# ALGORITMI CRITTOGRAFICI E FIRMA DIGITALE

# LA SICUREZZA INFORMATICA

Il progetto e la manutenzione della sicurezza dei dati e delle applicazioni nei sistemi informativi sono aspetti sempre più cruciali, sia a causa del progredire delle tecnologie, sia a seguito degli interventi legislativi che pongono precisi requisiti in materia di protezione delle informazioni. L' aspetto tecnologico vede continui progressi nei settori delle architetture, delle reti informatiche e delle applicazioni, che rendono disponibile, in maniera massiccia e veloce, una quantità enorme di informazioni a un gran numero di utenti.
L' aspetto legislativo ha visto vari interventi in materia di *privacy* e autenticazione della trasmissione di dati e documenti, ad esempio nella Pubblica Amministrazione.

Si può senz' altro affermare che la quantità e qualità dei dati quotidianamente affidati ai sistemi di gestione delle basi di dati (DBMS) o resi disponibili su reti e siti Web in sistemi distribuiti sono fattori vitali per il funzionamento delle aziende e delle istituzioni, e persino per la vita quotidiana di un qualunque cittadino.

I problemi della sicurezza nascono dal fatto che:

1. le reti sono per loro natura mezzi insicuri: in assenza di misure specifiche di protezione, la comunicazione avviene in chiaro (non cifrata), l' autenticazione degli utenti si basa semplicemente su password, non vi è in genere autenticazione dei server, le reti locali funzionano come mezzo di *broadcast*, e i collegamenti geografici non avvengono sempre tramite linee punto-punto ma attraverso linee condivise oppure tramite *router* di terzi;
2. le applicazioni, sia di sistema sia organizzative, possono contenere errori (accidentali e non) e *trapdoor* (scappatoie, botole) oppure *trojan horse* (codice malizioso che apparentemente svolge una certa funzionalità, ma che nel contempo copia/trasmette dati confidenziali) che possono essere utilizzati per vari scopi;
3. i dati tendono sempre più ad avere valore *semantico* (non sono semplicemente informazioni memorizzate su supporto magnetico) ed è pertanto necessario proteggerli in base al loro significato oltre che semplicemente proteggere l' accesso logico (delle applicazioni e degli utenti) e fisico ai file in cui sono memorizzati;
4. i dati sono condivisi fra vari utenti, su siti diversi in Rete, con politiche di protezione spesso contrastanti e occorrono *protocolli di negoziazione* fra le politiche di accesso alle basi di dati e ai siti Web, i quali permettano l' accesso controllato alle informazioni.

È quindi necessario garantire le seguenti quattro caratteristiche dei messaggi e dei dati:

1. ***confidenzialità:*** *protezione da letture non autorizzate;*
2. ***integrità:*** *protezione da modifiche non autorizzate;*
3. ***autenticità:*** *certezza della sorgente, della destinazione e del contenuto del messaggio;*
4. ***non ripudio:*** *certezza che chi trasmette e chi riceve non possano negare di avere rispettivamente inviato e ricevuto il messaggio.*

## CLASSIFICAZIONE DEI MECCANISMI DI SICUREZZA

I meccanismi di sicurezza utilizzabili si possono distinguere tra meccanismi *specifici* (*specific security mechanisms*) e meccanismi *pervasivi* (*pervasive security mechanisms*).

I meccanismi di sicurezza *specifici* sono:

- ***la crittografia,*** *per la confidenzialità dei dati;*
- ***la firma digitale,*** *per il non ripudio dei messaggi;*
- ***il controllo dell' accesso***
- ***l' integrità dei dati,*** *sia per le singole unità sia per le sequenze;*
- ***lo scambio dei dati di autenticazione,*** *attraverso un sistema di autenticazione ad esempio X.509 (PKI-Infrastruttura a chiave pubblica).*
- ***Il traffic padding,*** *che consiste nella generazione di traffico spurio per impedire attacchi basati sull' analisi dello stesso;*
- ***Il controllo di routing,*** *ossia dell' instradamento dei dati;*
- ***La notifica della ricezione da parte del destinatario.***

I meccanismi di sicurezza *pervasivi,* a differenza di quelli specifici, non sono caratteristici di un particolare servizio, ma riguardano aspetti globali della gestione della sicurezza di sistema. L' importanza di questi meccanismi è legata al livello di sicurezza che si vuole raggiungere.
Si possono individuare cinque meccanismi di sicurezza *pervasiva*:

- ***La trusted functionality,*** *concetto generale indicante che ogni funzionalità del sistema è controllata da meccanismi di sicurezza;*
- ***Le security labels,*** *dati aggiuntivi che vengono affiancati a quelli in transito nel sistema (ad esempio, chiavi pubbliche, firme o certificati);*
- ***La event detection,*** *che consiste nella segnalazione di ogni evento che possa portare al sospetto di una violazione di criteri di sicurezza;*
- ***Il security audit trail,*** *un' analisi a posteriori dei dati e dei log del sistema, alla ricerca di violazioni e dei possibili affinamenti delle politiche di sicurezza;*
- ***Il security recovery,*** *che consiste nell' applicare determinate regole nel caso si verifichino particolari eventi a carico del sistema.*

# TECNICHE DI SICUREZZA DEI DATI

## *LA CRITTOGRAFIA*

## *Che cos' è la Crittografia? E come viene applicata?*

La crittografia è la *scienza che si occupa di sviluppare metodi crittografici, ossia metodi finalizzati a nascondere il contenuto di un messaggio tramite l' uso di un "algoritmo" e di una "chiave".*

La crittografia dei dati è una tecnica utilizzata dall' uomo fin dall' antichità. Basti pensare, ad esempio, che Giulio Cesare era solito crittografare i messaggi da affidare ai suoi messi utilizzando un codice noto appunto con il nome di *Codice cifrato di Cesare.*

In questo tecnica l' algoritmo di crittografia consisteva nel traslare le lettere del messaggio originale di un numero di posizioni pari a *n (chiave di cifratura).* Supponendo *n=3,* le lettere *A, B, C, D* diventano rispettivamente *D, E, F, G.* Nonostante un malintenzionato possa conoscere l' algoritmo su cui si basa il Codice (in questo caso molto semplice), per decrittografare il messaggio deve conoscere la chiave (nel nostro caso: *n=3*).

