un altro sia all'interno dello stesso sito web, sia in siti web diversi. Queste connessioni vengono definite collegamenti ipertestuali (in inglese hyperlink) o semplicemente "link", e possono essere costituite da un'icona, da parole (in questo caso esse sono normalmente sottolineate) o da un'immagine.

Ad esempio, in una pagina dedicata ad un autore, si potrebbero trovare link che portano a ciascuno dei suoi libri, ma anche da un libro si può saltare alla pagina dell'autore.

In una pagina web, quando il puntatore del mouse è posizionato su collegamento, assume l'aspetto di una piccola mano con l'indice rivolto verso l'alto.

Per facilitare la ricerca degli elementi che hanno collegamenti ipertestuali, puoi passare da un link all'altro tramite TAB (link successivo) o MAIUSC + TAB (link precedente).

In generale, il termine "ipertesto" definisce un testo in cui, oltre alla normale lettura sequenziale, è possibile una fruizione non lineare, saltando cioè da una parte all'altra del testo mediante i link. Si parla invece di "ipermedia" se sono coinvolti anche dati multimediali come filmati o audio.

1.1.2 Capire come è strutturato l'indirizzo di un sito web. Identificare i tipi più comuni di domini, quali geografici, aziendali (.org, .edu, .com, .gov).

Abbiamo già detto che un sito è caratterizzato da un URL univoco. La struttura di un URL è la seguente:

protocollo://www.nome_server.dominio_di_primo_livello.

Il protocollo indica quali sono le regole utilizzate per la comunicazione; nella navigazione in Internet è spesso l'acronimo di HyperText Transfer Protocol.

L'Indirizzo è preceduto da due barre // ed è a sua volta diviso in più parti separate da un punto: l'acronimo www è presente nella maggior parte degli indirizzi, ma a volte può mancare. Il nome del server è quello mnemonico scelto dal proprietario del sito (ad esempio il nome di un'organizzazione, di un'azienda, di una persona). Il dominio di primo livello indica presso quale organizzazione delegata è stato registrato il sito.

Il dominio di primo livello può essere costituito da due caratteri alfabetici, che indicano la nazione in cui è stato registrato L'URL, o da più caratteri alfabetici che indicano il tipo di organizzazione a cui fa riferimento il sito, che viene in tal caso registrato dall'organizzazione internazionale delegata a gestire tale dominio di primo livello.

Esempi di domini di primo livello di tipo nazionale sono:

- it, Italia;
- fr, Francia;
- de, Germania;
- uk, Gran Bretagna;
- es, Spagna;
- at, Austria;
- ch, Svizzera;
- cn, Cina;
- jp, Giappone.

Esempi di domini di primo livello associati al tipo di organizzazione sono:

- com, commerciale;
- biz, business;
- edu, istituzione educativa;
- gov, ente governativo USA;
- mil, organizzazione militare;
- net, polo di rete;
- org, organizzazioni private non comprese nelle categorie precedenti;
- name, individuale.

Ad esempio l'indirizzo di ASPHI è <http://www.asphi.it>

1.1.3 Capire cosa è un browser e saper indicare il nome dei browser più comuni.

Dopo avere detto che i siti Web sono costituiti da pagine scritte in linguaggio HTML, occorre anche dire che per interpretare correttamente tali pagine sono necessari appositi programmi che traducano dal linguaggio HTML, mostrando all'utente una pagina per lui leggibile. Questi programmi sono i "browser".

Il browser viene installato sul computer dell'utente, e svolge i seguenti compiti: richiede un file HTML al server che gestisce le informazioni volute, lo traduce creando la pagina in modo che sia comprensibile per l'utente e chiedendo al server le immagini, i filmati, le registrazioni audio delle quali è previsto l'inserimento, visualizza la pagina definitiva per l'utente.

Inoltre, il browser mette a disposizione dell'utente una serie di funzioni per rendere più agevole la navigazione in rete. Le più usate di queste funzioni verranno analizzate nella Lezione 2.

