Firme digitali e firme camaleontiche

Outline

- Firma Digitale classica
- Il problema della trasferibilità della firma
- Chameleon Hashing
- Chameleon Signatures

FIRMA DIGITALE
classica

FIRMA DIGITALE
classica

- Nasce alla fine degli anni ’70 del XX secolo grazie all’invenzione della ***CRITTOGRAFIA ASIMMETRICA***

- Esistono vari algoritmi che la implementano, tra i più importanti:

  - **RSA**
  - **ElGamal**

FIRMA DIGITALE
classica

La ***CRITTOGRAFIA ASIMMETRICA*** (o *non convenzionale*) fa uso di due chiavi:

- la ***chiave pubblica***
- la ***chiave privata***

Le due chiavi sono ***COMPLEMENTARI*** infatti se si cifra un messaggio con una delle due chiavi, si deve utilizzare necessariamente l'altra per la decifratura

Le due chiavi sono ***DISTINTE***: se si possiede la chiave pubblica non c'è alcun modo per ricavare la chiave privata

CRITTOGRAFIA ASIMMETRICA

Fondamenti matematici

La crittografia asimmetrica fa uso di concetti matematici, che implicano l'uso di ***aritmetiche modulari***, quali:

- fattorizzazione
- logaritmo discreto

Vediamo un esempio di generazione di una coppia di chiavi asimmetriche bastata sul concetto di fattorizzazione di grandi numeri (RSA-like):

- si scelgono due numeri primi grandi (~256 bit ciascuno) p e q
- si calcola $n=pq$ e $\Phi(n) = (p-1)(q-1)$
- si sceglie un numero e primo con $\Phi(n)$
- si calcola (attraverso l'algoritmo di Euclide esteso) un numero d definito come l'inverso di e modulo n
- si pone la coppia $<e,n>$ come *chiave pubblica*
- si pone la coppia $<d,n>$ come *chiave privata*

FIRMA DIGITALE e CRITTOGRAFIA ASIMMETRICA

Tecnica di cifratura -RSA based-

NOME	METODO	DESCRIZIONE
Cifratura	$C = M^e \bmod n$	Il messaggio *M* è cifrato (*C*) per mezzo della chiave pubblica del destinatario *e*
Decifratura	$M = C^d \bmod n$	La decifratura del messaggio *M* può essere effettuata solo da chi è in possesso della chiave *d*
Firma digitale	$F = M^d \bmod n$	**Il messaggio *M* è firmato (*F*) per mezzo della chiave privata del firmatario *d***
Verifica	$V = C^e \bmod n$	**La verifica della firma (F) può essere effettuata da chiunque per mezzo della chiave pubblica *e***

FIRMA DIGITALE e CRITTOGRAFIA ASIMMETRICA

Vantaggi e debolezze

Punti di forza della crittografia asimmetrica

- Mittente A e destinatario B non devono preaccordarsi su una chiave comune
- Chiunque in possesso della chiave pubblica di B può cifrare un messaggio a lui diretto, ma solo B con la sua chiave privata (segreta) può decifrarlo
- Si introduce la ***FIRMA DIGITALE***:
  - un messaggio cifrato con la chiave privata di B, può essere stato generato solo da B
  - chiunque in possesso della chiave pubblica può decifrare il messaggio, accertandosi dell'autenticità del firmatario

FIRMA DIGITALE e CRITTOGRAFIA ASIMMETRICA

Vantaggi e debolezze

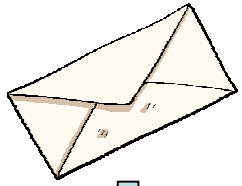
debolezze della crittografia asimmetrica

- I meccanismi matematici utilizzati rendono particolarmente lenta l'elaborazione; quindi in un protocollo di crittografia asimmetrica di solito ci si deve appoggiare ad algoritmi convenzionali e **funzioni hash**

In particolare oggi la *firma digitale* è sinonimo di **HASH-THEN-SIGN**: firmare un messaggio vuol dire cioè ***CIFRARE SOLO IL SUO DIGEST***, ricavato da funzioni hash

