

Crittografia



Moreno Marzolla
Dipartimento di Informatica
Università Ca' Foscari di Venezia
marzolla@dsi.unive.it
<http://www.dsi.unive.it/~marzolla>

Ringraziamenti

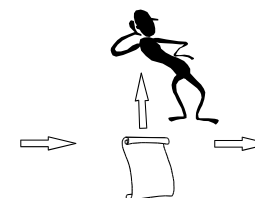
- prof. Francesco Dalla Libera
 - Corso di Commercio Elettronico, Dipartimento di Informatica, Università Ca' Foscari di Venezia.

Scopo della crittografia

- Proteggere i dati dall'essere letti da persone non autorizzate
 - Privacy
- Impedire a persone non autorizzate dall'inserire, cancellare, modificare messaggi
 - Integrità
- Verificare il mittente di ogni messaggio
 - Autenticazione
- Consentire agli utenti di firmare elettronicamente i messaggi
 - Non ripudiabilità

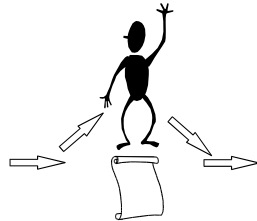
Privatezza

- Garanzia per il mittente
 - Solo i destinatari autorizzati possono leggere il contenuto dei messaggi



Autenticazione e integrità

- Garanzia per il Ricevente
 - Conosce l'identità del Mittente
 - I messaggi non sono stati alterati
 - I messaggi non sono stati ritardati ad arte nella consegna



Crittografia

- Disciplina che si occupa di studiare le tecniche per scrivere un messaggio in modo tale che solo il legittimo destinatario sia in grado di leggerlo.
 - Si occupa dunque del problema della segretezza
- I requisiti principali di tale tecnica sono:
 - 1) Ragionevole efficienza nella creazione del messaggio
 - 2) Estrema difficoltà nella interpretazione del messaggio da parte di chi non è autorizzato
 - 3) Possibilità di cambiare con estrema rapidità il metodo usato

Sfatiamo alcuni miti

- Un algoritmo crittografico tenuto segreto è automaticamente sicuro perché nessuno sa come funziona

NIENTE DI PIU' FALSO!!!!

 - E' impossibile dimostrare che un algoritmo crittografico è sicuro
 - Un algoritmo crittografico è sicuro finché non viene rotto
 - Lo esponete allo scrutinio pubblico per verificare se gli esperti individuano delle falle

La sicurezza sta nelle chiavi

- La sicurezza di un algoritmo crittografico deve risiedere SOLO ed ESCLUSIVAMENTE sulle chiavi crittografiche che usa, NON nel modo in cui le chiavi vengono usate
 - Se una persona non conosce la chiave NON deve poter leggere il messaggio cifrato...
 - ...anche se conosce il modo con cui il messaggio è stato cifrato

Esempio

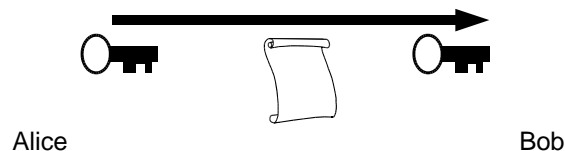
- Adobe impiega nei libri elettronici pubblicati nel suo formato proprietario un algoritmo crittografico “segreto”
- Un programmatore ha analizzato questo formato, e ha scoperto che la protezione si può violare quasi con carta e penna
- Non fidatevi MAI MAI MAI di soluzioni crittografiche “a scatola chiusa”

Sistemi crittografici

- A chiave segreta (o crittografia simmetrica)
 - Mittente e ricevente devono avere la stessa chiave per poter leggere il messaggio
- A chiave pubblica (o crittografia asimmetrica)
 - Mittente e ricevente NON condividono le stesse chiavi
- Funzioni hash unidirezionali