I browser attualmente più diffusi sono: Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome.

1.1.4 Identificare diverse attività su internet, quali ricerca di informazioni, acquisti, formazione, pubblicazione, e-banking, servizi della pubblica amministrazione, intrattenimento, comunicazione.

Le applicazioni su Internet, ed in particolare l'utilizzo del servizio World Wide Web, sono entrate nella realtà quotidiana, portando sensibili cambiamenti nelle nostre attività, che sempre più trovano in Internet la possibilità di ottenere informazioni e servizi direttamente dal nostro computer. Ormai sono innumerevoli le attività possibili.

La quantità di informazioni disponibili in Internet e la loro varietà non hanno confronto con nessun altro strumento di comunicazione utilizzabile. La vastità delle banche di dati a disposizione fa sì che sia praticamente impossibile immaginare una domanda a cui non sia data risposta dal web. Le informazioni spaziano dall'attualità alla storia, dalle letterature alla scienza, dalla politica alla società, sino ad arrivare alle notizie giornalistiche, orari ferroviari e aerei, spettacoli in programmazione, calendari di eventi, previsioni meteo, mappe e percorsi stradali, informazioni turistiche, ecc. Il tutto è arricchito dalla presenza di dati multimediali come immagini, filmati, registrazioni audio, che forniscono l'informazione di un valore aggiunto, spesso insostituibile.

Un altro settore in forte sviluppo, nonostante la crisi economica a livello mondiale, è il commercio elettronico, electronic commerce (e-commerce), cioè l'utilizzo della rete per la vendita di beni o servizi. Il ruolo di Internet in questo caso può riguardare tutte le fasi della transazione: catalogo e presentazione dei prodotti e servizi offerti (vetrina virtuale), acquisizione dell'ordine (carrello degli acquisti), pagamento con moneta elettronica, consegna del prodotto, nel caso di prodotti immateriali (libri elettronici, film, registrazioni musicali, biglietti di viaggio, prenotazioni alberghiere o a spettacoli, software) o di servizi (di consulenza, finanziari, legali).

Oltre al vantaggio di poter effettuare acquisti direttamente dal proprio computer, l'acquirente ha la possibilità di scegliere tra più negozi virtuali, cercando le condizioni economiche più vantaggiose, di scegliere tra un elevato numero di prodotti concorrenti, di disporre di documentazione tecnica a supporto della scelta, di accedere al servizio 24 ore al giorno, 365 giorni all'anno.

Per il venditore il vantaggio è di poter disporre dell'intero mercato mondiale, con investimenti molto contenuti.

Il pagamento elettronico può avvenire secondo varie modalità: carta di credito, carta di addebito (Bancomat), moneta elettronica prepagata (borsellino elettronico), assegno circolare elettronico rilasciato da un'azienda di credito.

A fronte di questi vantaggi, si presentano alcuni svantaggi: per alcuni prodotti le caratteristiche sono esclusivamente immagini e informazioni riportate su un catalogo e non derivano dal contatto con il prodotto reale, e la transazione non può essere anonima, come nel commercio tradizionale; inoltre, al negozio virtuale devono essere trasmessi alcuni dati personali, con il pericolo che ne venga fatto un utilizzo non autorizzato, e possono essere effettuate truffe sia da parte dell'acquirente che del fornitore, non è garantita la totale sicurezza dei pagamenti.

Nella formazione assistita da computer (e-learning) le attività possono riguardare la formazione a distanza, l'autoistruzione (via rete o libri elettronici su CD o DVD), l'autovalutazione, la simulazione di esperimenti.

A livello mondiale molte università erogano i corsi esclusivamente per via telematica.

I vantaggi possono essere la qualità della didattica, supportata da dati multimediali, i tempi di apprendimento possono variare in funzione della preparazione dell'allievo, che può saltare argomenti a lui noti e ripetere parti di lezioni che necessitano di una maggiore attenzione, distribuzione del corso sul territorio senza la necessità di concentrare gli allievi in una sede (con conseguenti costi di trasferimento e soggiorno), minori costi di erogazione, anche se accompagnati da maggiori costi nella preparazione del corso.