Questo semplice esempio mostra anche come sia fondamentale, in un algoritmo di crittografia, fare in modo che la chiave sia scelta tra un vastissimo numero di combinazioni. Nel nostro esempio, la chiave può essere scelta tra 21 combinazioni possibili (le lettere dell' alfabeto italiano) e, conoscendo l' algoritmo di cifratura, non sarebbe dunque difficile risalire al messaggio originale.

La crittografia moderna utilizza due tipologie di algoritmi per crittografare:

- gli algoritmi a ***chiave segreta (o simmetrici),*** in cui la chiave per crittografare è la stessa utilizzata per decrittografare;
- gli algoritmi a ***chiave pubblica (o asimmetrici),*** in cui ogni parte in gioco nella comunicazione possiede due chiavi: una *chiave privata,* che conosce solo il possessore, e una *chiave pubblica,* che viene resa nota a tutti. Tali algoritmi son detti anche asimmetrici perché implementano due funzioni: una-diretta e molto semplice-per crittografare e l' altra-inversa e generalmente molto complicata-per decrittografare.

La crittografia è oggi lo strumento più utilizzato per garantire la *confidenzialità.* Solo ultimamente, con l' avvento della *firma elettronica* si è riusciti a garantire anche *integrità, autenticità* e *non ripudio* nella trasmissione dei dati.

## *Crittografia a chiave simmetrica o segreta.....*

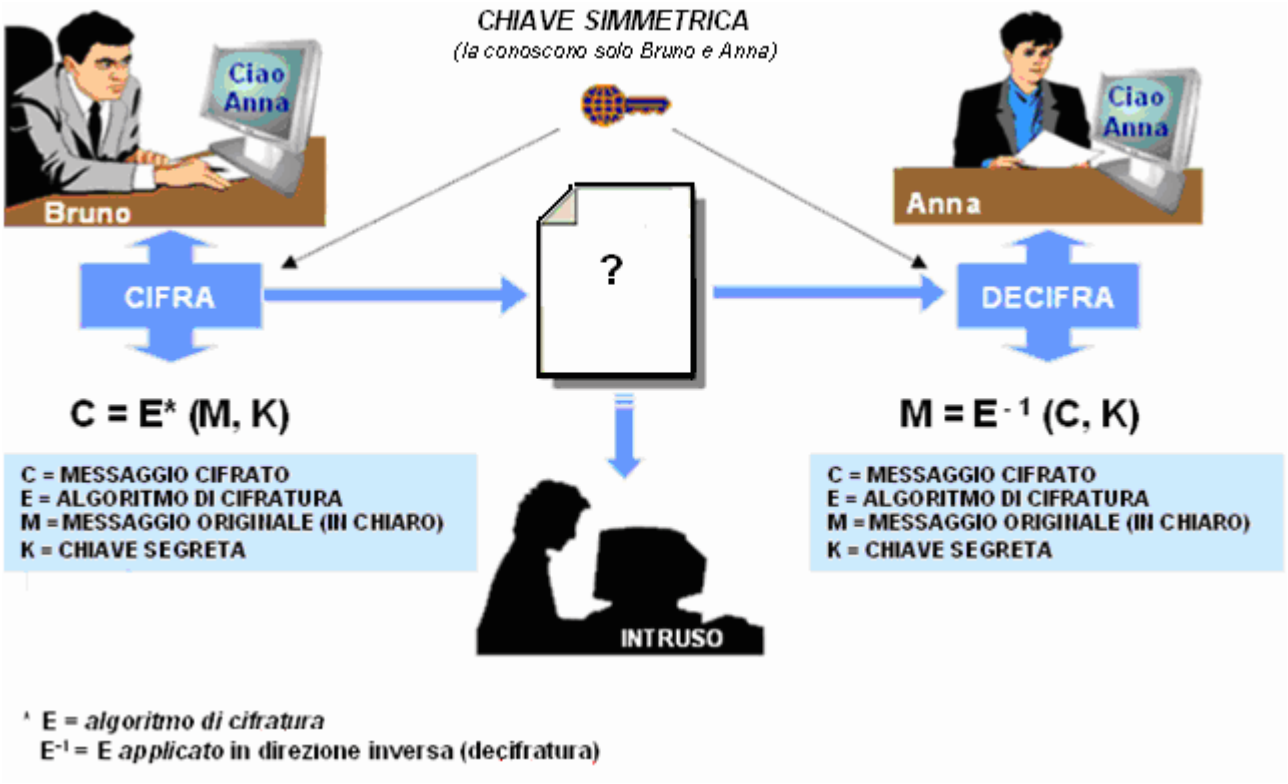
*Nella crittografia a chiave segreta (o comunemente chiamata "crittografia simmetrica" ) sono due i componenti fondamentali:*

- ***Algoritmo/funzione di cifratura:*** *procedura che* trasforma *il messaggio originale (messaggio in chiaro) in messaggio cifrato.*
- ***Chiave segreta (password o parola segreta):*** *è nota soltanto al mittente ed al destinatario del messaggio*

*È importante sottolineare il fatto che algoritmo e chiave sono imprescindibili in quanto* la trasformazione da messaggio in chiaro a messaggio cifrato (cifratura) è soltanto un procedimento che, per essere attuato, ha bisogno di un'informazione ulteriore (la chiave), da cui dipende fortemente il risultato.