Crittografia simmetrica

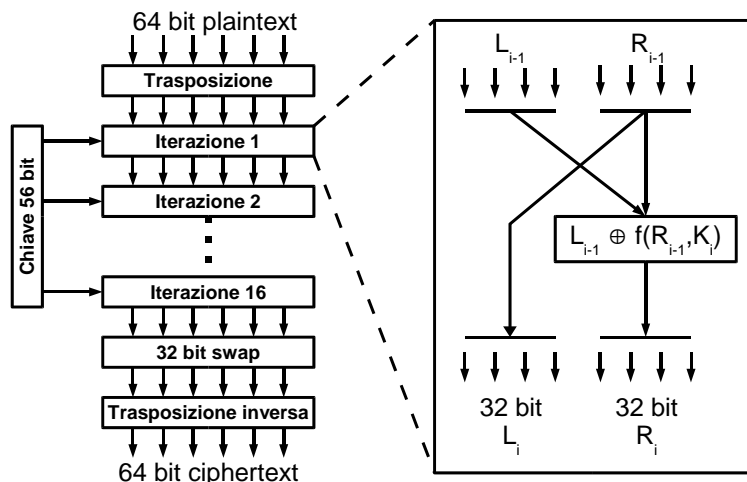
- Alice cifra il messaggio con la chiave K
- Bob decifra il messaggio con la stessa chiave
 - Ovviamente nessun altro deve conoscere la chiave!



Algoritmo DES (Data Encryption Standard)

- Progettato dall'IBM e adottato come standard del governo U.S.A. nel 1977
- Caratteristiche
 - Chiave da 56 bit
 - Il testo in chiaro è codificato in blocchi di 64 bit, che producono ciascuno 64 bit di testo cifrato (cifratura a blocchi)
- In teoria, senza sapere la chiave è impossibile decodificare il messaggio...
 - ...a meno di provare tutte le chiavi possibili, che sono 2^{56} , cioè circa 1 seguito da 16 zeri

DES all'interno



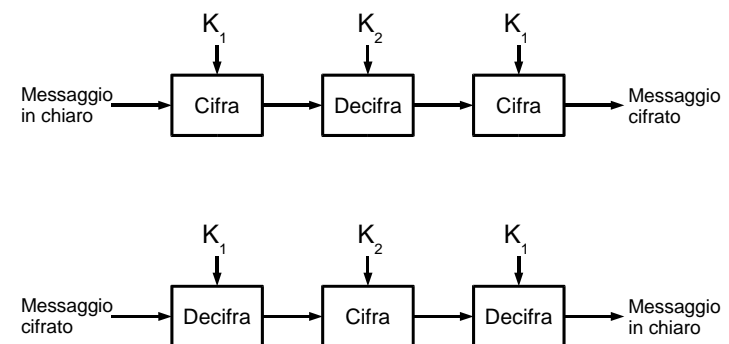
Problemi con DES

- Nonostante lo spazio delle chiavi sia molto ampio, l'algoritmo DES non è oggi considerato sufficientemente sicuro
 - La versione iniziale era basata su un codice IBM chiamato Lucifer, con chiave a 128 bit
 - La versione standardizzata di DES però aveva una chiave di 56 bit,
 - Il procedimento con cui la IBM aveva sviluppato DES fu tenuto segreto
- E' possibile effettuare una ricerca esaustiva dello spazio delle chiavi con macchine dedicate
- Morale: non usatelo!

Triplo DES

- Una variante dell'algoritmo DES (Triplo DES) combina fa uso di più passi di codifica in cascata che usano due chiavi
 - Lo spazio delle chiavi sale a 2^{112} , cioè circa 1 seguito da 33 zeri
 - Questo è un numero sufficientemente elevato per considerare l'algoritmo triplo DES sufficientemente sicuro
 - ...ma per quanto?

Triplo DES



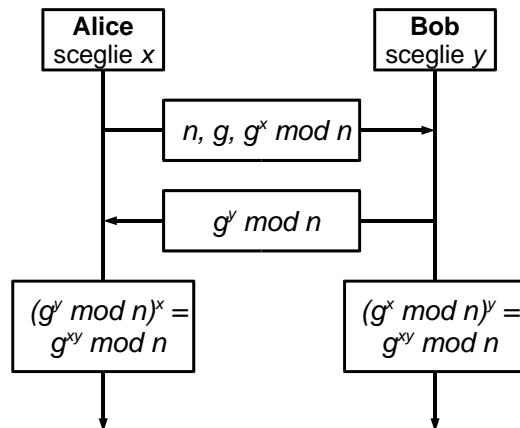
Oltre DES

- DES viene ancora largamente utilizzato
- Tuttavia, la sua sicurezza viene costantemente messa in discussione
- Successori di DES
 - IDEA, sviluppato in Svizzera
 - Chiave di 128 bit
 - Cifra a sostituzione su blocchi di 64 bit
 - AES (Advanced Encryption Standard), precedentemente nodo come Rijndael, sviluppato in Belgio
 - Chiave di 128, 192 o 256 bit
 - Cifra a sostituzione su blocchi di 128 bit

