6. Impatto Sociale

6.1 Elaboratori e società

6.1.1 Introduzione

Durante questo periodo, grazie all'utilizzo delle nuove tecnologie, si sta assistendo al passaggio dalla società industriale alla società dell'informazione; ci si trova di fronte alla terzializzazione dell'economia visto che diventa più importante la produzione di servizi rispetto alla produzione dei beni tradizionali.
I benefici portati da simili trasformazioni inducono un miglioramento delle condizioni generali di vita, derivante alla qualità dei servizi offerti; questo per tutte le persone ed in tutti gli aspetti, in particolare è favorita l'integrazione dei soggetti in situazione di handicap che, con hardware e software specifici, svolgono attività fino a poco tempo fa loro precluse.
La rapida diffusione dell'informazione comporta però dei rischi, come la nascita di nuove emarginazioni legate a fenomeni di analfabetismo tecnologico: chi non ha dimestichezza con le modalità di utilizzo dei nuovi strumenti, viene escluso dal godimento dei benefici.
L'elaboratore trova impiego in diversi campi dell'esperienza quotidiana, per esempio: in casa, nell'ambito lavorativo, nell'istruzione; di seguito esamineremo ognuno di questi aspetti.

6.1.2 Il computer nella casa

Le applicazioni dell'informatica all'ambiente domestico investono i seguenti campi:

- contabilità familiare
- studio
- informazione (navigazione in Internet)
- svago (giochi)
- attività lavorativa (supporto all'attività o vero telelavoro di cui si tratterà più avanti)
- negozio elettronico (possibilità di acquisti *on line*)

Gli sviluppi nell'immediato futuro prevedono elettrodomestici ed edifici "intelligenti"; questi ultimi, evoluzione dei già esistenti edifici cablati, prevedono un computer centrale che gestisce i servizi generali quali l'illuminazione, il riscaldamento e/o la climatizzazione degli ambienti, il sistema antincendio, i sistemi di sicurezza, ecc.
Per quanto riguarda gli elettrodomestici esistono già in commercio, anche se non sono ancora molto diffusi, esempi della tecnologia sopracitata (condizionatori, forni, lavatrici, ecc.).

6.1.3 Il computer nel lavoro e nell'istruzione

Nel luogo di lavoro l'elaboratore mette a disposizione strumenti per:

- **migliorare la produttività individuale** (una persona può gestire da sola il lavoro che, trent'anni fa, era gestito da tre persone; oltre ai vantaggi legati alla mera automazione se ne riscontrano altri, per esempio: la manutenzione di un programma che può essere fatta in tempo reale via Internet, con un enorme risparmio sia di tempo che di denaro; la possibilità del lavoro in teleconferenza ecc.)
- **controllare processi produttivi**
- **automatizzare procedure** (l'uomo viene sollevato dai lavori ripetitivi, alienanti e dannosi)
- **archiviare informazioni** (numerose le ripercussioni: nella pubblica amministrazione migliora il rapporto con il cittadino sia in termini di efficienza che di trasparenza; nel settore sanitario è possibile l'informatizzazione delle prenotazioni con il CUP (centro di prenotazione unica), l'informatizzazione coordinata del 118 ecc.)

In tale contesto la rivoluzione tecnologica, che da una parte ha affermato l'avvento delle reti ed in particolare di Internet e dall'altra ha notevolmente migliorato le prestazioni e i costi del mezzo informatico aumentandone esponenzialmente la diffusione, ha favorito la nascita di una nuova tipologia di lavoro: il *Telelavoro*. Di questo aspetto ci occuperemo nel prossimo paragrafo.

Nell'ambito dell'istruzione può essere utilizzato per:

- **migliorare il processo educativo** (con CD-ROM interattivi o programmi specifici)
- **consentire l'apprendimento a distanza**
- **abituare lo studente all'utilizzo di nuove tecnologie**
- **consentire l'autoapprendimento guidato**

6.1.4 Telelavoro

E' opportuno chiarire cosa si intenda quando si parla di *telelavoro*; non esiste una definizione univoca di tale attività, bensì una gamma di definizioni che sono ben rappresentate dalla seguente:

Un'attività si configura come telelavoro qualora siano rispettate le seguenti condizioni:

- esista una delocalizzazione dell'attività rispetto alla sede tradizionale di lavoro

- si usino strumenti telematici nello svolgimento del lavoro

- l'attività svolta a distanza abbia caratteristiche di sistematicità

L'arco delle definizioni del telelavoro, come già visto, è piuttosto ampio e ammette, di conseguenza, diverse pratiche telelavorative.