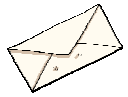
FIRMA DIGITALE = HASH-THEN-SIGN

Messaggio originale



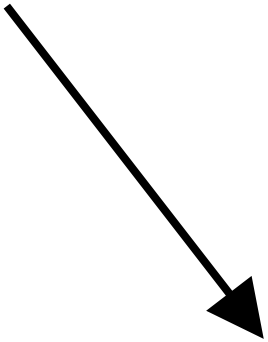
Funzione hash (o digest)

Message digest

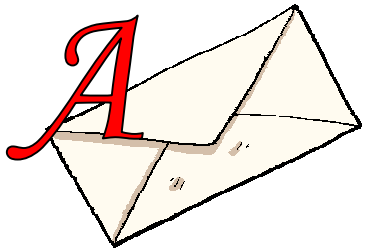


Algoritmo di cifratura asimmetrica (con chiave privata)

FIRMA DIGITALE



Messaggio corredato di firma digitale



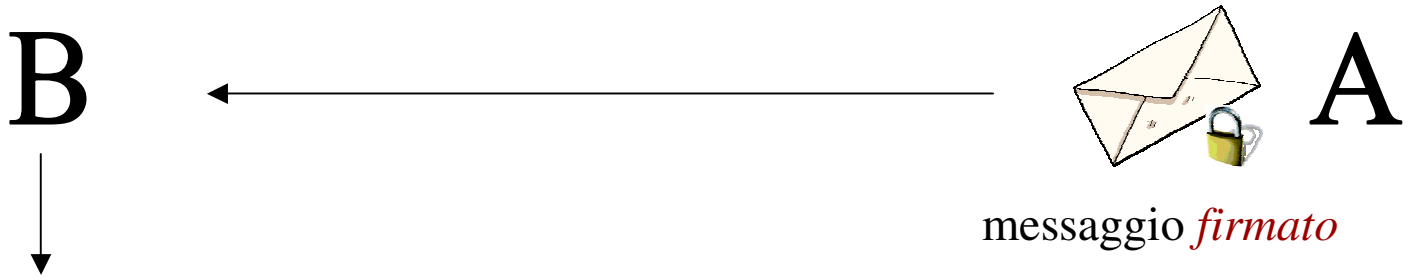
Le *due parti* (messaggio originale e sua firma digitale) vengono *concatenate* ovvero sintatticamente giustapposte

FIRMA DIGITALE

Proprietà (1/3)

AUTENTICAZIONE :

Cifrando il messaggio con la *chiave privata* il mittente è univocamente identificato; infatti essendo la chiave *personale ed esclusiva*, è il solo in grado di cifrarvi un messaggio

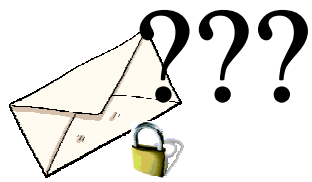


FIRMA DIGITALE
Proprietà (2/3)

NON RIPUDIO :

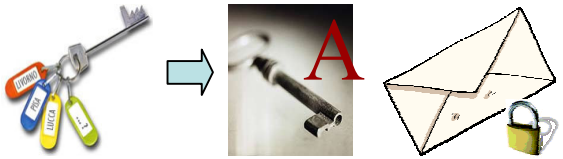
Deriva direttamente dalla proprietà di autenticazione; visto che un utente che firma un messaggio con la chiave privata è l'***UNICO*** in grado di farlo, egli non potrà negare di aver generato quel messaggio

B



messaggio *firmato* da un anonimo

Tra tutte le chiavi pubbliche in possesso di B, solo quella di A *verifica* il messaggio