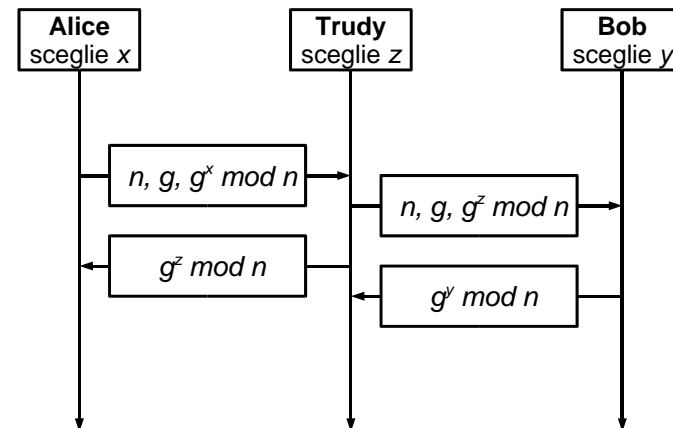
Scambio di una chiave condivisa: l'algoritmo Diffie-Hellman

- Scegliere due numeri primi n e g con certe proprietà
- Alice sceglie un numero segreto x (lungo 512 bit ad esempio)
- Alice manda a Bob $[n, g, g^x \text{ mod } n]$
- Bob sceglie un numero segreto y (lungo 512 bit)
- Bob manda ad Alice $[g^y \text{ mod } n]$
- Alice calcola $(g^y \text{ mod } n)^x = g^{xy} \text{ mod } n$
- Bob calcola $(g^x \text{ mod } n)^y = g^{xy} \text{ mod } n$

Diffie-Hellman



Problema



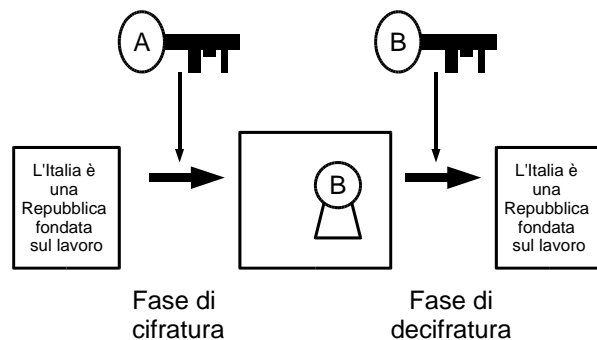
Crittografia simmetrica: problemi

- Un problema si ha quando aumenta il numero di persone che vogliono comunicare fra loro
- Ogni coppia di persone deve essere in possesso di una corrispondente chiave
 - Se N persone desiderano comunicare fra loro ci vogliono $N(N-1)/2$ chiavi, cioè una per ogni coppia
 - Questo rende estremamente difficile il problema della distribuzione delle chiavi, che resta il punto debole di tutto il sistema

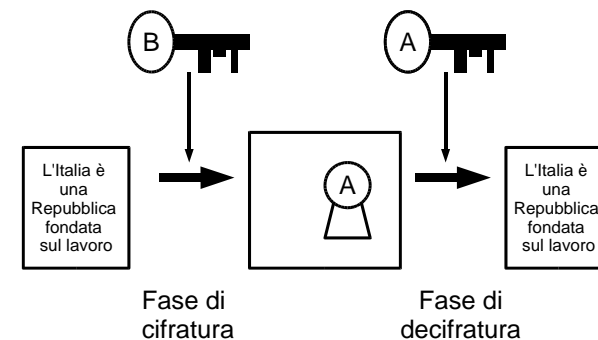
Crittografia a chiave pubblica (asimmetrica)

- Nella seconda metà degli anni '70 fu introdotto (Diffie e Hellmann, Stanford University) un tipo di crittografia radicalmente nuovo, detto a chiave pubblica (o asimmetrica)
- Idea
 - Ciascun utente ha due chiavi
 - Se si usa una delle due chiavi per codificare un messaggio, l'altra (e solo quella!) può essere usata per decodificarlo
 - E' quasi impossibile derivare la prima chiave anche se si conosce la seconda