La tipologia del telelavoro si ripartisce secondo alcuni criteri di identificazione:

- il *luogo* dove si svolge il telelavoro;
- il *tempo* di durata della prestazione telelavorativa;
- lo *status* di impiego del telelavoratore;
- la *forma* della pratica telelavorativa: individuale o collettiva.

Esaminiamo ora i tipi di telelavoro che discendono da questa classificazione generale.

- **a domicilio (home office)**
- **mobile**
- **ufficio satellite**
- **telecentri, telecentri di quartiere (neighbourhood offices) e telecottages**
- **ufficio virtuale**

Il *telelavoro a domicilio* costituisce la prima modalità di telelavoro sperimentata; ancora oggi, a dire il vero, si tende a identificare il telelavoro esclusivamente con questa modalità. Le condizioni di attivazione sono semplici: basta disporre di un PC collegato, attraverso le linee telefoniche o attraverso apposite ISDN, a dei network di computer remoti.
All'interno di questa categoria è stata fatta un'ulteriore distinzione: a) telelavoratori a domicilio costantemente *on line*; b) telelavoratori che possono regolare in autonomia il tempo della propria prestazione.
In genere, le imprese optano per la soluzione denominata *telelavoro alternato* che prevede il lavoro a domicilio solo per una frazione di tempo, con il ritorno in ufficio per la restante parte della giornata lavorativa. Questa forma di telelavoro, rispetto al telelavoro a domicilio a tempo pieno, presenta il vantaggio di offrire una maggiore possibilità di comunicazione tra dipendente e datore di lavoro.
La prestazione telelavorativa può avvenire attraverso ripetuti spostamenti: in questi casi, il lavoratore presta la sua opera qualunque sia il posto in cui si trova (albergo, casa, sede di un cliente o addirittura in viaggio). Le figure professionali più diffuse per il *telelavoro mobile* sono: agenti di vendita, ingegneri e, in generale, quadri dirigenti.
Quando si parla di *ufficio satellite* ci si trova in presenza di una forma collettiva di telelavoro, simile alla tradizionale filiale, presente da tempo nell'organizzazione territoriale di molte società.
La differenza tra la filiale classica e l'ufficio satellite di telelavoro è la seguente:

- la filiale ha la funzione limitata di soddisfare e incanalare i bisogni dei clienti e/o dei mercati locali;
- l'ufficio satellite, seppur lontano dagli uffici centrali, usando connessioni in rete, può svolgere la propria attività a favore dell'intera organizzazione, non già in funzione del solo mercato locale.

Un caso tipico di ufficio satellite è quello dei *call centres*, istituiti dalle banche per gestire direttamente le operazioni con i clienti.

I vantaggi arrecati dagli uffici satellite sono intuibili, per i benefici assicurati dalle minori spese immobiliari e da spese generali inferiori. Inoltre, i costi per il personale possono essere più bassi nelle zone geograficamente lontane e può anche aumentare la disponibilità di posti di lavoro.
Che l'ufficio satellite sia una risorsa di tipo strategico e globale è dimostrato dalla crescente diffusione di centri specializzati per l'elaborazione dei dati nelle destinazioni cosiddette "offshore" (come i Caraibi, le Filippine e la Cina popolare).
Quando si parla di *telecentri, telecentri di quartiere (neighbourhood offices) e telecottages* si fa riferimento a un ufficio a distanza, equipaggiato con le necessarie connessioni di rete, affinché sia utilizzato da singoli lavoratori, su base regolare e/o occasionale. È assai diffusa la pratica che vede i telecentri fungere come infrastrutture di supporto alla comunità, in aree rurali, periferiche o economicamente svantaggiate
Essi hanno lo scopo principale di stimolare lo sviluppo economico dell'area territoriale in cui sono dislocati. In questo modo, forniscono ai telelavoratori un'alternativa all'ufficio a casa e, nel contempo, evitano alle aziende l'onere di dover installare dei propri uffici satellite: è al telecentro che, in questo caso, viene imputato il compito di allestire un ufficio satellite.
L'*ufficio virtuale* è la forma estrema e più avanzata di telelavoro che vede tutto il personale di una società lavorare a distanza, comunicando attraverso la rete. La società, in questo caso, non ha più un ufficio centrale nel senso fisico del termine, ma è allocata, articolata e "distribuita" in uno spazio virtuale; le aziende virtuali possono collegare lavoratori non soltanto tra aree geografiche diverse dello stesso paese, ma anche tra paesi e continenti diversi.
Le particolari caratteristiche del telelavoro implicano che il lavoratore abbia delle competenze multidisciplinari, relative ai seguenti aspetti:

