Firma digitale
Profili applicativi

Prof. ing. Pierluigi Ridolfi

- **Cifratura di documenti riservati**
- **Commercio elettronico**
- **Archiviazione ottica**
- **Protocollo informatico**
- **Atti notarili**
- **Fisco telematico**
- **Processo telematico**
- **Problemi aperti**

Sistemi a doppia cifratura

Si utilizzano per cifrare messaggi "lunghi" (documenti riservati oppure transazioni finanziarie o commerciali).

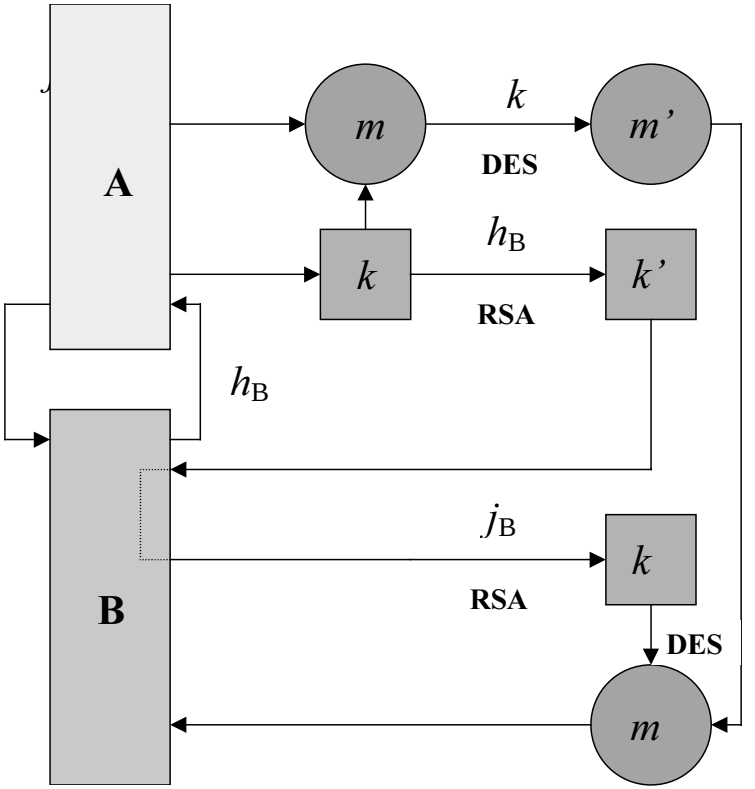
$\Rightarrow$ Si cifra il messaggio con il DES.

$\Rightarrow$ Si cifra la chiave del DES con RSA.

Principio della doppia cifratura

- A deve inviare a B un messaggio *m*, non breve.
- A sceglie a caso una chiave *k*, di 64 bit.
- A cifra (con il DES) *m* mediante la chiave $k \Rightarrow m'$.
- A cifra *k* con $h_B \Rightarrow k'$
- A invia a B *m'* e *k'*
- B decifra *k'* con $j_B \Rightarrow k$
- B decifra (con il DES) *m'* con *k* $\Rightarrow m$

Schema di funzionamento



Commento sulla sicurezza

- I **sistemi a due chiavi** offrono le maggiori garanzie, ma richiedono elaborazioni complesse: è difficile applicarli se il messaggio è lungo.
- I **sistemi a una chiave** offrono minori garanzie, ma richiedono elaborazioni semplici: la lunghezza del messaggio è in pratica ininfluente.
- L'utilizzo combinato di entrambi i sistemi ("**doppia cifratura**") offre il massimo della sicurezza insieme a una relativa semplicità di elaborazione, qualunque sia la lunghezza del messaggio.

Commercio elettronico

- A: acquirente, con accesso a Internet.
- B: venditore, con catalogo in Internet.
- A sceglie e attiva la transazione.
- B fornisce ad A h_B.
- Il PC di A automaticamente:
  - prepara l'ordine elettronico *m*
  - genera una chiave *k* con cui cifra (DES) *m* $\Rightarrow m'$
  - cifra *k* con $h_B \Rightarrow k'$
  - invia *m'* e *k'* a B
- Il computer di B automaticamente:
  - decifra *k'* con $j_B \Rightarrow k$
  - con *k* decifra *m'* e ottiene l'ordine *m*
- B spedisce la merce.

Pagamento con carta di credito (schema teorico)

CC indichi la Società della Carta di credito.