Per decifrare il messaggio (decifratura), quindi, non basta conoscere l'algoritmo di cifratura utilizzato, ma è necessario conoscere anche la chiave (*vedi figura 1).*


***FIGURA 1. Crittografia simmetrica***




La crittografia a chiave segreta (o simmetrica) utilizza un' unica chiave (*secret key)* che deve necessariamente rimanere segreta e nota alle sole persone, o macchine, che si scambiano il messaggio. Ogni persona che ne entra in possesso è in grado di decrittografare il messaggio.

Il limite di questo tipo di crittografia consiste nel fatto che costringe gli interessati a comunicarsi la chiave, con il pericolo che questa possa cadere nelle mani sbagliate.

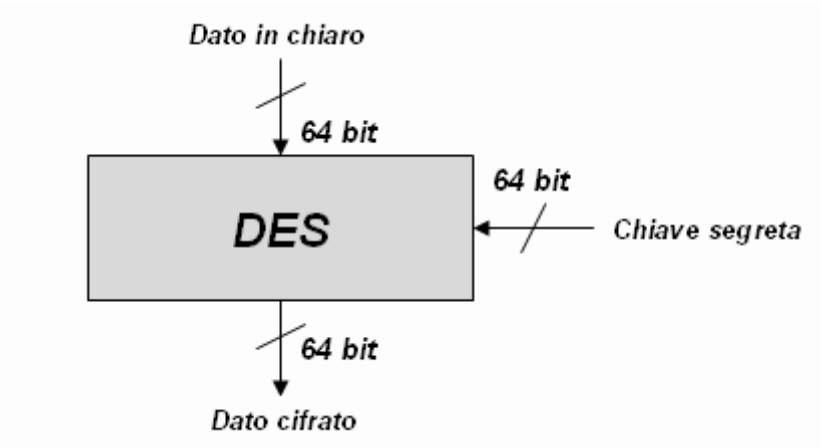
Per ovviare a questo fatto, nel 1976 venne proposto da Diffie e Hellman un algoritmo per lo scambio sicuro delle *secret key.*

Attualmente gli algoritmi a chiave simmetrica più diffusi sono: ***DES*** (utilizzato fin dalla fine degli anni Settanta dal Governo degli Stati Uniti e violato durante una sfida Internet), ***Triple DES, IDEA, RC2, RC4*** (utilizzati in browser come Netscape Navigator e Microsoft Internet Explorer). Alcuni di questi algoritmi sono stati pubblicati e verificati da famosi crittoanalisti; altri, proprietari, non sono resi pubblici e potenzialmente potrebbero contenere nel loro codice *bug* o *backdoor* che permettono di violarli

## L' ALGORITMO DES

Il *Data Encryption Standard (DES)* è stato considerato a partire dal 1977 uno standard per la crittografia per alcune decine di anni, dopo che diverse compagnie avevano fino a quel momento sviluppato in modo autonomo e incompatibile tra di loro diversi algoritmi di cifratura il cui grado di robustezza e di sicurezza non venivano divulgati.

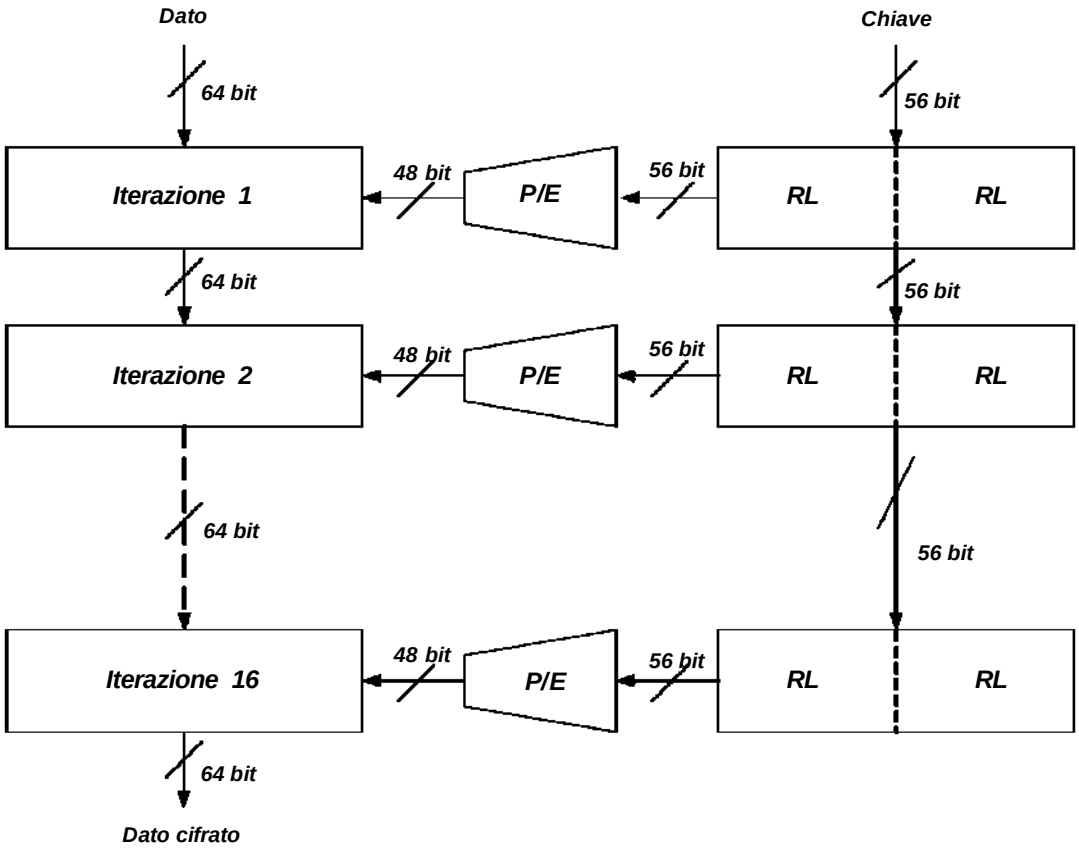
L' algoritmo DES è progettato per criptare e decriptare dati in blocchi di 64 bit.




