

14 La crittografia per la sicurezza dei dati

La comunicazione di dati riservati o le transazioni commerciali richiedono garanzie per quanto riguarda l'invulnerabilità dei dati trasmessi. Per questo sono stati sviluppati i protocolli e le tecniche che possano fornire una valida risposta alle esigenze di sicurezza in rete.

L'adozione di soluzioni adeguate ai problemi connessi con la sicurezza, che possano essere applicate in modo semplice e senza la necessità di risorse eccessive, può dare sicuramente un impulso alla diffusione di Internet in tutte le attività.

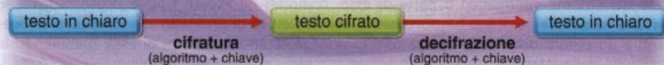
La **crittografia** è la tecnica che consente di rendere visibili le informazioni soltanto alle persone a cui sono destinate.

Per esempio, in una comunicazione, i messaggi trasmessi tra gli interlocutori vengono crittografati per renderli illeggibili tranne che agli interlocutori stessi.

La crittografia è nota fin dall'antichità e si è sviluppata, nel corso del tempo, soprattutto in campo militare, basandosi generalmente su algoritmi matematici.

Il messaggio che può essere letto da tutti si chiama **testo in chiaro**. Tramite i metodi di **cifratura** (codifica) si trasforma il testo in chiaro in un **testo cifrato** in cui l'informazione viene codificata e resa illeggibile. L'operazione inversa, chiamata **decifrazione** (decodifica), serve per ricostruire il testo in chiaro a partire dal testo cifrato.

La codifica e la decodifica sono eseguite da uno o più **algoritmi crittografici**. Questi algoritmi implementano le funzioni matematiche e vengono utilizzati insieme a una **chiave**, solitamente un numero molto grande. Un sistema di crittografia usa gli algoritmi crittografici e la chiave per codificare e decodificare i testi in chiaro.



La paternità dell'invenzione della crittografia è attribuita a Giulio Cesare che, durante le battaglie, spediva i dispacci usando i simboli alfabetici che differivano di una costante nota (chiave) dall'alfabeto naturale.

Se per esempio la chiave è 3, l'algoritmo crittografico di Giulio Cesare prende tutte le occorrenze della lettera A (posizione 1 nell'alfabeto) e le sostituisce con la lettera D (posizione 4 nell'alfabeto), la B con la E, la C con la F e così via fino alla Z con la C.

ABCDEFGHIJKLMNOPQRSTUVWXYZ



DEFGHILMNOPQRSTUVWXYZABC

Supponendo di avere come testo in chiaro le parole "GIULIO CESARE" la codifica con chiave 3 genera il seguente testo cifrato: "LNAOR FHVDUH".

Chi riceve il messaggio cifrato, per poter risalire al messaggio originale, deve conoscere la chiave usata. A questo punto applica l'opportuno algoritmo di decodifica e sostituisce le lettere usando il valore della chiave segreta.

Questo sistema di crittografia è noto con il nome di **cifrario a sostituzione**.

Un altro sistema di crittografia è il **cifrario a trasposizione**, in cui la chiave (una parola) serve per spezzare il messaggio su più righe e successivamente per ordinare le colonne risultanti ottenendo il testo cifrato. Con questa tecnica, non si sostituiscono le lettere del messaggio originale, ma si scambiano in modo opportuno per rendere illeggibile il messaggio.

Supponiamo di voler cifrare il seguente testo in chiaro usando come chiave la parola *vince*.

Messaggio: *la cavalleria deve attaccare sull'ala sinistra*.

Si crea una tabella con un numero di colonne uguale al numero di caratteri della parola chiave, e successivamente si posiziona sulla prima riga la parola chiave. I caratteri del messaggio vengono distribuiti sulle righe sottostanti, sotto ogni lettera della parola chiave.