Esempio

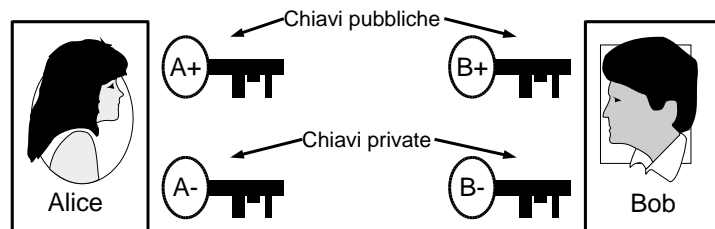


...ma anche



Idea di base

- Ogni utente possiede due chiavi
 - Una è pubblica, e viene resa disponibile a chiunque la richieda
 - La seconda è privata, e l'utente deve custodirla gelosamente e non darla a nessuno

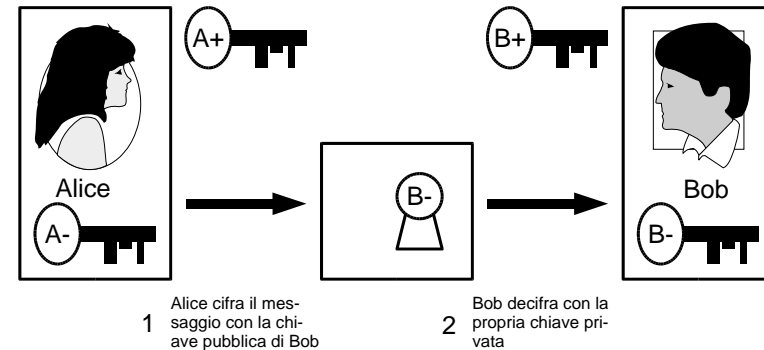


Moreno Marzolla

Tecnologie Web

25

Alice e Bob



Moreno Marzolla

Tecnologie Web

26

Vantaggi

- Alice è sicura che solo Bob riuscirà a decodificare il messaggio
- Se N persone devono comunicare, è sufficiente che ciascuno sia in possesso di tutte le chiavi pubbliche (oltre alla propria chiave privata)
 - Nel caso della comunicazione con chiave simmetrica, N comunicazioni richiedevano $N(N-1)/2$ chiavi
 - Non è necessario scambiarsi chiavi segrete; le uniche chiavi che vengono trasferite sono le chiavi pubbliche
- Svantaggio
 - La crittografia asimmetrica è più lenta di quella simmetrica

Moreno Marzolla

Tecnologie Web

27

Proprietà della crittografia asimmetrica

- Consideriamo la coppia di chiavi (k_A^+, k_A^-)
 - k_A^+ chiave pubblica
 - k_A^- chiave privata
- Codifica e decodifica
 - $E(k, m)$ = codificare il messaggio m con la chiave k
 - $D(k, m)$ = decodificare il messaggio m con la chiave k
- Vale la proprietà
 - $D(k_A^+, E(k_A^-, m)) = m$
 - $D(k_A^-, E(k_A^+, m)) = m$

Moreno Marzolla

Tecnologie Web

28

Un po' più formalmente...

- Alice genera una coppia di chiavi (k_A^+ , k_A^-) rende pubblica k_A^+ e tiene segreta la chiave k_A^-
- Chi vuole mandare un messaggio m in modo sicuro con Alice
 - si procura k_A^+
 - calcola $c = E(k_A^+, m)$
 - invia c ad Alice
 - solo Alice può calcolare $m = D(k_A^-, c)$ perché la chiave è segreta

Algoritmo RSA

- All'inizio:
 - Scegliere due numeri primi p e q ($> 10^{100}$)
 - Calcolare $n=p \times q$, $z=(p-1) \times (q-1)$
 - Scegliere un numero d relativamente primo a z
 - Scegliere e tale che $e \times d \equiv 1 \pmod{z}$
- Le chiavi sono:
 - pubblica: (e, n)
 - privata: (d, n)
- Codifica e decodifica
 - Codifica: Calcolare $C = P^e \pmod{n}$
 - Decodifica: Calcolare $P = C^d \pmod{n}$

Però...