- tecnologico
- organizzativo
- normativo
- sindacale
- economico-finanziario

I **vantaggi** e gli **svantaggi** che il telelavoro implica per il **lavoratore**, per le **imprese** e per **la collettività** sono riassunti nella seguente tabella:

	Lavoratore	Imprese	Collettività
Vantaggi	• maggior flessibilità nella gestione del tempo • riduzione dei tempi per gli spostamenti • distribuzione delle responsabilità (il lavoro viene modularizzato, le responsabilità si riferiscono quindi ad ambiti più ristretti e più facilmente individuabili)	• riduzione dei costi generali per uffici • riduzione dei costi di viaggio • efficace gestione delle sedi periferiche • maggior flessibilità nell'impiego delle risorse umane	• miglioramento delle politiche occupazionali nelle aree marginali • strumento di politica ambientale e di riduzione del traffico • miglior gestione del tempo collettivo • ingresso nel mondo del lavoro di esponenti delle categorie deboli
Svantaggi	• isolamento sociale • rischio di emarginazione delle carriere • rischio di passare da un impiego a retribuzione fissa ad uno basato sulla produttività	• riorganizzazione dei carichi di lavoro • problemi di riservatezza del know-how aziendale • gestione del personale e misura della qualità del prodotto	• possibilità di sviluppo di doppio lavoro, del lavoro nero, ecc. • pericolo di una diffusa evasione fiscale • uscita dei lavoratori dal sistema di protezione sociale

6.1.5 Il computer nella vita quotidiana

Come testimoni dell'evoluzione tecnologia in atto, ci si può rendere conto di come gli strumenti informatici attualmente disponibili siano applicati in moltissimi aspetti della vita quotidiana.
Da un lato, infatti, l'elaboratore è usato per rendere più efficienti i servizi cui ognuno di noi accede. Per esempio:

- **supermercato** (casse intelligenti)
- **biblioteca** (sistemi automatizzati di prenotazione e consultazione)
- **ambulatorio** (base di dati per la gestione dei pazienti)
- **banca** (base di dati per la gestione dei conti, sportelli automatici, ecc)

Dall'altro le tecnologie informatiche avanzate permettono di accedere in modo sempre più semplice ed immediato a questi servizi.
In tale contesto diamo ora dei cenni riguardo ad un interessante utilizzo delle tecnologie viste: la *smart card*.
Una **smart card** o **carta intelligente** è simile ad un badge magnetico cui è stato aggiunto un piccolo "computer" dotato di CPU e memoria propria; il sistema operativo della scheda è cablato nell'area di memoria a sola lettura (ROM), a ciascuna smart card è associato un codice PIN che ne abilita l'uso. Le *smart card* permettono l'autenticazione di azioni (ordini di pagamento, trasmissione di documenti importanti come i referti medici) per mezzo di uno strumento *crittografico* denominato *firma elettronica*; in questo modo non solo è possibile risalire al mittente del messaggio ma ogni modifica dello stesso viene automaticamente rilevata. Della firma elettronica si parlerà più avanti nell'ambito della *sicurezza dei dati*.
E' previsto, nei prossimi anni, l'utilizzo della smart card per l'unificazione delle varie tessere magnetiche (benzina, bancomat, carta di credito) e l'automazione di documenti riservati e non (carta d'identità, certificati elettorali ecc.); in tal modo questa costituirà un ausilio nella fruizione di servizi pubblici e privati.

6.1.6 Computer ergonomia e salute

La diffusione dei computer negli ambienti lavorativi ha portato il legislatore ad intervenire nel merito, inserendo in un decreto più generale (**Decreto Legislativo 19 settembre 1994 N° 626**) anche specifici riferimenti all'ambito informatico.
Il Decreto, che si occupa del miglioramento della sicurezza e della salute dei lavoratori nei luoghi di lavoro, introduce nell'ordinamento giuridico italiano diverse novità.
Una di queste è quella che riguarda i principi ***ergonomici***, la necessità cioè di realizzare condizioni di lavoro che rispondano ai più moderni criteri di tutela della salute e del benessere dei lavoratori (per ***ergonomia*** si intende la scienza che *studia il miglior modo di strutturare un ambiente di lavoro al fine di non danneggiare la salute del lavoratore*).
Questa esigenza si rileva in modo esplicito od implicito, in diversi articoli delle nuove norme di prevenzione.
Va innanzitutto ricordata la lettera f) del primo comma dell'articolo 3, che include tra le misure generali di tutela, all'osservanza delle quali i diversi soggetti sono tenuti, quella del "rispetto dei principi *ergonomici* nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, anche per attenuare il