- A consulta il catalogo di B, sceglie la merce da acquistare, fornisce i dati della propria Carta di credito e attiva la transazione.
- Il PC di A automaticamente:
  - prepara l'ordine elettronico senza i dati della Carta di credito e lo invia a B;
  - prepara la nota di debito con i dati della Carta di credito e con riferimento a B; cifra questa nota con un sistema di doppia cifratura e la invia a CC.
- CC decodifica la nota di debito, effettua i controlli rituali, contabilizza l'addebito su A e l'accredito su B, comunica a B il buon esito contabile dell'operazione.
- B riceve il messaggio da CC ed evade l'ordine.

Sistema sicuro ma informaticamente complesso (2 collegamenti indipendenti).

Pagamento con carta di credito (schema reale 1a)

Protocollo SSL
(*Secure Socket Layer*)

- Sviluppato da Netscape e utilizzato anche da Microsoft.
- All'atto del collegamento tra A e B si realizza un complesso sistema di reciproco riconoscimento.
- *m* contiene sia i codici della merce sia le coordinate della carta di credito.
- *m* viene cifrato da A con un sistema a doppia cifratura.
- *m* viene inviato a B.
- L'inoltro delle coordinate della carta di credito a CC è a cura del venditore B.

Osservazioni sulla sicurezza

Pro

- *k* viene generata presso il mittente A, cambia ad ogni transazione e non esce dal PC di A.
- A è sicuro di ordinare merce da un fornitore B affidabile, la cui garanzia è fornita indirettamente da CC.
- B è sicuro di ricevere tramite CC il corrispettivo della merce spedita.

Contro

- B viene a conoscere le coordinate della carta di credito di A: la sicurezza del sistema pertanto è anche in funzione dell'etica di B, non valutabile a priori.

Pagamento con carta di credito (schema reale 1b)

Variante del precedente

- *m* contiene sia i codici della merce sia le coordinate della carta di credito.
- *m* viene cifrato da A con un sistema a doppia codifica.
- *m* viene inviato a CC.
- L'inoltro dell'ordine al venditore B è a cura di CC.

$\Rightarrow$ Scompaiono i contro.

Pagamento con carta di credito (schema reale 2)

Protocollo SET

(*Secure Electronic Transaction*)

- Sviluppato su iniziativa di Visa e Mastercard (CC).
- Le coordinate della carta di credito sono prima cifrate con la chiave pubblica di CC poi affiancate ai codici della merce: il tutto forma il messaggio *m*, che viene cifrato con h_B .
- B al ricevimento di *m'* estrae le coordinate della carta di credito - che sono cifrate - e le invia a CC.
- CC le decifra e autorizza B a spedire la merce.

Osservazioni sulla sicurezza

Pro

- A è sicuro di ordinare merce da un fornitore B affidabile, la cui garanzia è fornita indirettamente da CC.
- B è sicuro di ricevere il corrispettivo della merce spedita.
- B non viene a conoscere le coordinate della carta di credito di A: la sicurezza del sistema pertanto dipende solo dell'etica di CC, che si presume altissima.

Contro

- Sistema nuovo, complesso, in corso di diffusione.

Aspetti innovativi del commercio elettronico

- Mercato vasto quanto il mondo.
- Spese di marketing centralizzate sul sito Internet.
- Spese di distribuzione centralizzate sulla spedizione: efficienza del sistema di consegna.
- Fiducia nel processo.
- Banche come “garanti”.

Tipi di commercio elettronico

- Business to Business
  - aziende comprano tra loro
  - ricerca di prodotti via Internet
  - pubblicità: sito Internet efficace
  - inviti a gare
  - effettuazione di gare
- Business to Customer
  - acquisti al dettaglio
  - pubblicità: occorre arrivare al sito $\Rightarrow$ banner e/o pubblicità tradizionale

Archiviazione ottica

- **DPR 445/00, art. 6 comma 2:**

  "gli obblighi di conservazione e di esibizione di documenti per finalità amministrative e probatorie si intendono soddisfatti anche se realizzate mediante supporto ottico, purché le procedure siano conformi a regole tecniche dettate dall'AIPA"

- **Deliberazione AIPA 42/01**

  "Regole tecniche per l'uso di supporti ottici"

Tipi di archiviazione

- **Archiviazione ottica**:

  riversamento su supporto ottico non riscrivibile di documenti formati in origine su supporto informatico.

- **Archiviazione ottica sostitutiva:**

  trasformazione degli archivi cartacei in archivi digitali e successiva loro archiviazione ottica.

Vantaggi

- Drastica riduzione del consumo di carta.
- Minor occupazione di spazi per l’archiviazione fisica.
- Circolazione dei documenti e loro accesso più facili.
- Risparmio di tempi nell’attività amministrativa.