Se il messaggio è più grande, lo si divide in tanti campi di 64 bit ciascuno; se è minore, i bit mancanti alla sinistra vengono completati con zeri. La chiave utilizzata è di 64 bit, di cui però, vengono presi in considerazione solo i primi 56.
Poiché le combinazioni su 56 bit sono circa $10^7$ , risulta praticamente impossibile, non conoscendo la chiave, ricostruirla per tentativi. Il sistema è così complesso che nemmeno conoscendo sia il messaggio da codificare sia quello codificato è possibile risalire alla chiave.

L' algoritmo DES utilizza blocchi di espansione/permutazione (***figura 1***) che modificano l' ordine e la quantità delle informazioni presenti in un blocco dati utilizzando tabelle come la ***Tabella 1***. Il numero in una casella indica la posizione del bit nel blocco di ingresso.

*Figura 1 - Schematizzazione del funzionamento dell' algoritmo DES*




In linea di massima l' algoritmo è composto da 16 iterazioni, dove sia il messaggio sia la chiave sono sottoposti a operazioni di permutazione, XOR bit a bit e shifting verso sinistra (quest' ultimo indicato dall' operatore RL).

*Tabella 1 – Esempio di tabella di Permutazione/Espansione da blocchi di 32 bit a blocchi di 48 bit*

| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

***Facciamo un esempio pratico per capire il funzionamento dell' algoritmo....***

*Utilizzando la **tabella 1**, ipotizziamo di avere la seguente stringa in ingresso*


*Il testo permutato/espanso in uscita è il seguente (mostrato su righe diverse per analogia alla tabella, ma che in realtà si presenta su un' unica riga):*

| | | | | | |
|---|---|---|---|---|---|
| A | M | I | C | H | E |
| H | E | L | A | | H |
| | H | A | | P | E |
| P | E | R | S | O | |
| O | | L | A | | S |
| | S | U | A | | B |
| | B | O | R | S | E |
| S | E | T | T | A | M |

Il sistema illustrato è quello effettivamente utilizzato nella maggioranza dei casi. Ne esistono però anche delle varianti, diffuse in settori particolari: molto frequente è quella denominata *Triple Des.*

## *Crittografia a chiave asimmetrica o pubblica.....*

Il concetto di crittografia a chiave pubblica ha rivoluzionato il mondo della crittografia. La sua potenzialità è insita nel fatto che ***non è necessario che le parti in comunicazione si scambino alcuna chiave,*** così come avviene invece per la crittografia a chiave segreta.

Ogni parte possiede infatti due chiavi:

- **Una pubblica** da distribuire a tutti quelli con cui vuole comunicare
- **Una privata** da tenere segreta.

Non è possibile risalire alla chiave privata (tenuta segreta dal proprietario) partendo dalla chiave pubblica (resa disponibile a tutti). L' algoritmo di crittografia è fatto in modo che quanto cifrato con la chiave pubblica possa essere decifrato solamente con la rispettiva chiave privata (***figura 2***) e, dualmente, quanto firmato con la chiave privata possa essere decriptato solo con la rispettiva chiave pubblica.

In questo caso le funzioni di criptazione e decriptazione sul testo in chiaro e su quello cifrato sono definibili dalle seguenti espressioni:

$$Testo\_Cifrato = Funzione\_di\_cifratura_{[chiave\ privata]}\ (Testo\_in\_chiaro)$$

$$Testo\_in\_chiaro = Funzione\_di\_decifratura_{[chiave\ pubblica]}\ (Testo\_Cifrato)$$

I due scenari di impiego della crittografia a chiave pubblica sono i seguenti:

Il mittente cripta il messaggio con la propria chiave privata; il destinatario, che conosce l' identità di chi gli invia il messaggio, lo decripta utilizzando la chiave pubblica del mittente. In questo contesto si garantiscono l' autenticazione del mittente e l' integrità del messaggio. Non è invece garantita la confidenzialità poiché la chiave pubblica del mittente è a disposizione di tutti, quindi tutti possono decrittografare il messaggio (meccanismo di ***firma digitale***);
(***figura 2***) Il mittente cripta il messaggio con la chiave pubblica del destinatario, che è nota a tutti; il destinatario riconosce che il messaggio è per lui e lo decripta con la propria chiave privata, nota solo a lui. Solo il destinatario, che conosce la chiave segreta corrispondente alla chiave pubblica utilizzata dal mittente, sarà in grado di leggere il messaggio. Così si garantisce la confidenzialità.