lavoro monotono e quello ripetitivo"; come detto il decreto si occupa anche della protezione dei lavoratori contro i rischi derivanti dal lavoro ai videoterminali, in particolare nel Titolo VI, art.52 e seguenti.
Sono presi in considerazione i fattori del lavoro con il computer e le precauzioni da adottare; nello specifico vengono regolamentati:

- obblighi del datore di lavoro
- organizzazione del lavoro
- svolgimento quotidiano del lavoro
- sorveglianza sanitaria
- informazione e formazione
- consultazione e partecipazione
- adeguamento alle norme
- prescrizioni minime per attrezzature e ambiente

L'allegato VII della stessa legge fissa inoltre le prescrizioni minime per le attrezzature e l'ambiente nelle situazioni di lavoro che prevedono l'utilizzo di computer; in tal senso l'allegato fa proprie e regolamenta, relativamente ai lavoratori che interagiscono con i sistemi di elaborazione, una serie di regole derivanti dagli studi condotti sulle migliori mutue posizioni tra operatore e computer e sulle condizioni ambientali più adeguate.
Fattori da considerare sono:

- altezza da terra dei vari componenti
- posizione dello schermo (dai 40 ai 60 cm più in basso degli occhi)
- illuminazione ambientale (va evitata la luce solare diretta quindi le finestre devono essere dotate di opportuni dispositivi regolabili, i terminali devono essere attrezzati con schermi antiriflesso)
- calore (le attrezzature non devono produrre un eccesso di calore che possa costituire fonte di disturbo per i lavoratori)
- radiazioni (tutte le radiazioni, fatta eccezione per la parte visibile dello spettro elettromagnetico, devono essere ridotte a livelli trascurabili dal punto di vista della tutela della sicurezza e della salute dei lavoratori)
- umidità (deve essere ottenuta e mantenuta un umidità soddisfacente)
- rumore stampanti (la tecnologia attuale rende un po' superato questo fattore, comunque il rumore non deve perturbare l'attenzione e la comunicazione verbale)

Nella legge, ad esempio viene chiarito che il datore di lavoro deve controllare:

" *a) i rischi per la vista e per gli occhi;*
b) i problemi legati alla postura ed all'affaticamento fisico e mentale;
c) le condizioni ergonomiche e di igiene ambientale ."

Inoltre:

"*il lavoratore comunque ha diritto ad una pausa di quindici minuti ogni centoventi minuti di applicazione continuativa al videoterminale*"

Oltre alla legge e comunque opportuno osservare delle regole di buon senso relative a:

- cavi elettrici collegati in modo sicuro
- prese di corrente non sovraccaricate
- abbagliamento dello schermo
- errate posture

6.2 Impatto sociale

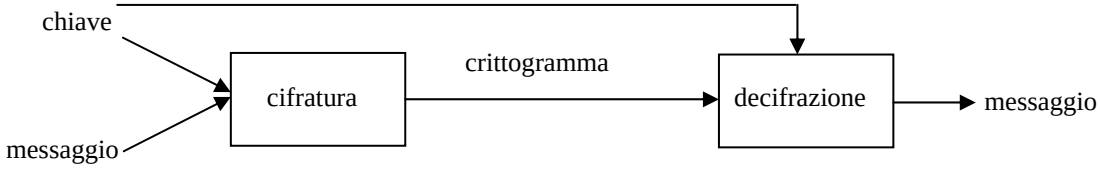
6.2.1 Sicurezza dei dati e delle transazioni