V	I	N	C	E
L	A	C	A	V
A	L	L	E	R
I	A	D	E	V
E	A	T	T	A
C	C	A	R	E
S	U	L	L	A
L	A	S	I	N
I	S	T	R	A

Se l'ultima riga non è completa, si aggiungono dei caratteri di riempimento, per esempio il carattere *.

Il messaggio cifrato viene generato prendendo le colonne della precedente tabella secondo l'ordine alfabetico delle lettere della parola chiave, cioè prima la colonna C, poi la E, la I, la N e la V.

Il testo cifrato è *AEETRLIRVRVAEANAALAACUASCLDTALSTLAIECSLI*, ottenuto accodando correttamente le colonne nel seguente modo:

AEETRLIR	VRVAEANA	ALAACUAS	CLDTALST	LAIECSLI
C	E	I	N	V

Il destinatario del messaggio cifrato, conoscendo la parola chiave, è in grado di ricostruire il messaggio individuando le colonne e posizionandole nell'ordine corretto all'interno della tabella.

Opposte alla crittografia si sono sviluppate tecniche di **crittoanalisi** con lo scopo di analizzare e cercare di violare le comunicazioni cifrate. Chi si occupa di crittoanalisi conosce il testo cifrato e deve riuscire a decifrarlo senza conoscere l'algoritmo crittografico e la chiave. In alcuni casi l'algoritmo crittografico è noto e la difficoltà sta nel trovare la chiave.

L'algoritmo di Giulio Cesare non è un buon algoritmo per garantire la sicurezza dei messaggi, perché può essere violato molto facilmente anche non conoscendo la chiave. Se il crittoanalista conosce il testo cifrato e sa che l'algoritmo utilizzato è quello di Giulio Cesare, può provare in modo esaustivo tutte le chiavi finché non ottiene il testo in chiaro. La ricerca esaustiva può essere eseguita perché il numero di chiavi da provare è piccolo, infatti con l'alfabeto italiano ci sono 21 possibili chiavi.

15 Chiave simmetrica e chiave asimmetrica

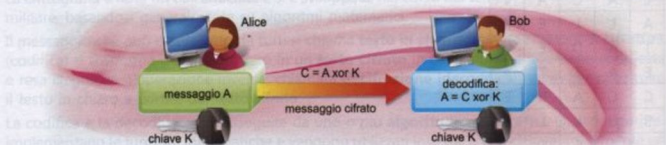
Le tecniche crittografiche possono essere classificate in due principali sistemi: a chiave simmetrica e a chiave asimmetrica.

La **crittografia a chiave simmetrica** è un sistema di codifica convenzionale nel quale viene utilizzata una sola chiave per cifrare e decifrare i messaggi. Il mittente e il destinatario devono possedere la stessa chiave per potersi scambiare i messaggi in modo sicuro.

Il cifrario a sostituzione, usato da Giulio Cesare, è un esempio di crittografia a chiave simmetrica. Un semplice esempio di chiave simmetrica è rappresentato dal metodo che effettua la codifica e la decodifica sulla base della considerazione che applicando due volte l'operatore **XOR** si ottiene il messaggio di partenza

$$(A \text{ xor } K) \text{ xor } K = A$$

L'operatore XOR produce un valore vero (1) quando i valori di verità delle due proposizioni sono opposti e un valore falso (0) quando i valori di verità sono uguali.



Indicando con A il messaggio da trasmettere (in binario), con K la chiave privata e con C il messaggio cifrato, si ha:

A	1 1 0 0 1 1 0 1 0
K	1 0 1 1 1 0 0 0 1
C	0 1 1 1 0 1 0 1 1
C xor K	1 1 0 0 1 1 0 1 0

Crittografare un messaggio, componendolo in XOR con una chiave segreta, non è un buon sistema di crittografia, perché, come si può verificare dall'esempio, la chiave K è ricavabile con la relazione: $K = A \text{ xor } C$.

La chiave utilizzata può essere interpretata come un numero molto grande e la sua dimensione viene misurata in numero di bit: più grande è la chiave e più difficile sarà il compito di chi vuole infrangere i messaggi cifrati.