Controlli

- La sequenza di bit che rappresenta i documenti, insieme alla marca temporale, va firmata digitalmente da chi effettua l’operazione di archiviazione.
- Garanzia di autenticità, integrità e tempificazione.

Autenticazione

- I documenti cartacei originali che vanno su supporto ottico devono essere autenticati da un Pubblico ufficiale. Tale formalità si intende assolta attraverso la firma digitale del Pubblico ufficiale .

- Per i documenti in copia, basta la firma digitale del file di chiusura a cura del dirigente responsabile.

Protocollo informatico

Una nuova strategia per la gestione dei documenti della P.A.

- Riorganizzazione e concentrazione degli uffici di protocollo $\Rightarrow$ **Aree Organizzative Omogenee**.
- Creazione di nuovi **servizi per la tenuta del protocollo** e la gestione degli archivi.
- Adozione di precisi **standard di protocollo** (identici per tutte le amministrazioni).
- Adozione di un nuovo **sistema di classificazione e fascicolazione**.
- Rivisitazione delle attuali procedure informatiche ai fini interoperabilità e accesso da parte dei cittadini/utenti.

Basi normative

- DPR 428/98 “Regolamento per la tenuta del protocollo amministrativo con procedura informatica”
  ⇒ DPR 445/00 “Testo Unico in materia di documentazione amministrativa”
- DPCM 31/10/00 “Regole tecniche per il protocollo informatico”
- Circolare Aipa n. 28 del 7/5/01 “Standard, ecc.”
- Rivolte a tutta la pubblica amministrazione.

Cosa si intende per P.A.

- le amministrazioni dello Stato;
- le aziende e le amministrazioni dello Stato ad ordinamento autonomo;
- le regioni, le province, i comuni, le comunità montane;
- i consorzi e le associazioni dei predetti enti;
- gli istituti autonomi case popolari;
- le camere di commercio, industria, artigianato e agricoltura, e le loro associazioni;
- gli enti pubblici non economici;
- gli istituti e le scuole di ogni ordine e grado e le istituzioni educative;
- le istituzioni universitarie;
- le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale.

Punti focali

- Aree Organizzative Omogenee (AOO)
- Nucleo minimo del protocollo informatico
- Nuovo sistema di classificazione e archiviazione

Aree Organizzative Omogenee (AOO)

- Un insieme di unità organizzative che usufruiscono degli stessi servizi per la gestione dei flussi documentali.
- Evitare attuali frammentazioni (protocolli di reparto, di settore, ecc.)
- All'interno di un'AOO un solo servizio di protocollazione con un'unica sequenza numerica (rinnovata annualmente).
- Obiettivi: risparmio di risorse, maggiore facilità di ricerca e di accesso ai documenti, miglior organizzazione dell'archivio.

Nucleo minimo del protocollo informatico

- La componente del sistema del protocollo informatico in grado di effettuare le operazioni di:
  - registrazione
  - segnatura
  - classificazione
- Sono le operazioni necessarie e sufficienti per la tenuta del sistema di gestione automatica dei documenti da parte di un'amministrazione.

Registrazione (1)

- La registrazione di un documento spedito consiste nella memorizzazione su supporto informatico, in modo permanente e non modificabile, di:
  - n. protocollo e data registrazione del documento (generati dal sistema);
  - destinatario;
  - oggetto;
  - impronta (se inviato per via telematica).
- Prima della registrazione l'operatore all'AOO deve controllare che il documento abbia una corretta firma elettronica da parte del mittente.

Registrazione (2)

- La registrazione di un documento ricevuto consiste nella memorizzazione su supporto informatico, in modo permanente e non modificabile, di:
  - n. protocollo e data registrazione del documento;
  - mittente;
  - oggetto;
  - impronta (se ricevuto per via telematica).
- Prima della registrazione l'operatore all'AOO deve controllare che il documento abbia una corretta firma elettronica da parte del mittente.

Documento e impronta

- L'impronta garantisce l'integrità del documento.
- L'impronta va sempre associata ai dati di protocollo.
- L'impronta può non essere associata al documento trasmesso (in quanto il ricevente la può calcolare).

Segnatura

- La segnatura di protocollo consiste nell'associare al documento, in modo permanente e non modificabile, come minimo le seguenti informazioni:
  - codice dell'amministrazione;
  - codice dell'AOO;
  - numero di protocollo;
  - data di protocollo.
- L'operazione di segnatura è contemporanea a quella di registrazione.

Classificazione

- Attività che consente di organizzare tutti i documenti prodotti da un'AOO secondo uno schema articolato di voci logiche (*piano di classificazione*).
- È una caratteristica di ogni singola amministrazione.