Si è parlato dei vantaggi legati all'avvento delle nuove tecnologie, si è anche accennato ai rischi quali, per esempio, la possibile emarginazione legata al fenomeno dell'analfabetismo tecnologico. Si prendono ora in considerazione altre problematiche: quelle legate all'accesso ai dati.
Gli archivi di dati possono essere usati da diverse tipologie di utenti: il progettista deve quindi preoccuparsi di definire chi e a che livello può accedere ai dati. Questo implica la necessità dell'esistenza di una responsabilità centralizzata in grado di distribuire le autorizzazioni e le modalità di accesso.
In generale ad ogni *utente* viene associato un **profilo** il cui accesso è controllato mediante **password**; al profilo sono associate una serie di azioni, di permessi e di divieti relativi all'utente stesso.
Questi controlli vengono realizzati a diversi livelli: gestione delle basi di dati, sistemi operativi, reti di utenti; per esempio una *password* è richiesta per la connessione da casa al *provider internet* o per entrare in un'area di servizi a cui l'utente è abilitato ad accedere gratuitamente o dietro pagamento di un canone.
Quando (al primo accesso ad una rete, ad una base di dati ecc.) un gestore chiede all'utente di scegliersi una *password*, devono essere seguiti dei criteri per sceglierla ed utilizzarla nel miglior modo possibile, ovvero:

- La *password* deve essere la più *lunga* possibile
- La *password non* deve essere in alcun modo *collegata* alla vita privata dell'utente (soprannomi, diminutivi, date di nascita ecc.)
- La *password non* deve essere una *parola comune* riportata in un vocabolario
- La *password non* deve venire *scritta* da nessuna parte

Il numero di reti in uso in tutto il mondo aumenta di giorno in giorno, e molte fra queste si connettono direttamente o indirettamente a Internet. Tale collegamento apre nuove possibilità di accesso alle informazioni, di commercio e di produttività ma espone la rete al rischio di attacchi o furti: Internet è un mezzo decisamente insicuro per comunicare e quindi sono stati inventati, oltre a quanto sopra specificato relativamente alle password, vari **sistemi crittografici** allo scopo di proteggere il contenuto delle comunicazioni e\o di autenticare l'identità del mittente di un messaggio.
In un **sistema crittografico** il *testo in chiaro*, o messaggio, viene *trasformato* seguendo opportune regole nel *testo cifrato* o **crittogramma**; l'operazione di trasformazione si dice **cifratura**. Il *crittogramma* viene quindi spedito attraverso la rete, che come già detto è

insicura; lungo il percorso, infatti, una "spia" potrebbe intercettare il *crittogramma* e tentare di *decifrarlo*. Anche il destinatario *decifra* il *crittogramma* riottenendo il *testo in chiaro*, se il sistema è ben progettato la decifrazione deve risultare semplice per il destinatario, di difficoltà insormontabile per la spia.
Questo è possibile poiché il destinatario conosce certe informazioni che devono rimanere inaccessibili alla spia, e quindi non devono essere trasmesse per mezzo della rete sulla quale "viaggia" il *crittogramma* che è insicura; queste informazioni costituiscono la **chiave** del cifrario.
Il **sistema crittografico** appena descritto viene detto **a chiave segreta**, lo schema è:



Dalla figura si nota che la chiave, pur segreta, deve essere comunicata al destinatario, per mezzo di un canale speciale "sicuro"; perché allora non inviare tutto il messaggio su tale canale? Le dimensioni delle chiavi sono di norma più ridotte di quelle del messaggio e l'uso del canale speciale, non soggetto ad intercettazioni, potrebbe essere costoso o lo stesso potrebbe essere disponibile per intervalli di tempo troppo brevi per trasmettere l'intero messaggio ecc. Si intuisce come il problema della *distribuzione delle chiavi* sia di importanza cruciale per il buon funzionamento di un *sistema crittografico*; il problema della *distribuzione delle chiavi* viene risolto con una innovazione radicale rispetto a quella vista: i **sistemi crittografici a chiave pubblica.**
Con questa tecnologia la chiave di cifratura è un'informazione pubblica, esistono quindi degli elenchi nei quali accanto al nome dell'utente compare la chiave; il più noto sistema a chiave pubblica è il sistema RSA (Rivest-Shamir-Adleman) originariamente sviluppato dal governo degli Stati Uniti.
La **firma elettronica** combina la tecnologia a chiave privata con quella a chiave pubblica; la situazione di riferimento è la seguente: un mittente deve spedire un documento ed il destinatario deve essere certo che il documento è l'originale spedito da quel preciso mittente; lo scopo viene ottenuto utilizzando appunto la *firma elettronica*.
I *programmi di firma* generano la firma digitale utilizzando un processo a due passi; per prima cosa il programma passa il file da trasmettere attraverso una funzione matematica pubblica che associa al file un numero (per esempio si potrebbe contare quante vocali ci sono al terzo posto in ogni parola del testo, dividerle per sette ed estrarne la radice quarta, cfr. Fig.1).