Per esempio se la chiave è lunga 10 bit esistono 2^{10} differenti chiavi, se la chiave è lunga 20 bit esistono 2^{20} differenti chiavi e così via. Si deduce che il numero delle chiavi è esponenziale rispetto alla lunghezza in bit della chiave stessa. Questo significa che, per decifrare un messaggio provando tutte le chiavi tramite una ricerca esaustiva, si devono eseguire un numero esponenziale di prove rispetto alla lunghezza della chiave.

Con una chiave di 40 bit, chi volesse decifrare i messaggi dovrebbe cercare tra 2^{40} possibili chiavi, cioè tra circa 10^{12} possibili chiavi. Supponendo di provare una chiave ogni millisecondo, servirebbero 10^9 secondi, cioè circa 10^4 giorni. Ma un normale personal computer è in grado di testare anche 10^8 chiavi ogni secondo, per cui la chiave verrebbe trovata in 10^4 secondi (meno di 3 ore). Una chiave di 128 bit è ritenuta sicura.

Un sistema crittografico a chiave simmetrica molto conosciuto è il **DES** (*Data Encryption Standard*), sviluppato da IBM nel 1977. Questo sistema utilizza una chiave di 56 bit. Per rendere più sicuro il DES, è stato realizzato il **Triple-DES** (o 3DES) che lavora con una chiave di maggiori dimensioni.

Altri sistemi crittografici più recenti sono **CAST**, sviluppato da *Nortel*, e **IDEA** (*International Data Encryption Algorithm*), sviluppato in Svizzera nel 1990. Entrambi usano una chiave a 128 bit. Nei sistemi di crittografia a chiave simmetrica, la segretezza della chiave è il fattore principale per garantire la sicurezza delle comunicazioni. Il problema di questo sistema crittografico è rappresentato dalla distribuzione sicura delle chiavi, cioè dallo scambio sicuro della chiave tra mittente e destinatario. Infatti, se qualcuno venisse in possesso di questa chiave segreta, potrebbe decifrare le comunicazioni.

La **crittografia a chiave asimmetrica**, chiamata anche *crittografia a chiave pubblica*, è stata introdotta nel 1975 con l'obiettivo di risolvere il problema della distribuzione sicura delle chiavi. Il termine asimmetrica si riferisce al fatto che il sistema utilizza una coppia di chiavi:

- una **chiave pubblica**;
- una **chiave privata**.

Le due chiavi sono correlate matematicamente, per cui i messaggi codificati con la chiave pubblica possono essere decodificati soltanto da chi possiede la chiave privata, e viceversa. La particolarità e la forza di questo sistema crittografico è che, anche conoscendo la chiave pubblica, non è possibile risalire alla corrispondente chiave privata se non con calcoli che richiedono tempi molto elevati.

La coppia di chiavi viene generata da un software opportuno. Ogni persona che vuole ricevere i messaggi cifrati deve fornirsi di una coppia di chiavi: la chiave privata viene tenuta segreta, mentre la chiave pubblica viene distribuita liberamente a tutte le persone con cui si vuole comunicare.

Diverse combinazioni nell'uso delle chiavi pubbliche e private determinano diversi livelli di sicurezza nella comunicazione dei messaggi. Si possono considerare le seguenti situazioni:

a) Garanzia dell'identità del mittente

Il mittente di un messaggio, Alice, usa la propria chiave privata per codificare il messaggio. Il destinatario, Bob, utilizza la chiave pubblica di Alice per decifrare il messaggio.