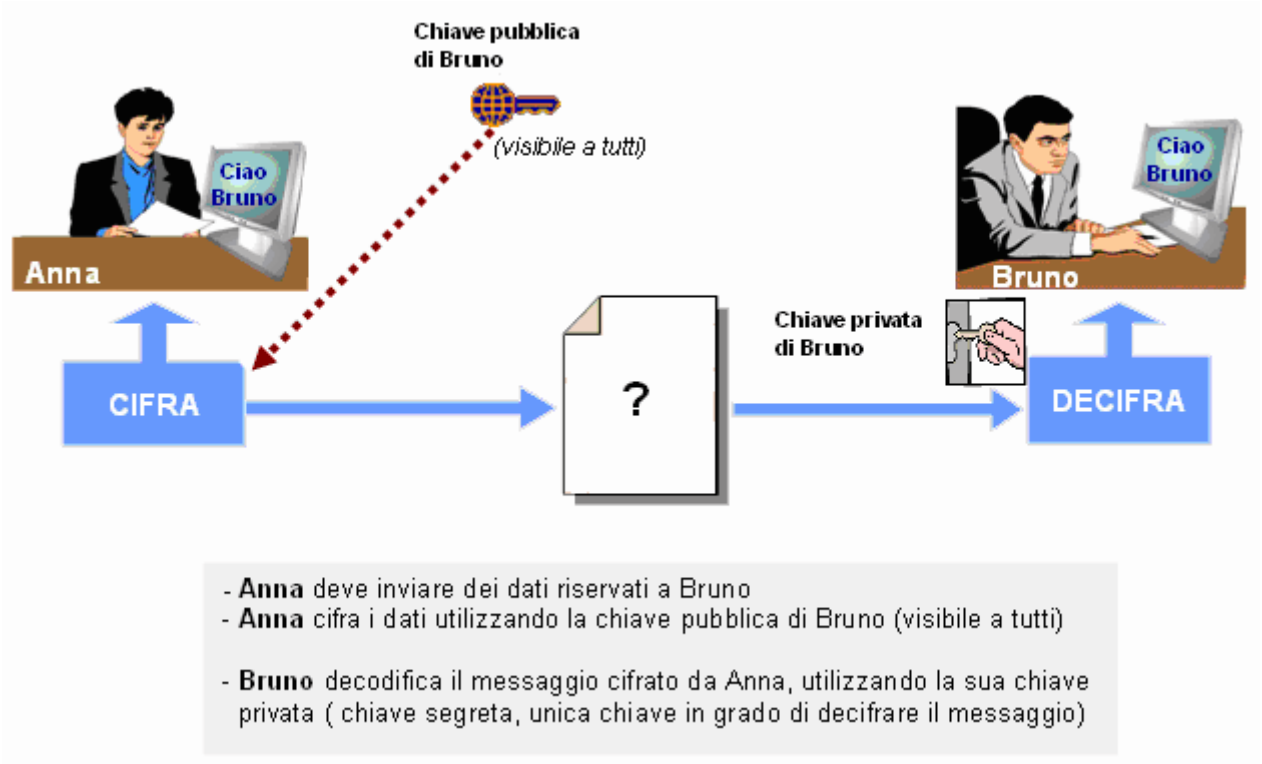
Questi due passaggi possono essere eseguiti sullo stesso messaggio in modo combinato, ottenendo in tal modo sia la confidenzialità sia l' integrità.



**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

Vediamo qualche esempio:


***FIGURA 2. Crittografia Asimmetrica***






**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

**Come fa il mittente a trovare la chiave pubblica del destinatario?**

Mittente e destinatario possono inviarsi le loro chiavi pubbliche tramite e-mail, telefono, fax, posta, possono incontrarsi di persona, ecc.

**Che cosa succede se qualcun altro vede la chiave pubblica?**

Nessun problema; è pubblica!

## Problemi di questo metodo

È interessante notare come gli algoritmi a chiave pubblica siano sensibilmente più lenti di quelli a chiave privata: infatti, confrontando le prestazioni, si scopre che il DES, nella realizzazione software, è almeno 100 volte più veloce di RSA, mentre nella realizzazione hardware si arriva a una differenza di velocità di circa 1000 o addirittura 10000 volte.

La soluzione a questo problema è stata:

**Combinare la cifratura a chiave simmetrica e la cifratura a chiave pubblica.**

La chiave “simmetrica” è veloce  e robusta (se la chiave è lunga)

La chiave “pubblica” è valida per lo scambio delle chiavi.

Gli algoritmi a chiave pubblica vengono utilizzati, solitamente, solo nella fase di *handshaking*, durante la quale le parti si scambiano una chiave detta “di sessione”  utilizzata per la crittazione dei dati durante la trasmissione da algoritmi a chiave segreta.

***Vediamo come vengono combinate....***

- Generiamo una chiave simmetrica, utilizzabile una sola volta (**chiave di sessione**)
- Cifriamo il messaggio con la chiave di sessione
- Cifriamo la chiave di sessione con la chiave pubblica del destinatario



**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni  Phone: +39.0744. 441214  Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it  Cap. Soc. € 2.750.000 i.v.  REA 89371  P.I .01339760553

***Dimostrazione:***


1. *Viene generata in maniera randomica una chiave di sessione.*
2. *Anna utilizza la suddetta chiave per cifrare il messaggio che deve inviare a Bruno*
3. *Bruno non è in grado di decifrare il messaggio senza conoscere la chiave di sessione utilizzata da Anna. Per questo motivo Anna invia sia il messaggio cifrato, sia la chiave di sessione. Quest' ultima viene cifrata usando la chiave pubblica di Bruno.*
4. *Bruno utilizza la sua chiave privata per conoscere la chiave di sessione.*
5. *Bruno decifra il messaggio utilizzando la chiave di sessione.*

Tra gli algoritmi a chiave pubblica vi sono gli algoritmi RSA e Diffie-Hellmann.