⇒

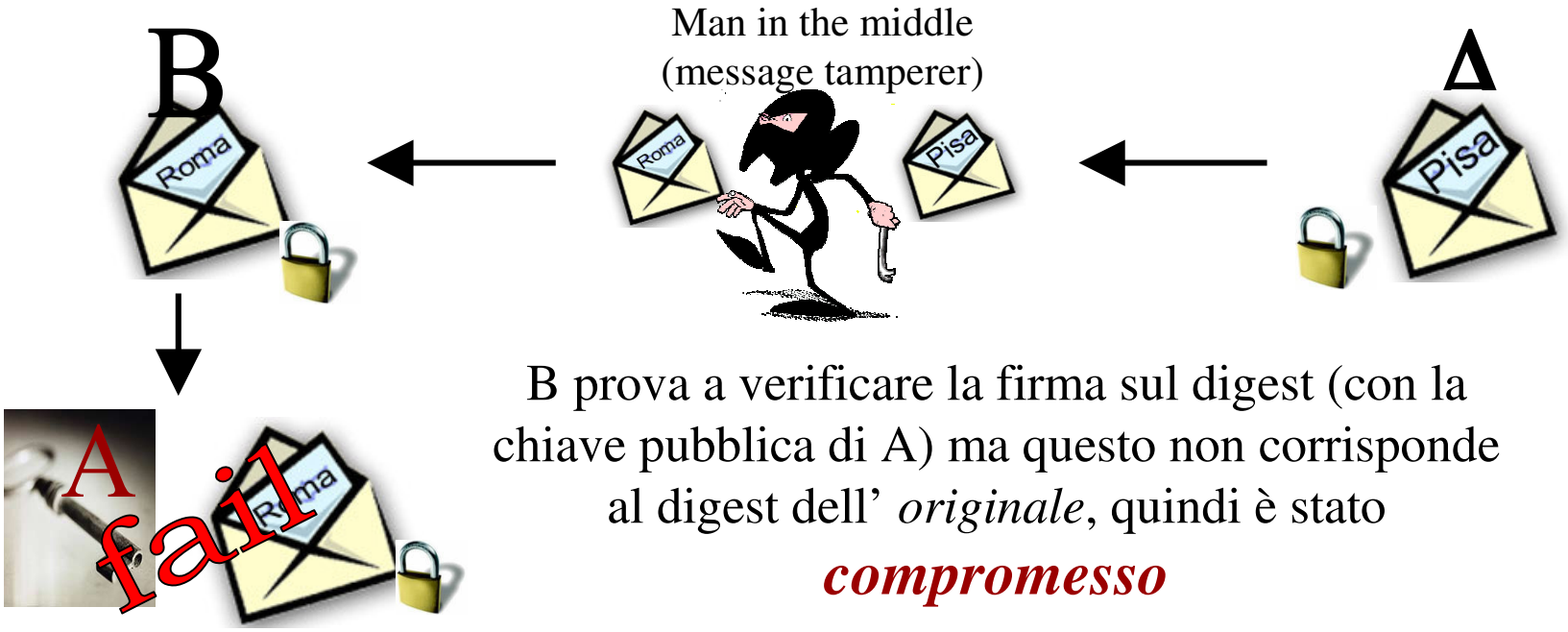
Il messaggio è stato *firmato* da A, che non può ripudiarlo!

FIRMA DIGITALE

Proprietà (3/3)

INTEGRITA' :

Un messaggio *firmato* non può essere manomesso (il testo non può essere alterato) perché altrimenti la verifica di uguaglianza tra il message digest firmato e il message digest del messaggio ricevuto, non andrebbe a buon fine

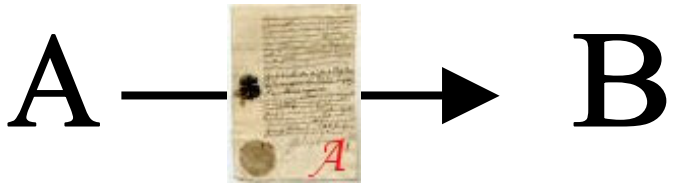


B prova a verificare la firma sul digest (con la chiave pubblica di A) ma questo non corrisponde al digest dell' *originale*, quindi è stato