A fronte sono da considerare gli svantaggi derivanti dalla mancanza di rapporto diretto tra allievo e docente (che il computer può sostituire esclusivamente per le attività previste in fase di progettazione del corso) e, per quanto riguarda l'autovalutazione, le limitazioni che riguardano le possibilità di risposta dell'allievo; spesso nella autovalutazione vengono utilizzati test con risposte predefinite a scelta singola o multipla.

L'attività di pubblicazione via rete riguarda in primo luogo quotidiani e periodici; i vantaggi rispetto alle versioni cartacee riguardano sia i minori costi di pubblicazione e distribuzione, sia la possibilità di aggiornare in continuazione le notizie. Ma l'editoria via rete mette a disposizione anche libri digitali, eventualmente anche multimediali, che

possono essere letti direttamente sul computer, ma anche scaricati sul proprio sistema per una lettura successiva, senza necessità di collegamento.

La moneta elettronica e il trasferimento elettronico del fondo sono utilizzate dalle banche sin dalla disponibilità delle prime reti telematiche. Le applicazioni riguardavano allora esclusivamente i rapporti interbancari. Con l'arrivo di Internet, le aziende di credito hanno reso disponibili ai propri clienti una vasta gamma di servizi, tra cui fondamentali la gestione dei propri conti bancari, l'esecuzione di operazioni di pagamento (bonifici, bollettini), il pagamento di tasse, tributi, servizi, contravvenzioni, l'acquisto e la vendita di azioni e obbligazioni. L'insieme di queste applicazioni prende il nome di e-banking.

Nella maggior parte dei casi questi servizi si affiancano a quelli di sportello tradizionali, ma esistono anche banche nelle quali non esistono sportelli tradizionali, ma tutte le transazioni avvengono via rete telematica. I vantaggi principali per i clienti sono quelli di operare direttamente dal proprio computer e di disporre di un servizio 24 ore al giorno e 365 giorni all'anno, per le imprese di credito un risparmio di costi di infrastrutture e personale.

Con il termine e-government si indica normalmente il complesso dei servizi telematici che gli enti della pubblica amministrazione, centrale e locale, mettono a disposizione di cittadini, professionisti ed imprese. Gli obiettivi, in questo caso non sono solo quelli di facilitare la comunicazione tra utente e pubblico ufficio, ma soprattutto di integrare i sistemi informativi dei vari enti, in modo da presentare agli utenti un'unica interfaccia verso la pubblica amministrazione di qualsiasi livello.

Accanto alla erogazione di servizi tradizionali, quali il supporto all'autocertificazione, l'avviamento e la verifica dello stato di avanzamento delle pratiche, il pagamento di servizi e di contravvenzioni, una delle aree attualmente di maggior interesse riguarda la trasparenza degli atti amministrativi. Per conseguire tale risultato, recenti leggi obbligano tutti gli enti pubblici a pubblicare le delibere approvate, gli stipendi e le carriere dei funzionari di più alto livello, i compensi e i curricula dei consulenti utilizzati, le gare d'appalto emesse e assegnate, ecc.

Anche il settore dell'intrattenimento ha subito una profonda trasformazione a fronte di una sempre più capillare diffusione di Internet. Molti spettacoli, sia di intrattenimento che sportivi, si possono seguire in diretta tramite la rete. Altri vengono registrati e messi a disposizione a richiesta dell'utente. I giochi in formato elettronico possono prevedere partite tra utente e computer, ma anche tra due o più utenti in rete. Inoltre si possono trovare registrazioni di film, di concerti, spettacoli teatrali, ecc. La fruizione di tali forme di intrattenimento può essere gratuita o a pagamento.