È garantita l'identità di Alice, ma nulla impedisce a una qualunque persona di leggere il messaggio di Alice, essendo disponibile a tutti la sua chiave pubblica.



b) Garanzia della segretezza

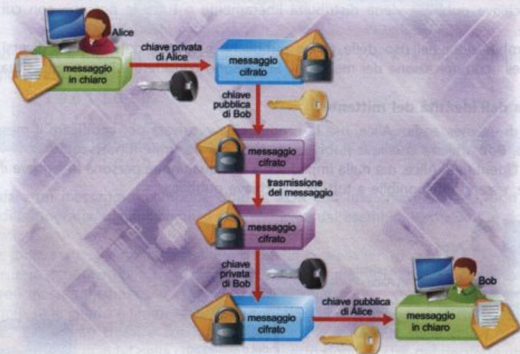
Alice conosce la chiave pubblica di Bob e la può usare per codificare il messaggio. Il testo cifrato può essere decodificato soltanto da Bob, perché è l'unica persona che possiede la chiave privata correlata con la chiave pubblica con cui è stato cifrato il messaggio. Bob, essendo in possesso di questa chiave privata e segreta, può leggere il messaggio dopo averlo decifrato.



La lettura del messaggio è consentita solo a Bob, ma non c'è nessuna garanzia sul fatto che il messaggio provenga proprio da Alice, perché chiunque potrebbe utilizzare la chiave pubblica di Bob e inviare un messaggio cifrato.

c) Garanzia dell'identità e della segretezza

Alice prima effettua la codifica del messaggio usando la sua chiave privata, nota solo a lei. Il risultato di questa codifica viene ulteriormente codificato usando la chiave pubblica di Bob. Al ricevimento del messaggio cifrato, Bob è in grado di decifrare il messaggio una prima volta usando la propria chiave privata e successivamente può anche decifrare il risultato ottenuto con la chiave pubblica di Alice.



Bob ha la garanzia che il messaggio provenga da Alice, perché solo Alice possiede la chiave privata; nello stesso tempo Bob è l'unica persona in grado di decifrare il messaggio, perché possiede la chiave privata correlata con la chiave pubblica utilizzata da Alice.

In questa terza situazione si ha anche una garanzia dell'integrità del messaggio, cioè che il messaggio non sia stato modificato da altri durante la trasmissione, perché la codifica alla partenza è stata fatta da Alice con la sua chiave privata.

Il vantaggio del sistema crittografico a chiave asimmetrica è che il mittente e il destinatario non devono condividere una chiave segreta. I mittenti dei messaggi devono solo conoscere la chiave pubblica del destinatario, mentre la chiave privata deve essere conservata in modo segreto dal destinatario.

Utilizzare un algoritmo crittografico a chiave asimmetrica.

Un algoritmo crittografico a chiave asimmetrica è **RSA** (dalle iniziali dei creatori: Rivest, Shamir, Adleman, 1978). Questo algoritmo si basa sulla difficoltà di fattorizzare i numeri molto grandi, anche di trecento cifre (10^{300}).

In questo sistema crittografico la chiave pubblica è composta da due numeri (*pub*, *n*), serve per codificare i messaggi e deve essere resa pubblica. Anche la chiave privata è composta da due numeri (*pri*, *n*), serve per decodificare i messaggi e deve essere mantenuta segreta.

Supponendo di avere a disposizione le precedenti chiavi, per cifrare un testo in chiaro con RSA si deve usare la seguente funzione:

$$c = m^{\text{pub}} \bmod n$$

m rappresenta un carattere (o meglio un blocco) del messaggio in chiaro trasformato in forma numerica binaria, mentre *c* rappresenta la versione codificata. Il simbolo *mod* è l'operatore *modulo* e calcola il resto della divisione.

Per decodificare il testo cifrato con RSA si deve usare la seguente funzione:

$$m = c^{\text{pri}} \bmod n$$

Il metodo per costruire le chiavi pubbliche e private consiste nello scegliere due numeri primi grandi *a*, *b*. A partire da questi numeri si calcola il valore di *n* e *z* nel seguente modo:

$$n = a \cdot b;$$

$$z = (a-1) \cdot (b-1).$$

Il valore *n* rappresenta il secondo numero della coppia di chiavi.

Il primo numero della chiave privata *pri* viene scelto in modo tale che non abbia fattori in comune con *z*.