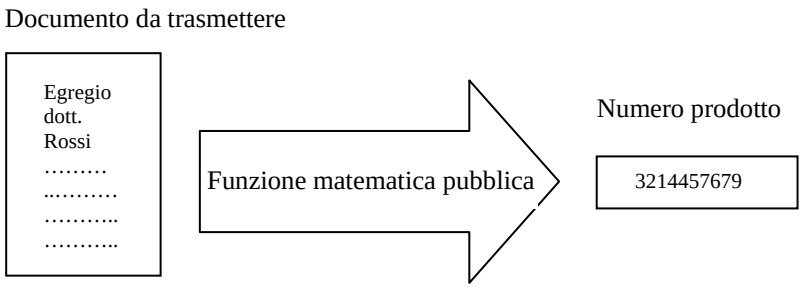


Fig. 1 – generazione numero dal documento da trasmettere

Risulta evidente che questa funzione calcola il numero in modo che non sia possibile ottenere il contenuto del file conoscendo la funzione; dopo aver creato il numero questo viene crittografato utilizzando la *chiave privata* (memorizzata nella scheda e non nota pubblicamente), producendo la *firma elettronica*, che verrà spedita assieme al testo in chiaro (Fig. 2).

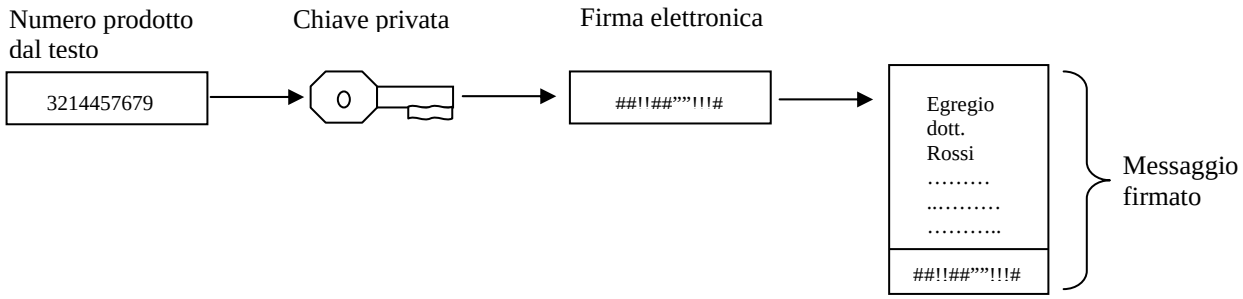


Fig. 2 – il programma inserisce la firma nel file

Per verificare la firma, il programma del destinatario esegue un software che decifra il numero associato alla firma utilizzando la chiave pubblica del mittente (Fig. 3.1);

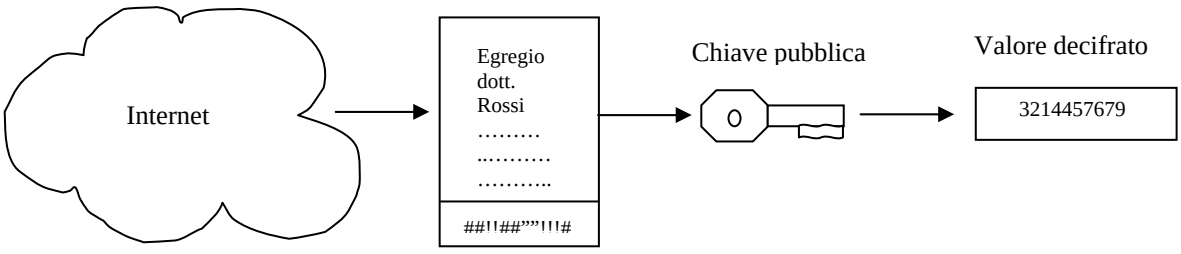


Fig. 3.1 – il destinatario utilizza la chiave pubblica del mittente per decifrare il valore della firma

in un secondo momento passa il testo che gli è stato trasmesso attraverso la stessa funzione matematica utilizzata dal mittente, che come già detto è nota (Fig. 3.2).