- ...come fa Bob ad essere sicuro che un messaggio proviene proprio da Alice e non da qualcun altro?
 - Infatti chiunque può codificare il messaggio con la chiave pubblica di Bob, dato che tale chiave è disponibile a chiunque
- La crittografia asimmetrica può essere usata per risolvere anche questo problema!

Autenticazione del mittente

- Prendiamo il messaggio m
- Alice lo codifica con la propria chiave privata
 - Si ottiene $E(k_A^-, m)$
- Alice lo codifica ulteriormente con la chiave pubblica di Bob
 - Si ottiene $E(k_B^+, E(k_A^-, m))$
- Bob decodifica prima con la sua chiave privata
 - Si ottiene $D(k_B^-, E(k_B^+, E(k_A^-, m))) = E(k_A^-, m)$
- Bob decodifica poi con la chiave pubblica di A
 - Si ottiene $D(k_A^+, E(k_A^-, m)) = m$

Integrità e firma

- La crittografia a chiave pubblica può essere usata per *autenticare* l'origine di un messaggio e per garantirne *l'integrità*, ossia di fatto per firmare un messaggio.
- Si fa uso delle funzioni *one-way hash* (dette anche funzioni *digest*, cioè funzioni riassunto) che vengono applicate al messaggio e ne producono un riassunto (MD = *message digest*).

Cos'è una funzione hash?

- Consideriamo un messaggio m
- Una funzione hash produce un “riassunto” del messaggio m , che indichiamo con $MD(m)$, con la seguente proprietà
 - Il riassunto $MD(m)$ deve apparire come “scelto a caso” rispetto a m
 - Se due messaggi m ed m' differiscono di un solo bit, i riassunti $MD(m)$ e $MD(m')$ dovrebbero apparire completamente diversi
 - Deve essere difficile costruire un messaggio m che abbia un certo riassunto
- MD5 funzione standard

Funzioni hash usate

- MD5
 - Sviluppato da Ronald Rivest
 - Genera una signature di 128 bit
- SHA-1
 - Sviluppato dalla NSA
 - Genera una signature di 160 bit
 - E' stato recentemente forzato e non è ritenuto sicuro. Meglio usare alternative più robuste come SHA-256 o SHA-512

Esempio / 1

Spettabile ditta,
con la presente vi richiediamo l'invio di 10 confezioni da 5 pezzi dell'articolo di codice CX409W, che pagheremo alla consegna.
Cordiali saluti.

MD5

b67ceef802e72ad8c14de17de0e58e9e

Esempio / 2

Spettabile ditta,

con la presente vi richiediamo l'invio di **11** confezioni da 5 pezzi dell'articolo di codice CX409W, che pagheremo alla consegna.

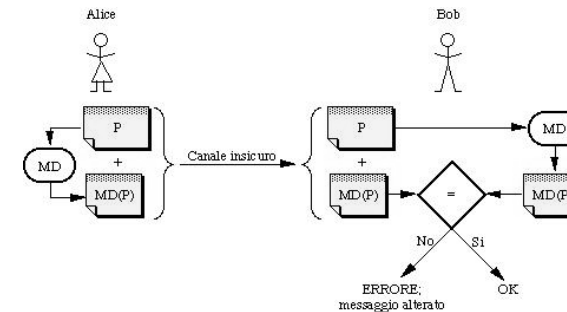
Cordiali saluti.

MD5

04eb92e6d8e2a932ebe14e85d887a3dd

Uso delle funzioni hash

- Vengono utilizzate per garantire l'integrità di un messaggio, cioè che un messaggio non è stato alterato



Problemi?