**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

## L' ALGORITMO DI DIFFIE-HELLMAN

L' algoritmo di Diffie-Hellman permette a due soggetti di generare e condividere una chiave segreta in un ambiente pubblico senza che, naturalmente, le informazioni criptate con tali chiavi possano essere decifrate.

Si supponga che due utenti (i, j) vogliano comunicare tra di loro in modo sicuro. Entrambe le parti dovranno calcolare e notificare al rispettivo interlocutore il valore:

$\mathbf{Y_i = a^{Xi} \ mod \ q}$ ( per l' utente i )

$\mathbf{Y_j = a^{Xj} \ mod \ q}$ ( per l' utente j )

dove **x** viene preso casualmente, e tenuto segreto, dall' insieme (1, ....., p-1) con **p** numero primo e **a** radice primitiva di **p**, ovvero:

$\mathbf{aX_t \ mod \ p = (1,2,.....,p-1)}$ non necessariamente in ordine

Ad esempio:

p=7, a=3

$3^1$ mod 7 = 3
$3^2$ mod 7 = 2
$3^3$ mod 7 = 6
$3^4$ mod 7 = 4
$3^5$ mod 7 = 5
$3^6$ mod 7 = 1

Anche l' algoritmo di Diffie-Hellman ha una forte base matematica e la sua sicurezza risiede nella difficoltà di ricavare il valore di un logaritmo in uno spazio discreto: anche rendendo pubblico il valore $Y_t$ si dimostra che è praticamente impossibile risalire al valore di $X_t$, che risulta pari a $\log_a$ (b mod p).

La chiave segreta che permetterà lo scambio dei dati tra le due entità in comunicazione può essere calcolata tramite la formula:

$\mathbf{K_{ij} = a^{XiXj} \ mod \ q}$

Resta comunque il fatto che entrambe le parti in comunicazione conoscono solo uno dei valori $\mathbf{X_t}$, il proprio, quindi per il calcolo della chiave segreta di comunicazione ci si poggia sul fatto che questa può essere calcolata come.

$\mathbf{K_{ij} = Y_j^{Xi} \ mod \ q}$ (per l' utente i )

$\mathbf{K_{ij} = Y_i^{Xj} \ mod \ q}$ (per l' utente j )



**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

## L' ALGORITMO RSA

L' insieme degli algoritmi asimmetrici, o a chiave pubblica, di cui RSA fa parte, si basano su una forte componente matematica. Il nome dell' RSA, presentato nel 1978, deriva dalle iniziali dei cognomi dei suoi tre inventori: Rivest, Shamir e Adleman, i quali basarono il loro algoritmo su quanto proposto da Diffie-Hellmann per i sistemi di crittografia a chiave pubblica. La sicurezza dell' RSA deriva dalla difficoltà (tempo di risoluzione non polinomiale) di fattorizzare un numero intero, grande, in due fattori primi, grandi anch' essi.
Il suo funzionamento è schematizzabile nel seguente modo:

**$c_i$ = funzione_di_cifratura ($m_i$) = $m_i^e$ mod n** **$c_i$ = testo cifrato**
**$m_i$ = funzione_di_decifratura ($c_i$) = $c_i^d$ mod n** **$m_i$ = testo in chiaro**

La chiave pubblica (e, n) e la chiave privata (d, n) vengono generate da una serie di calcoli effettuati su una coppia di numeri primi molto grandi (p, q) presi casualmente. In particolare:

**n = p * q :** *anche se reso noto, questo valore(molto grande) non permette di risalire ai suoi fattori visto che essi sono primi;*
**e** *è scelto casualmente con il vincolo di essere primo rispetto a (p-1)(q-1);*
**d** *è tale che* **e * d mod [(p-1)(q-1)] = 1**

Vediamo un esempio, solo a titolo dimostrativo, in cui adottiamo numeri piccoli (al contrario di quanto avviene nella realtà, dove la lunghezza in bit delle chiavi può superare 1024). Partendo dalla coppia di numeri primi *p=3* e *q=5* , seguendo i calcoli illustrati in precedenza si ottengono i seguenti valori:

*n = p * q = 15 e=11 d=3 (11 * d mod 8=1)*

la chiave pubblica sarà quindi (e, n)=(11, 15) mentre la chiave privata è (d, n) =3, 15. Supponendo che il messaggio da inviare sia m=2, il corrispondente cifrato (leggibile solo al destinatario e quindi crittato con la sua chiave pubblica) sarà:

$c= 2^{11} \text{ mod } 15 = 8$

Una volta ricevuto il messaggio, la fase di decrittazione si limiterà (utilizzando la chiave privata) al calcolo di:

$8^3 \text{ mod } 15 = 2$ *(= messaggio originale)*

In ambito di *comunicazione sicura*, l' utente A che vuole comunicare con B codifica il messaggio con la chiave pubblica di B e lo spedisce. Il messaggio in questione può essere letto unicamente da B che è l' unico possessore della corrispondente chiave privata.