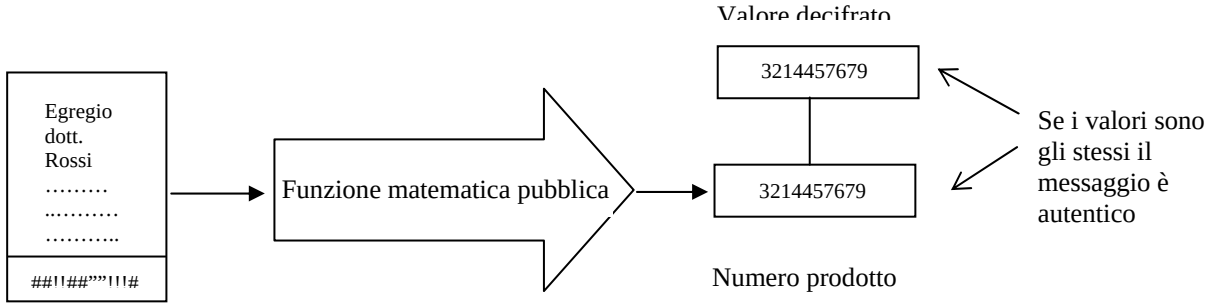


Fig. 3.2 – il calcolo e il confronto dei valori

Se il numero così ottenuto coincide con quello decifrato il programma informa il destinatario che il documento ricevuto è l'originale spedito dal vero mittente; quando i numeri non coincidono può essersi verificata una delle due situazioni:

a) il testo è stato modificato da un "estraneo", visto che la firma è autentica (il numero ottenuto con la funzione dal testo è errato quello decifrato è esatto).

b) La firma è falsa: chi ha spedito il messaggio non conosceva la chiave privata, visto che il testo ricevuto è quello spedito (il numero decifrato dalla firma è errato, quello ottenuto con la funzione dal testo è esatto)

Si noti che non è possibile per il destinatario sapere quale delle due situazioni si sia verificata; in ogni caso il documento trasmesso non è valido.

6.2.2 Virus ed hacker

La diffusione esponenziale delle utenze telefoniche domestiche dedicate alla trasmissione dati ha reso se non più importante, visto che le aziende da anni studiano metodologie per la difesa dei dati, sicuramente molto più sentito il problema dagli attacchi al computer che provengono dalla rete.
I **virus** sono programmi così denominati poiché sviluppati con lo scopo di:

- infettare altri programmi, inserendosi in essi
- rendersi in qualche modo visibili
- autoriprodursi nell'ambiente in cui sono inseriti e danneggiare la macchina infettata o danneggiare altre macchine ad essa connesse

Gli effetti di un *virus* si concretizzano in azioni che questo compie sui computer infettati; le azioni possono essere solo dimostrative, come la comparsa di un messaggio sul video, o produrre effetti gravi, come la distruzione di dati e programmi, o addirittura la formattazione dell' hard disk.
La protezione contro i virus può essere realizzata attraverso il controllo sistematico di tutti i supporti usati e attraverso il controllo degli accessi alla rete; esistono società specializzate nella ricerca ed identificazione dei *virus* e nella produzione di programmi che li rimuovono: l'utente acquista un programma antivirus (che eseguito identifica e, se li riconosce, elimina i *virus*), si abbona ad un servizio e periodicamente scarica dalla rete gli aggiornamenti che contengono le definizioni degli ultimi *virus* scoperti.
Purtroppo non sempre è possibile eliminare i *virus* senza intaccare il programma, a volte a questo scopo è necessario addirittura cancellare il programma infettato; diventa pertanto fondamentale prevenire i *virus* con un lavoro di filtro sugli accessi, sui dati e sul software.
A questo scopo ai pacchetti antivirus spesso sono abbinati i **firewall** (letteralmente, muri di fuoco): *software di protezione* che si appoggiano a un computer (o un insieme di computer) posto sul "confine" telematico (ad esempio sul *gateway*) tra una rete locale, o una sua parte "protetta", e il resto del mondo.
Gli **hacker** sono persone che si collegano, con sistemi di elaborazione, sfruttando i meccanismi della rete senza avere l'autorizzazione all'accesso; essi hanno il gusto della sfida, si divertono a scoprire i **bug** dei programmi e i punti deboli dei sistemi di protezione dei dati allo scopo di provare la propria abilità con il calcolatore e la propria intelligenza.
Ben diversi sono i **cracker**, ossia quelle persone che si dedicano alla pirateria informatica, rimovendo le protezioni dai programmi e distribuendone copie illegalmente, a scopo di lucro.