- Alice invia il messaggio corredato del riassunto; quando Bob riceve il tutto, ricalcola il riassunto e lo confronta con quello ricevuto
- Modalità esposta all'attacco di un intruso
 - Potrebbe intercettare il messaggio, sostituirlo con uno diverso correlato del relativo digest, e inviarlo a Bob come se fosse quello proveniente da Alice.
- Soluzione: firma elettronica

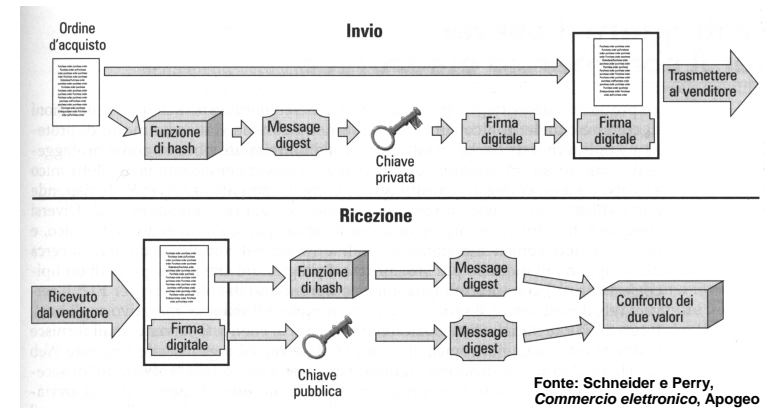
Firma elettronica: obiettivi

- Il ricevente può verificare l'identità del mittente
- Il mittente non può ripudiare in seguito il contenuto del messaggio
 - Cioè negare di aver inviato proprio lui quel messaggio, con quel contenuto
- Il ricevente non può aver "costruito" in proprio il messaggio
- Il messaggio è arrivato integro

Firma elettronica: in pratica

- Si calcola il riassunto del messaggio con una funzione hash
- Il riassunto, prima di essere spedito, viene *cifrato dal mittente con la propria chiave privata* e decifrato dal destinatario con la chiave pubblica del mittente.
- Un riassunto cifrato in questo modo si dice firma elettronica del mittente
 - Si dice firma digitale (*digital signature*) del mittente, perché assicura sia l'integrità del messaggio che l'autenticità del mittente, proprio come una firma apposta (in originale) in calce a un documento cartaceo

Schema



Problemi di sicurezza risolti dalla crittografia

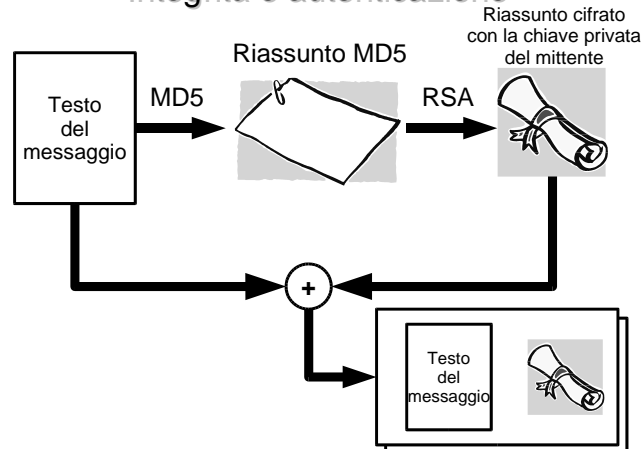
- Privacy di dati, messaggi, conversazioni
- Commercio Elettronico sicuro
- Non-ripudiabilità delle transazioni
- Autenticazione degli utenti
- Sicurezza della posta elettronica

Mail privata

Obiettivi

- **Confidenzialità**
 - Solo il destinatario può interpretare il contenuto del messaggio
- **Autenticazione**
 - Il destinatario sa che il messaggio proviene proprio dal mittente, e non da qualcun altro che ne ha preso il posto
- **Non-ripudiabilità**
 - Il destinatario sa che il mittente non potrà in seguito negare di aver spedito quel messaggio con quel contenuto