Il primo numero della chiave pubblica *pub* viene scelto in modo tale che soddisfi la seguente equazione:

$$(\text{pub} \cdot \text{pri}) \bmod z = 1.$$

Il seguente esempio numerico mostra come viene costruita una coppia di chiavi usando l'RSA. Si scelgono inizialmente due numeri primi $a=17$ e $b=5$ (i numeri sono piccoli per rendere semplice la spiegazione). A partire da questi valori si ottiene che $n=85$ e $z=64$. Si sceglie $\text{pri}=5$ perché non ha fattori in comune con z e successivamente si sceglie *pub* in modo che $(\text{pub} \cdot 5) \bmod 64 = 1$. Si ottiene $\text{pub}=13$.

Riassumendo la chiave pubblica è (13, 85) mentre la chiave privata è (5, 85).

Utilizzando la precedente chiave pubblica si possono cifrare i messaggi in modo tale che possano essere decifrati soltanto da chi conosce la chiave privata.

Il seguente esempio mostra come cifrare la parola "EUROPA" usando la chiave pubblica (13, 85). L'operazione di codifica considera una lettera per volta *m* trasformata in forma numerica binaria ($A=1, \dots, Z=21$) e applica la funzione $m^{\text{pub}} \bmod n$, cioè $m^{13} \bmod 85$.

Testo in chiaro	<i>m</i>	m^{13}	$m^{13} \bmod 85$
E	5	1220703125	20
U	19	42052983462257059	49
R	16	4503599627370496	16
O	13	302875106592253	13
P	14	793714773254144	39
A	1	1	1

Il testo cifrato corrisponde alla sequenza di numeri 20, 49, 16, 13, 39, 1.

Soltanto chi possiede la chiave privata (5, 85) può decifrare il messaggio applicando la funzione $c^5 \bmod n$ dove c rappresenta il carattere cifrato.

Testo cifrato (c)	c^5	$c^5 \bmod 85$	Testo in chiaro
20	3200000	5	E
49	282475249	19	U
16	1048576	16	R
13	371293	13	O
39	90224199	14	P
1	1	1	A

Nelle applicazioni pratiche, i numeri utilizzati per le chiavi sono molto più grandi e la codifica non avviene carattere per carattere, ma per blocchi di caratteri.

16 La firma digitale

La **firma digitale** è un metodo elettronico che permette a una persona di apporre un segno distintivo ai documenti digitali. I requisiti della firma digitale sono:

- **autenticità**, per garantire l'identità della persona che ha sottoscritto il documento;
- **integrità**, per essere sicuri che il documento non sia stato modificato dopo la sottoscrizione;
- **non ripudio**, cioè il documento sottoscritto con firma digitale ha piena validità legale e non può essere ripudiato dal sottoscrittore.

Quindi il documento elettronico è un messaggio che il mittente firma in modo digitale e spedisce al destinatario. Quest'ultimo, dopo aver ricevuto il messaggio, può verificare, controllando la firma digitale se il messaggio ha origine dal mittente e se è stato modificato durante la trasmissione. La firma digitale viene realizzata usando i sistemi di crittografia a chiave asimmetrica. In questo caso, il ruolo delle chiavi è diverso rispetto al loro utilizzo per la codifica dei messaggi destinati al possessore della chiave privata. Una persona firma un documento usando la sua chiave privata, mentre le altre persone, che vogliono controllare l'autenticità e l'integrità, usano la chiave pubblica.

A partire dal documento, viene generata un'**impronta** (*fingerprint*), cioè una sequenza binaria di lunghezza fissa (128 o 160 bit) che rappresenta un **digest** (riassunto) del documento. L'impronta viene generata usando una particolare funzione, chiamata **funzione di hash**, con la garanzia che a partire da documenti diversi si ottengono impronte diverse. Questa impronta viene poi codificata utilizzando la chiave privata e il risultato rappresenta la **firma digitale**.

La firma così costruita viene accodata al documento in chiaro.