6.2.3 Diritti d'autore e Privacy

Nel corso degli anni l'utilizzazione dell'informatica ha investito tutti gli ambiti della vita sociale: il trattamento delle informazioni tramite l'elaboratore elettronico è utilizzato negli uffici pubblici, nelle aziende, negli ospedali ecc.
E' chiaro come sorgano una serie di nuovi problemi giuridici relativi al trattamento di questi dati; di seguito si analizzeranno brevemente i problemi dei **diritti d'autore** e della **privacy**.
Come tutte le opere d'ingegno anche i programmi informatici sono **protetti** dalla **legge sul *diritto d'autore*** (o meglio da una sua modifica effettuata con **D.L. n.518 del 29/12/1992**) e non possono essere quindi usati o riprodotti senza autorizzazione; esistono comunque delle categorie di software che, per concessione dell'autore, non risentono della completa applicazione della legge sul copyright.
Si distinguono i programmi:

- *Public Domain* (**PD**): i programmi distribuiti come PD sono liberi da ogni vincolo di copyright: l'autore li mette a disposizione di chiunque rinunciando ai propri diritti
- **Freeware**: questi programmi sono copiabili e utilizzabili gratutitamente da chiunque, ma l'autore mantiene su di essi i propri diritti (nel senso che sono usabili ma non modificabili)

- **Shareware**: questa è la categoria più grande, i programmi che ne fanno parte possono essere copiati liberamente (molti autori incoraggiano a farlo) ma possono essere utilizzati esclusivamente allo scopo di valutarne la validità in vista di un eventuale acquisto (possono avere una data di scadenza dopo la quale non sono più utilizzabili a meno che non si paghi una quota oppure possono permettere di svolgere solo alcune funzioni tra tutte quelle previste dai programmi che, se ritenuti validi, possono essere acquistati)

I moderni elaboratori consentono di raccogliere un numero praticamente illimitato di dati ed informazioni; queste informazioni, che già da sole permettono di avere un quadro completo e particolareggiato relativo ad una data persona, possono essere diffuse attraverso Internet.
La rete è aperta a tutti e quindi il diritto alla riservatezza corre maggior rischio di essere leso rispetto al passato; in tutti i paesi è sorto il problema di identificare e disciplinare mezzi efficaci di tutela della **privacy** delle persone rispetto al trattamento dei dati.
In Europa la disciplina della tutela alla riservatezza è stata affrontata a partire dalla **Convenzione Europea del 1981** e successivamente, con la **Direttiva dell'Unione Europea 95/46/CE del 24/10/1995** "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*": i Paesi membri furono invitati a recepirne le indicazioni in apposite leggi nazionali.
L'Italia ha attuato questa direttiva comunitaria con la **Legge n.675 del 31/12/1996**, questa è stata poi modificata dal **D.L. 382 del 30/07/1999** che regolamenta l'uso dei dati personali negli archivi elettronici.
Con la **Legge n. 547 del 23/12/1993** vengono stabilite le **pene** per i **reati informatici** che sono considerati dei veri e propri crimini elettronici ; per esempio **costituisce reato**:

- Violare la sicurezza di archivi e computer della rete
- Violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata
- Compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente

6.2.4 Netiquette

Fra gli utenti dei servizi telematici di Internet si sono sviluppate, visto che non esistono autorità superiori che regolino la comunicazione, una serie di "tradizioni" e di "principi di buon comportamento" (galateo) che vanno collettivamente sotto il nome di **"netiquette"** (da *net*, rete, ed *etiquette*, buone maniere).
La regola principale da seguire è quella della cortesia, che non consiste tanto nel rispetto formale delle buone maniere, quanto soprattutto nella considerazione e nell'attenzione per gli altri e per se stessi: nulla di dissimile da quanto ci si propone anche nelle forme più tradizionali di comunicazione.
Esempi di regole sono i seguenti:

- Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto

- Non pubblicare mai, senza l’esplicito permesso dell’autore, il contenuto di messaggi di posta elettronica
- Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state sollecitate in modo esplicito
- Essere sintetici, evitando informazioni inutili o poco pertinenti: per messaggi più lunghi usare la funzione *allegato*
- Usare regolarmente un programma antivirus, soprattutto quando si scaricano file dalla rete
- Non lasciare mai in rete materiale delicato o personale come informazioni riservate proprie o di altre persone
- Rispettare i diritti d’autore: non lasciare in rete le parole di un testo; imparare piuttosto a parafrasarle