Mail privata: Integrità e autenticazione

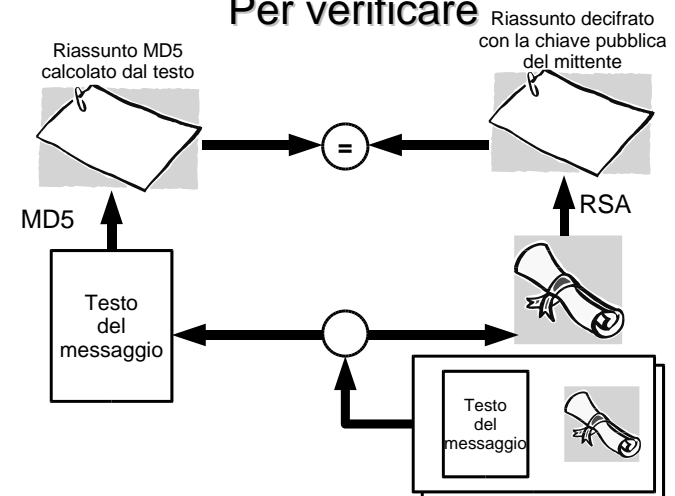


Moreno Marzolla

Tecnologie Web

45

Per verificare



Moreno Marzolla

Tecnologie Web

46

Sistemi ibridi di cifratura

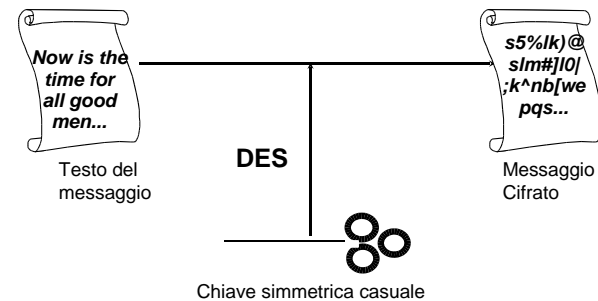
- La cifratura a chiave simmetrica (chiave condivisa tra mittente e ricevente) è molto veloce, ma è difficile distribuire le chiavi in modo sicuro
- La cifratura a chiave pubblica rende facile distribuire le chiavi, ma è meno veloce
- Soluzione: usare la cifratura a chiave pubblica per distribuire una chiave privata condivisa, e successivamente effettuare la cifratura mediante la chiave simmetrica

Moreno Marzolla

Tecnologie Web

47

Esempio / 1

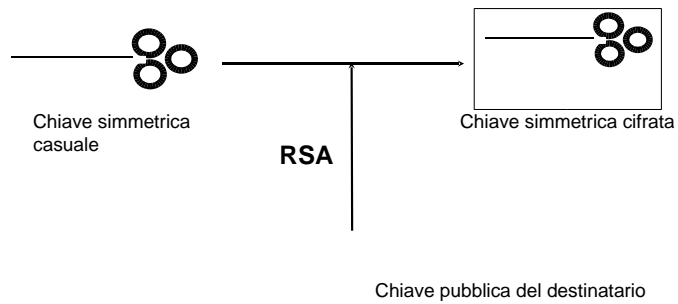


Moreno Marzolla

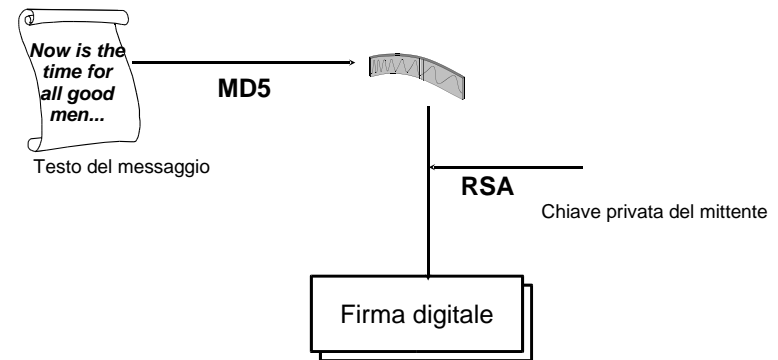
Tecnologie Web

48

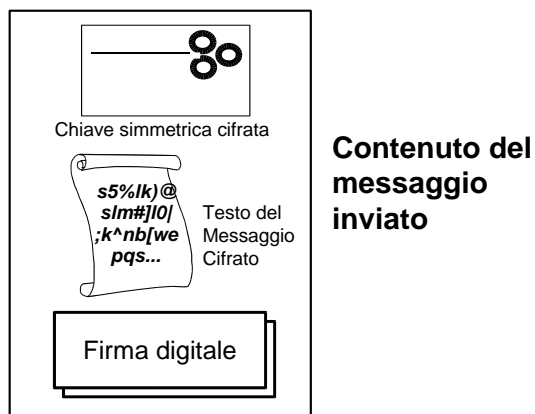
Esempio / 2



Esempio / 3



Esempio / 4



Tecniche di autenticazione forte

- Smart cards or tokens
 - Software (server) and smartcard based
 - PIN-protected smartcard private key
 - System issues challenge based on user
 - User uses password to unlock smartcard, which reads challenge, calculates cryptographic response
 - Response is used as response to challenge