Fascicolazione

- Attività di riconduzione logica di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti.
- Fascicoli, dossier: $\Rightarrow$ cartelle elettroniche.

Commenti

- Si tratta di una normativa di tipo generale (linee guide con standard).
- Ogni amministrazione deve rivedere le procedure esistenti per tener conto delle nuove normative.
- Specifiche strutture di coordinamento all'interno di ogni amministrazione.
- Organismo di coordinamento generale presso la Presidenza del Consiglio dei ministri.
- Data obiettivo: 1 gennaio 2004.

Atti notarili

- **Notartel**: rete informatica che collega i 5 mila studi notarili italiani.
- Rete privata che offre particolari garanzie.
- Collegamento con altre Reti:
  - Catasto
  - Conservatorie
  - Cancellerie
  - Camere di Commercio
- Ricevimento e trasmissione di atti per via telematica, sottoscritti con firma digitale.

Fisco telematico

- Soluzione tecnica autonoma, non in linea con le norme sulla firma digitale.
- Soggetti abilitati a inviare dichiarazioni per via telematica.
- Requisiti di ogni soggetto (A):
  - PC con modem;
  - abilitazione Ministeriale;
  - programmi per la gestione delle procedure;
  - chiave $h_{A,}$ assegnata dal Ministero (su dischetto attivabile con PIN).
- Più dichiarazioni $\Rightarrow$ file.
- File + impronta cifrata con $h_A \Rightarrow$ Ministero per via telematica.
- Ministero decifra con j_A, verifica e rilascia ricevuta elettronica.

Problemi

- Concentrazione degli invii all'ultimo minuto potrebbe rendere impossibile la ricezione in tempo utile:

  $\Rightarrow$ ampio margine di tempo

- Autonomia garantita al Ministero Finanze potrebbe rendere impossibile il colloquio con le altre P.A.

  $\Rightarrow$ modifica delle norme

Norme (1)

- **Principio di autonomia:**

  DPCM 8/2/99: art 62, c. 3:

  "Restano salve le disposizioni contenute nel decreto del Ministero delle finanze 31 luglio 1998, concernenti le modalità tecniche di trasmissione telematica delle dichiarazioni, e le successive modificazioni e integrazioni."

Norme (2)

- **Principio di uniformità**

  DLgs 10/02, art. 9

  "Le istanze e le dichiarazioni inviate per via telematica [alla P.A.] sono valide:

  a) se sottoscritte mediante firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore **accreditato**, e generata mediante un dispositivo per la creazione di una firma sicura;

  b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi".

Norme (3)

- **Principio di transitorietà**

  DLgs 10/02, art. 12

  "Le disposizioni vigenti … che consentono di presentare per via telematica istanze o dichiarazioni alla pubblica amministrazione … secondo procedure diverse da quelle indicate nell'art. 9 continuano ad avere applicazione fino alla data fissata … con DPCM … comunque non posteriormente al 31/12/2005".

Processo telematico

- DPR 123/01:

  “Uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti”.

- Applicazione integrale delle norme sulla Firma digitale.

Struttura informatica

- **Dominio giustizia**: l'insieme delle risorse hardware e software, mediante il quale l'amministrazione della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura;
- **Sistema informatico civile**: il sottoinsieme delle risorse del dominio giustizia mediante il quale l'amministrazione della giustizia tratta il processo civile.
- Vengono assicurati:
  - l’individuazione dell’ufficio e del procedimento;
  - l’individuazione del soggetto in relazione all’atto;
  - l’avvenuta ricezione.

Campo d’applicazione

- È ammessa la formazione, la comunicazione e la notificazione di atti del processo civile mediante documenti informatici nei modi previsti dal DPR.

- L’attività di trasmissione, comunicazione o notificazione è effettuata per via telematica attraverso il sistema informatico civile oppure attraverso l’indirizzo “ufficiale” di posta elettronica del difensore (comunicato tramite l’Ordine).

Sintesi delle tecnologie applicate

Applicazione	**Tecnologie**			
	DES	***RSA***	***Impronta***	***Firma Digitale***
Sottoscrizione di documenti				sì
Trattamento di documenti cifrati	sì	sì		
Commercio elettronico	sì	sì		
Archiviazione ottica			sì	sì
Protocollo informatico			sì	
Atti notarili				sì
Fisco telematico		sì	sì	2006
Processo telematico				sì

Problemi aperti

- Pluralità di chiavi e di dispositivi di firma.
- Coesistenza di più standard.
- Area privata e area pubblica.
- P.A. centrale e periferica.
- Coesistenza e compatibilità con la carta di identità elettronica.
- Garanzia di quello che si firma.