Basta pensare all'enorme successo del sito YouTube, che permette di vedere filmati, in molti casi caricati direttamente dagli utenti, ma anche resi disponibili da importanti aziende, che hanno un rapporto di collaborazione con YouTube. Ne sono un esempio vecchi film, non più reperibili in altro modo.

L'obiettivo principale delle reti che hanno preceduto Internet era la realizzazione di un valido strumento di supporto alle comunicazioni. La svolta impressa da Internet è stata quella di rendere molto diffuso il servizio, grazie ad una riduzione notevole dei costi. Inoltre, nel tempo il servizio iniziale di posta elettronica (email), di cui parleremo in dettaglio alla fine di questo modulo, è stato affiancato da una vasta gamma di servizi in risposta ad esigenze specifiche.

Le mailing list, liste di distribuzione, sono messaggi di posta elettronica, che vengono inviati ad utenti che si sono iscritti al servizio, per avere informazioni sulle novità inerenti un tema specifico.

Le Chat line e l'Instant Messaging, messaggistica istantanea, sono servizi per lo scambio, in tempo reale, di brevi messaggi di tipo testo tra due o più utenti. La principale differenza con l'email è che in questo caso lo scambio è sincrono, cioè gli interlocutori sono tutti connessi contemporaneamente alla rete.

Il servizio VoIP, Voice over Internet Protocol, consente le conversazioni telefoniche audio e video mediante la rete Internet, con un notevole abbattimento di costi rispetto alle linee telefoniche tradizionali, soprattutto per le telefonate a lunga distanza.

I Gruppi di discussione (news group) possono essere considerati bacheche virtuali dedicate a utenti interessati a temi specifici; gli utenti iscritti ad un gruppo possono pubblicare e leggere le informazioni sul tema scelto.

Una evoluzione significativa delle comunicazioni e della diffusione di informazioni si è avuta con i social-network, cioè servizi che hanno come obiettivo quello di mettere in relazione e di tenere aggiornati i propri iscritti sugli interessi che li accomunano.

Le caratteristiche dei principali servizi verranno trattate in seguito.

1.2 Sicurezza

1.2.1 Conoscere le diverse modalità per proteggersi quando si è online: effettuare acquisti da siti web noti e di buona reputazione, evitare la comunicazione non necessaria di informazioni personali e finanziarie, scollegarsi dai siti web.

Abbiamo detto che in rete viaggia una grande quantità di dati. L'utilizzo della rete è improntato alla massima democrazia, in quanto non esistono di fatto controlli; tutti gli utenti possono inserirsi nella rete per immettere o prelevare informazioni di qualsiasi tipo, senza nessuna verifica e con la possibilità di rimanere anonimi. Da questa democrazia, che qualcuno definisce anche anarchia, derivano notevoli problemi in merito alla sicurezza e alla privacy.

Uno dei pericoli maggiori è costituito da quelli che vengono comunemente indicati come pirati informatici (in inglese cracker), che possono inserirsi nella rete per catturare identificativo utente e password, o numero di carta di credito, o altri dati sensibili, per utilizzarli in modo fraudolento o comunque non autorizzato.

La difesa contro questi pericoli sta nel collegarsi solo a siti di organizzazioni note, ignorare messaggi di posta elettronica che invitano a inviare i propri dati a siti dei quali viene inserito l'indirizzo nel messaggio, evitare di fare il download di programmi della cui provenienza non si è certi.

Anche nelle attività di commercio elettronico è bene effettuare acquisti solo da aziende sicure, verificare se hanno referenze, e comunicare i dati strettamente necessari per la fatturazione e l'eventuale spedizione. Tieni presente che nella home page dei siti aziendali devono essere pubblicati, per legge, la ragione sociale e la partita IVA (che possono essere controllati sul sito dell'Agenzia delle Entrate), il numero di telefono della rete fissa. Normalmente i dati da comunicare per un acquisto sono cognome e nome, indirizzo, prodotti ordinati e loro quantità, codice fiscale, e numero della carta di credito nel caso di pagamento elettronico.

Infine scollegati da un sito, quando hai terminato il suo utilizzo.