Nel generare *firme elettroniche*, l' uso dell' RSA si basa semplicemente sull' inversione del ruolo delle chiavi rispetto a quello finalizzato alla riservatezza, quindi l' utente A codifica il messaggio con la propria chiave privata; in tal modo chiunque può leggere il messaggio



**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

(essendo nota a tutti la relativa chiave pubblica) e accertarsi del fatto che il dato è stato spedito sicuramente da A. Nella pratica, per la firma si evita di applicare l' operazione di codifica, mediante la chiave privata, all' intero testo (con la conseguente convenienza a livello di complessità), applicandola solo al riassunto generato da una particolare funzione detta *hash.*

All' atto pratico le chiavi pubbliche e private vengono rilasciate, previa richiesta formale, da Enti di Certificazione (EC) le quali si poggiano su *Certification Authority* (CA) per garantire il fatto che chi presenta una chiave pubblica (il certificato) ne sia il reale possessore.
Gli EC sono società che hanno lo scopo di assegnare una coppia di chiavi a chi ne fa richiesta, secondo criteri di uniformità e garantendo la massima riservatezza.
L' EC sceglie una coppia di numeri *p* e *q* non utilizzata precedentemente da altri (in base al contenuto di particolari registri) e calcola, secondo quanto descritto prima, il valore di *n, e* e *d.* Al termine delle elaborazioni i numeri *p* e *q* vengono eliminati in modo da non permettere a terzi il calcolo del valore della chiave che, senza questi numeri, risulta praticamente impossibile.
Va precisato che le coppie di chiavi sono catalogate sulla base della loro lunghezza in bit partendo da 40 bit sino ad arrivare a più di 1024.
Naturalmente avere chiavi lunghe garantisce una maggiore sicurezza nei confronti di attacchi di tipo *brute-force*, ma porta a un aumento del tempo computazionale necessario alla codifica/decodifica del messaggio.
Considerando infatti il caso in cui *n* è di 128 bit la lunghezza di *p* e *p* sarà mediamente di 64 bit (quindi si ottengono $2^{64}$ combinazioni, che per dasre un ordine di grandezza più esplicito corrispondono a circa $10^{19}$ ).
In pratica i valori utilizzati per questi due numeri sono compresi tra $10^{15}$ e $10^{25}$ , un intervallo in cui è presente un numero notevole di numeri primi, dell' ordine di grandezza di molti miliardi. Un attacco che prevede la ricerca per tentativi dei valori *p* e *q* richiederebbe un tempo così lungo da far ritenere l' impresa impossibile.
Considerando che è proprio su questo aspetto che RSA basa la sua robustezza, qualche studioso ha avanzato dubbi sulla reale inviolabilità. Infatti, essendo noto l' algoritmo di crittazione, è possibile scovare, anche se in tempi lunghi, la chiave di cifratura, dividendo *n* per tutti i numeri primi minori della sua radice quadrata sino a che il resto di tale divisione sia nullo.

In conclusione, vista la robustezza e l' enorme flessibilità, l' algoritmo RSA è ormai da considerare il meccanismo più diffuso per la generazione di chiavi asimmetriche.

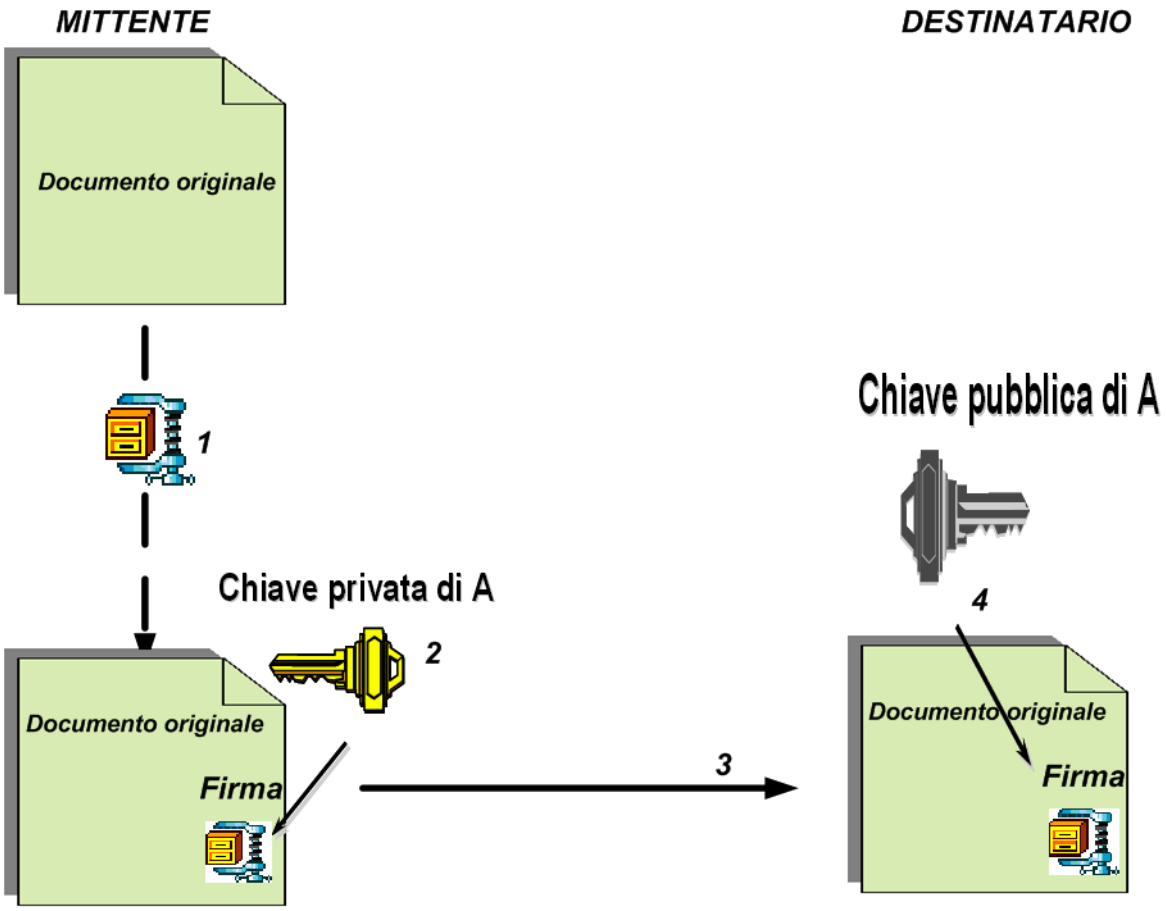


**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

## LA FIRMA ELETTRONICA

Mentre la crittografia garantisce la *confidenzialità* di un messaggio, la firma elettronica ne garantisce *l' integrità* e *l' autenticità* della provenienza, indipendentemente dal suo significato.