Le fasi per controllare la veridicità del documento sono:

1. usare la chiave pubblica del firmatario per decifrare l'impronta;
2. avendo il testo in chiaro e usando la stessa funzione di *hash*, calcolare l'impronta del documento;
3. se le due impronte coincidono significa che il documento è stato firmato dalla giusta persona ed è integro, cioè non è stato modificato.



Dopo l'apposizione della firma digitale, ogni modifica al documento comporta una modifica nell'impronta associata. Avendo a disposizione l'impronta originale contenuta nella firma digitale, si può rapidamente controllare se il documento è stato modificato. Si osserva che la firma digitale è diversa per ogni documento diverso, a differenza della firma autografa. La firma digitale, per questo motivo, offre il valore aggiunto dell'integrità.

La coppia di chiavi pubblica e privata, usate per firmare e verificare i documenti, deve essere rilasciata da un **ente di certificazione** (*Certification Authority*) che garantisce l'identità del possessore della chiave.

La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica è indicata con il termine **titolare**.

Uno strumento pratico e sicuro per conservare la chiave privata è rappresentato dalle schede **smart card**, simili per forma e dimensioni a una tradizionale carta di credito e protette da PIN (*Personal Identification Number*) di accesso.

La smart card viene collegata al computer attraverso un apposito lettore ed è gestita con un software che consente di apporre la firma digitale ai documenti elettronici.

Il destinatario può avere la garanzia sull'identità del mittente e nello stesso tempo ottenere la sua chiave pubblica attraverso il **certificato digitale** emesso e firmato dall'ente certificatore.

Il certificato è redatto secondo uno standard riconosciuto (*formato X.509*) e contiene:

- numero di serie del certificato
- ragione e denominazione sociale del certificatore
- nome, cognome e data di nascita del titolare delle chiavi
- valore della chiave pubblica
- algoritmi di generazione e di verifica
- inizio e fine del periodo di validità delle chiavi.

Quindi, in pratica, il destinatario riceve una **busta elettronica** contenente il documento, la firma digitale e il certificato con la chiave pubblica.

L'estensione **p7m** indica uno dei formati standard per i documenti firmati digitalmente (sistema di crittografia **pkcs #7**, *Public-Key Cryptography Standards*).

A questo punto il documento è pronto per essere inviato al destinatario. Il destinatario deve **verificare l'autenticità e l'integrità del documento**. Si possono usare software che sono in grado di aprire e verificare i documenti firmati: per esempio il software **Dike** di *Infocert* (www.firma.infocert.it).

Se il destinatario possiede il software *CRS Manager* per la tessera regionale CRS, lo può utilizzare per controllare e visualizzare il documento: clic sul pulsante **Verifica un documento firmato** nella finestra iniziale del programma (figura di pagina precedente).

The screenshot shows the 'Verifica firma' application window. It displays a file named 'LetteraConferma.pdf.p7m' and provides options to view original documents and certificates used in the signature. A callout '1' points to the 'Sfoga...' button. Callout '2' points to the 'Mostra certificato' button. Callout '3' points to the 'Certificati utilizzati nella firma' section. Callout '4' points to the 'Certificato' dialog box, which shows details like 'Rilasciato da: Regione Lombardia Certification Authority Cittadini 2' and 'Valido dal: 31/ 07/ 2010 al 31/ 07/ 2016'. The 'Attività' pane at the bottom left shows a successful verification log.

Clic per selezionare il file da verificare.

Clic per visualizzare le informazioni sulla Certification Authority e sul mittente.

Il software verifica il documento e visualizza l'esito del controllo.

Clic per conoscere le informazioni su validità, identificativi e algoritmi di crittografia utilizzati.

Quindi il software di gestione della CRS può essere utilizzato sia per firmare un documento attraverso la chiave privata contenuta nella tessera, sia per verificare un documento ricevuto.