1.2.2 Definire il termine "crittografia".

In campo militare si è sempre sentita l'esigenza di proteggere i messaggi trasmessi, in modo da renderli illeggibili per il nemico. Nella storia si conoscono sistemi di mascheramento dei messaggi usati dagli Ebrei, dagli Spartani e da Giulio Cesare che dalla Gallia rimaneva in contatto con i suoi alleati per preparare il suo ritorno a Roma.

La crittografia è la cifratura del messaggio, ossia la sua trasformazione in modo che diventi incomprensibile per chi non conosce le regole per tornare al messaggio originale. Il termine deriva dalle parole greche che corrispondono a nascosto e scrittura.

Con lo sviluppo di Internet e delle comunicazioni ad essa associate, e i conseguenti problemi di sicurezza di cui abbiamo appena parlato, la crittografia è diventata un argomento di grande interesse nelle comunicazioni in rete.

Un sistema molto semplice, ad esempio, consiste nella sostituzione di ogni lettera dell'alfabeto con un'altra corrispondente. Utilizzando un'apposita tabella di codifica per crittografare il messaggio e la stessa tabella per decrittarlo, si ottiene lo scopo. Questo sistema è facilmente individuabile in quanto ogni lingua presenta delle regolarità e delle frequenze di utilizzo delle lettere dell'alfabeto; ad esempio in italiano la lettera che compare con maggiore frequenza è la E, per cui se il messaggio è abbastanza lungo basta cercare la lettera che compare più volte e sostituirla con la E. Analogamente si può fare per diverse altre lettere, per cui questo sistema di crittografia è assai poco sicuro.

In genere si può dire che ogni sistema crittografico ha due elementi base: un "algoritmo di codifica" che è l'insieme delle regole per passare dal messaggio in chiaro a quello criptato, ed una "chiave" che viene usata dall'algoritmo per criptare e poi per decriptare il messaggio stesso.

E' evidente che per interpretare il messaggio occorre conoscere sia l'algoritmo che la chiave.

La sicurezza di un sistema di crittografia dipende dalla facilità con cui un malintenzionato può riuscire a decifrarlo. Se si fa uso di un algoritmo troppo semplice e di una chiave di lunghezza limitata, si sarà costretti a ripetere dei caratteri o delle sequenze di caratteri nel messaggio criptato: questo potrebbe fornire uno schema a chi cerca di interpretare il messaggio.

Altro fattore di sicurezza è il numero di chiavi che l'algoritmo ammette: se fosse, poniamo, di 10.000, si potrebbe pensare che con i moderni computer una persona che non conosca la chiave potrebbe in un lasso di tempo accettabile

provarle tutte e 10.000 fino a trovare quella voluta (utilizzando l'approccio cosiddetto della "forza bruta", basato non sull'intelligenza, ma solamente sulla velocità con cui si possono fare dei tentativi).

I primi sistemi di crittografia, adottati in campo informatico e telematico, erano basati su un sistema simmetrico, a chiave segreta. Questi sistemi prevedono l'utilizzo della stessa chiave per criptare e decriptare i messaggi. La chiave deve pertanto rimanere segreta, conosciuta solo ai due interlocutori che si scambiano il messaggio criptato. Questa soluzione presenta due svantaggi. Da un lato il proliferare di chiavi dovuto al fatto che deve essere generata una chiave per ogni coppia di interlocutori, dall'altro la vulnerabilità del sistema dovuta alla fase di comunicazione della chiave, durante la quale la chiave potrebbe essere intercettata.

La soluzione consiste nell'adozione di un sistema asimmetrico, a chiavi pubbliche, che prevede siano utilizzate due chiavi diverse per crittare e decriptare. La prima, chiave pubblica, è di pubblico dominio, in quanto inserita in cataloghi consultabili in Internet, la seconda, chiave privata, è conosciuta solo dal suo proprietario. Un messaggio criptato con una delle due chiavi, può essere decriptato solo con la seconda chiave.