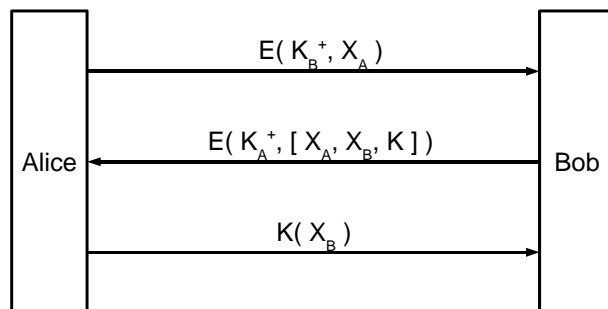
Meccanismo *challenge-response*

- **Idea**
 - Mittente e destinatario si scambiano una serie di messaggi che servono a dimostrare alla controparte che loro sono *in quel momento* chi dicono di essere
 - Si sfrutta il meccanismo di codifica asimmetrica (chiavi pubbliche e private)

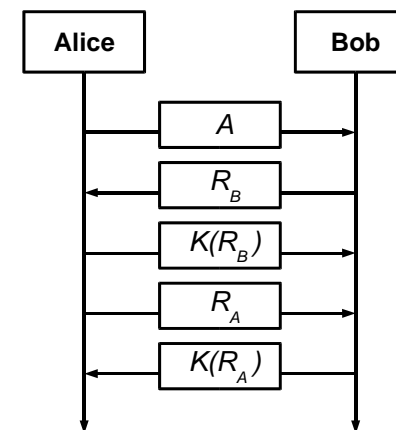
Come si fa

- Alice manda a Bob un messaggio contenente un numero casuale X_A da lei generato. Il messaggio è codificato con la chiave pubblica di Bob
- Bob riceve il messaggio, ed è in grado di decodificarlo. Invia una risposta contenente X_A , un numero casuale generato da Bob X_B e una chiave privata K (simmetrica) da usare successivamente
- Alice riceve il messaggio e lo legge. Vede che Bob è riuscito a decodificare il suo messaggio precedente (perché ha letto X_A), e invia un nuovo messaggio contenente il numero casuale di Bob codificato con la chiave di sessione K

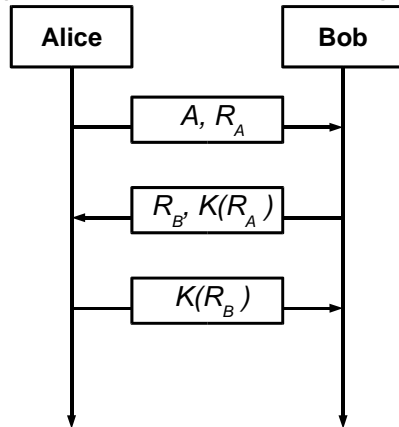
Esempio



Challenge-Response con chiave condivisa K



Una versione semplificata (che non funziona!)

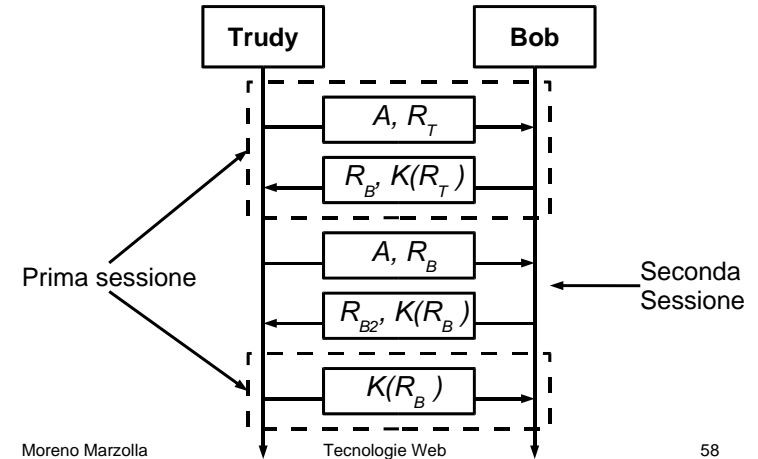


Moreno Marzolla

Tecnologie Web

57

Perché non funziona?



Moreno Marzolla

Tecnologie Web

58