• I programmi PGP

Il software più conosciuto per la crittografia a chiave asimmetrica è **PGP** (*Pretty Good Privacy*), ideato da Phil Zimmermann nel 1991. Questo programma consente di generare automaticamente le coppie di chiavi pubbliche e private, oltre che di cifrare e decifrare messaggi e di firmare digitalmente i messaggi di posta elettronica.

• Protocollo SSH

Il protocollo **SSH** (*Secure SHell*) permette di stabilire una connessione sicura con un computer remoto.

In effetti il protocollo consente anche di generare coppie di chiavi asimmetriche e di inviare o ricevere file cifrati. Genera una coppia di chiavi pubblica e privata usando il metodo RSA.

• Protocolli SSL e TLS

Il protocollo **SSL** (*Secure Sockets Layer*) gestisce la protezione delle comunicazioni nel Web, cifrando i messaggi che transitano sulla rete Internet. Risulta quindi particolarmente adatto per le connessioni nelle quali si devono fornire dati sensibili e nelle transazioni commerciali in rete. Fornisce inoltre garanzie sul sito a cui ci si collega.


L'evoluzione di SSL si chiama **TLS** (*Transport Layer Security*).


• Protocollo HTTPS


Il protocollo HTTP, supportato dal protocollo SSL o TLS, è indicato come protocollo **HTTPS**, che indica la comunicazione sicura di dati e informazioni sul Web.

Immagine del lucchetto nella casella dell'indirizzo.

L'indirizzo del sito Web inizia con **https://...**, anziché con **http://...**

 <https://accounts.google.com>

 **accounts.google.com**
L'identità di questo sito web è stata verificata da Thawte SGC CA.
[Informazioni certificato](#)

 La connessione a accounts.google.com è protetta con crittografia a 128-bit.

La connessione utilizza TLS 1.0.

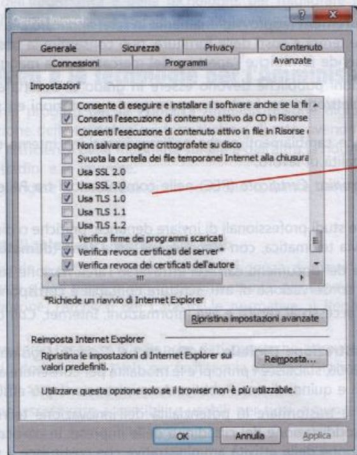
La connessione è stata crittografata utilizzando RC4_128, con SHA1 per l'autenticazione dei messaggi e ECDHE_RSA come meccanismo principale di scambio delle chiavi.

La connessione non è compressa.

Facendo clic sul lucchetto si ottengono le informazioni sul certificato digitale dell'azienda o dell'ente, con il quale si garantisce l'identità del sito Web.



Si può controllare la configurazione SSL e TLS del browser: per esempio in *Internet Explorer*, nel menu *Strumenti*, selezionare *Opzioni Internet* e poi, nella scheda *Avanzate*, verificare le impostazioni.



Segno di spunta su entrambe le caselle: Usa SSL 3.0 e Usa TLS 1.0.

Esercizi da 16 a 22 pag. 271

17 L'e-government

Il termine **e-government** indica l'utilizzo e l'applicazione delle tecnologie informatiche nelle amministrazioni centrali e periferiche dello Stato, con l'obiettivo di rendere la **Pubblica Amministrazione (PA)** più veloce, trasparente, efficiente e accessibile ai cittadini.

In questo contesto le reti e Internet hanno un ruolo centrale. È possibile prevedere che i prossimi sviluppi portino alla disponibilità di strumenti informatici e di rete per il coinvolgimento dei cittadini, con la partecipazione democratica e l'espressione del voto elettronico (**e-democracy**).

L'e-government riguarda:

- l'erogazione di servizi efficienti;
- l'identificazione digitale del cittadino o dell'impresa da parte dello Stato;
- lo scambio di informazioni;
- il miglioramento dei rapporti normativi e fiscali;
- la semplificazione delle procedure amministrative;
- la formazione del personale;
- l'approvvigionamento di beni o servizi.