La crittografia asimmetrica può quindi essere utilizzata sia come protezione della segretezza che per individuare con sicurezza l'autore del messaggio.

Infatti, nel caso il messaggio inviato venga criptato con la chiave pubblica del destinatario, solo quest'ultimo conosce la corrispondente chiave privata, ed è in grado di decriptare e quindi leggere il messaggio; che risulta segreto per tutti salvo che per il destinatario.

Nel caso il messaggio venga criptato con la chiave privata del mittente, chi lo riceve può decriptarlo solo con la chiave pubblica del mittente ed avere quindi la certezza su chi lo ha inviato. Di fatto ne viene certificato l'autore. In questo modo il mittente ha messo la propria "firma digitale" al messaggio.

Il messaggio può anche essere criptato con la chiave privata del mittente e con la chiave pubblica del destinatario; in questo caso si raggiungono entrambi gli obiettivi: segretezza e autenticazione del messaggio.

Per funzionare il sistema necessita di cataloghi on line delle chiavi pubbliche, ma è anche indispensabile che sia garantita l'identità del possessore delle chiavi, ossia ne siano verificate le generalità. Questo tema verrà sviluppato nel capitolo dedicato al certificato digitale.

L'unica controindicazione della crittografia asimmetrica è che entrambi i processi sono caratterizzati da elaborazioni complesse e quindi comportano tempi lunghi quando si devono trattare grandi quantità di dati. Per la firma digitale il problema viene risolto criptando la traccia del documento, ossia un suo riassunto digitale, mentre l'intero documento viene trasmesso in chiaro. Quando il problema è quello della segretezza si ricorre all'uso del sistema simmetrico, molto più veloce, avendo però cura che la trasmissione della chiave venga criptata con il sistema asimmetrico, che ne garantisce la segretezza.

1.2.3 Saper identificare un sito web sicuro: https, simbolo del lucchetto.

Alcuni siti in rete sono protetti, cioè le comunicazioni con il sito sono criptate. Se visiti un sito protetto, al momento della connessione viene inviato al browser il certificato del sito. Se il certificato è scaduto vieni avvisato con un messaggio. Inoltre, nella barra degli indirizzi compare l'immagine di un lucchetto, e il protocollo di trasmissione si modifica da TFTP a HTTPS (HyperText Transfer Protocol over Secure Socket Layer).

In qualsiasi momento puoi avere informazioni sul certificato selezionando con TAB il pulsante del lucchetto e premendo INVIO. Si apre la finestra che indica chi ha effettuato la verifica, chi è il proprietario del sito, e la conferma che la connessione al server è crittografata. Per avere ulteriori informazioni con TAB vai al pulsante "Visualizza certificati" e premi INVIO. Con Freccia GIU' raggiungi la voce "Visualizza certificati" e premi INVIO. Nel certificato, tra gli altri dati, è presente la data di scadenza. Per chiudere la finestra, in funzione di come questa si presenta raggiungi con TAB il pulsante "OK" e premi INVIO, o premi ALT + F4.

Nel protocollo HTTPS, usato come abbiamo detto per i siti protetti, tra il protocollo HTTP e quello TCP viene inserita una fase di crittografia dei dati, in modo che quanto trasmesso sia comprensibile solo per il server e il computer utente collegato.

1.2.4 Definire il termine "certificato digitale".

Nel punto precedente abbiamo parlato dei certificati digitali rilasciati ai siti della rete, ed abbiamo anche descritto come possono essere visualizzati questi certificati.

Analizziamo ora con maggior dettaglio le più importanti caratteristiche del certificato. Innanzitutto, come abbiamo già in parte anticipato, il documento riporta il numero del certificato, l'organizzazione che lo ha rilasciato, il soggetto a cui si riferisce, la chiave pubblica, e il tipo di algoritmo utilizzato nella crittografia, la data di rilascio e la data di scadenza.