***Vediamo come viene generata e utilizzata la firma elettronica....***




1. Il procedimento di cui ci si avvale in tutti gli algoritmi di firma elettronica consiste nel generare, con funzioni *one-way hash (es.SHA-1, MD5)*, un "riassunto" del contenuto del messaggio in una stringa di lunghezza relativamente limitata. Queste funzioni sono strutturare in modo tale che ogni cambiamento al messaggio originale si rifletta sul valore della stringa. Qualsiasi modifica al contenuto del messaggio, porta ad avere una diversa firma. In genere le stringhe utilizzate sono di 128 bit, o multipli di 128.
2. Successivamente, questa "impronta digitale" viene crittografata (utilizzando un algoritmo a chiave pubblica) con la chiave privata del mittente, ottenendo appunto la "firma digitale".
3. La firma elettronica può essere allegata in chiaro in calce al messaggio, e può essere inviato al destinatario.
4. Il destinatario, ottenuto il messaggio firmato, lo decripta utilizzando la chiave pubblica del

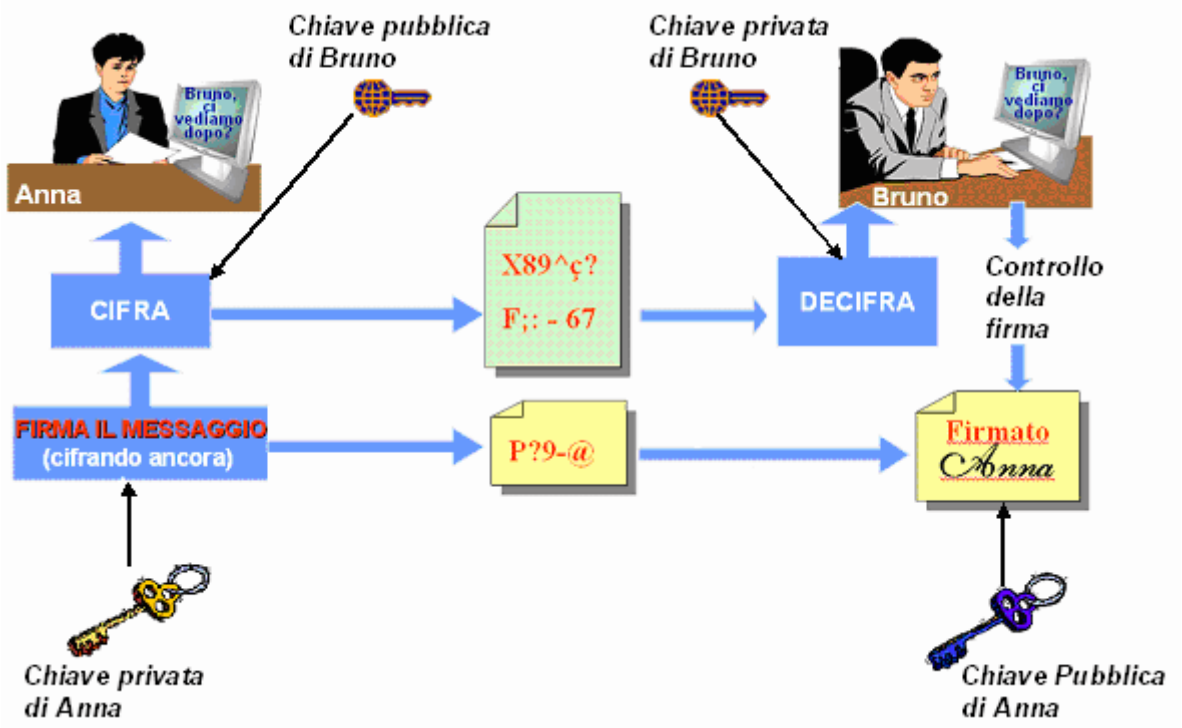


**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

mittente, ricavando in tal modo l' impronta digitale (fingerprint).
A questo punto sarà sufficiente al destinatario confrontare questo *fingerprint* con quello che egli calcolerà in modo autonomo.
Se i due fingerprint corrispondono, egli sarà sicuro che:

- Il messaggio non è stato manomesso (integrità);
- Chi ha spedito il messaggio è veramente chi dice di essere, perché è la sola persona che conosce la chiave privata corrispondente alla chiave pubblica con cui il destinatario ha decriptato il messaggio (autenticazione del mittente);
- Se, come spiegato, il mittente è la sola persona che ha potuto firmare il messaggio, egli non potrà ripudiare quanto firmato (non ripudio del messaggio).

## *METTIAMO INSIEME CIFRATURA E FIRMA ....*




Cifrando e firmando un documento vengono garantiti nello stesso tempo:

- confidenzialità del messaggio (protezione del messaggio)
- non ripudio
- autenticazione
- integrità del messaggio.



**GlobalTrust Italia S.p.A.**
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553