Avrai notato che abbiamo parlato di soggetti a cui è stato rilasciato il certificato e non di siti web. Questo perché il certificato può essere rilasciato anche a persone, aziende, organizzazioni.

Non solo, alla stessa persona possono essere rilasciati più certificati nel caso ricopra più ruoli (ad esempio presidente di una organizzazione e amministratore delegato di un'altra).

Essi vengono emessi da un'Autorità di Certificazione, Certificate Authority (CA,) e sono firmati con la chiave privata dell'Autorità.

L'Autorità di Certificazione ha il compito di identificare il soggetto certificato, rilasciare il certificato, assegnarli la coppia di chiavi, gestire le banche dati delle chiavi pubbliche, determinare e controllare la scadenza dei certificati, revocare, al verificarsi di certi eventi, il certificato e le chiavi rilasciate. In sintesi il certificato garantisce la corrispondenza tra le chiavi pubbliche e i soggetti a cui sono state rilasciate.

1.2.5 Identificare le possibilità di controllo dell'uso di Internet, quali supervisione, limitazioni alla navigazione sul web, limitazioni agli scaricamenti.

E' già stato detto che la rete non è soggetta a nessun controllo preventivo. La rete, pertanto, può essere utilizzata per distribuire contenuti illeciti anche dal punto di vista penale, quali la pedofilia, informazioni sulla costruzione di esplosivi, ecc.

Altri contenuti possono essere inadatti ad utenti giovani, ne sono un esempio la pornografia, le immagini e i filmati violenti, il bullismo, le scommesse, i giochi non adatti. La rete talvolta viene utilizzata anche per l'adescamento di minorenni.

Una possibile soluzione alla navigazione senza limiti può essere il firewall, di cui abbiamo già parlato nella lezione 6 del modulo 1, e che permette di bloccare l'accesso a siti giudicati non idonei.

In modo analogo, ma più semplice da gestire, può funzionare il filtro famiglia o controllo genitori (parental control in Inglese), che può essere un programma o un servizio, che permette di indicare le pagine Internet alle quali è vietato l'accesso, o anche, in modo più restrittivo, a quali pagine è consentito l'accesso.

Si può inoltre creare una navigazione differenziata, distinguendo tra utente minore e utente adulto, al momento del collegamento in Internet. Tale sistema opera mediante filtri che effettuano analisi sulle parole utilizzate nella ricerca e limitano i tempi di collegamento.

Windows 7 offre una valida funzione di controllo. Per attivarla apri il menu "Start" (ALT + ESC o tasto di AVVIO di WINDOWS), poi con FRECCIA DESTA vai sulla parte destra della finestra e con FRECCIA GIU' o "P" posizionati sul "Pannello di controllo" e dai INVIO:

Nella nuova finestra, fra le icone che compaiono, tramite le frecce direzionali seleziona "Controllo genitori" e premi INVIO. Si apre una nuova finestra nella quale sono presenti gli utenti riconosciuti dal sistema. Seleziona con FRECCIA GIU' l'utente a cui vuoi applicare il controllo, e che deve essere un utente per il quale è previsto l'accesso via password. Nel caso l'utente non fosse già generato lo puoi creare in questa fase. Una volta selezionato l'utente premi INVIO. Si apre la finestra controllo utente. Con TAB raggiungi la sezione "Controllo genitori" e con FRECCIA SU seleziona "Attivato applica le impostazioni correnti" e con il tasto SPAZIO attiva la scelta. Con TAB raggiungi il pulsante OK e premi INVIO.

In aggiunta o sostituzione puoi usare programmi, anche gratuiti, che permettono di verificare tutte le operazioni fatte sul computer, in modo da sapere quanto è stato fatto durante la tua assenza, o di limitare a certi giorni e a certe ore l'accesso ad Internet.

Il controllo più efficace è comunque la presenza di un adulto durante la navigazione in Internet di un minore.

Termina qui la prima lezione del Modulo 2.

Ora sei certamente pronto per iniziare ad immergerti nel mondo di Internet.