compromesso

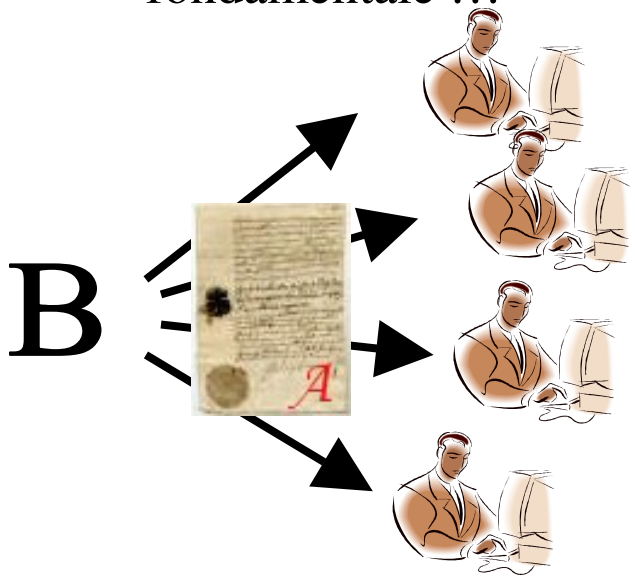
Il problema della TRASFERIBILITA' della firma

Il problema della TRASFERIBILITA' della firma



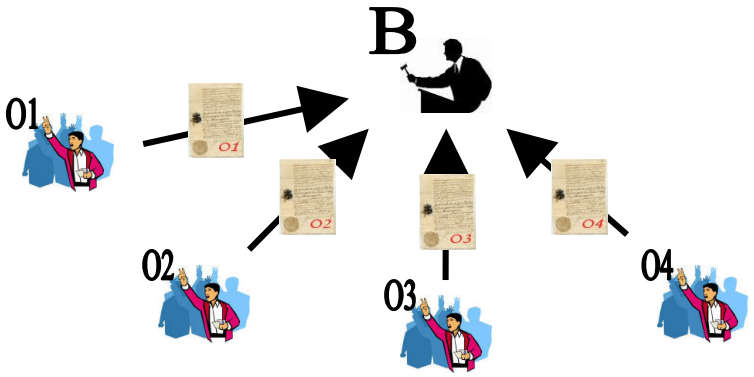
Il documento firmato certifica univocamente a *B* che *A* ne è l'autore (*autenticazione*): questa caratteristica è fondamentale …

… ma ciò consente a *B* di rilasciare l'informazione certificata a chiunque; nessuno sarà di fatto capace di negare la validità del documento …



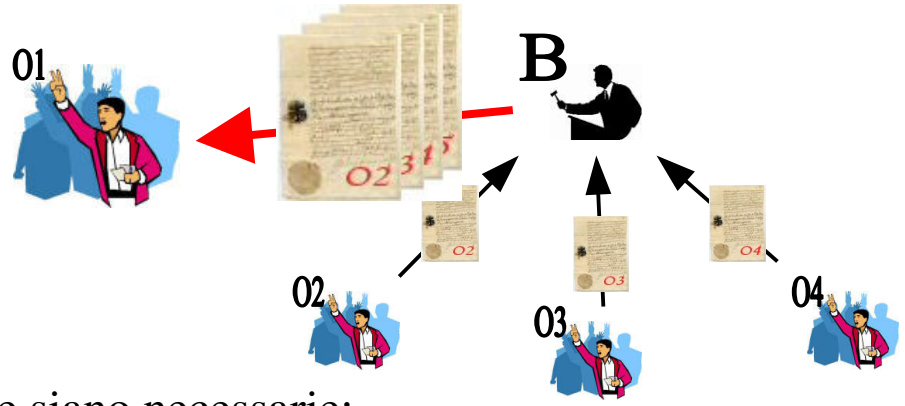
… ci sono dei contesti in cui questo ***DEVE ESSERE EVITATO*** …

… le aste on-line ad offerta segreta



In questo genere di aste ogni partecipante fa un'offerta segreta (on-line) e al termine del tempo previsto, il banditore (*B*), determina il vincitore dell'asta, ovvero chi ha fatto l'offerta maggiore (minore se è un'asta al ribasso)

Ma se il banditore ***fosse disonesto***, potrebbe colludere con uno dei partecipanti, rivelandogli le offerte degli altri per fargli vincere l'asta scorrettamente.



In questo caso, sebbene siano necessarie:

- *autenticazione* di ogni partecipante all'asta
- *non ripudio* delle offerte fatte

… la normale firma digitale non si adatta bene al contesto, perché *una firma digitale standard è trasferibile*!

… qual è il problema della FIRMA DIGITALE standard ?

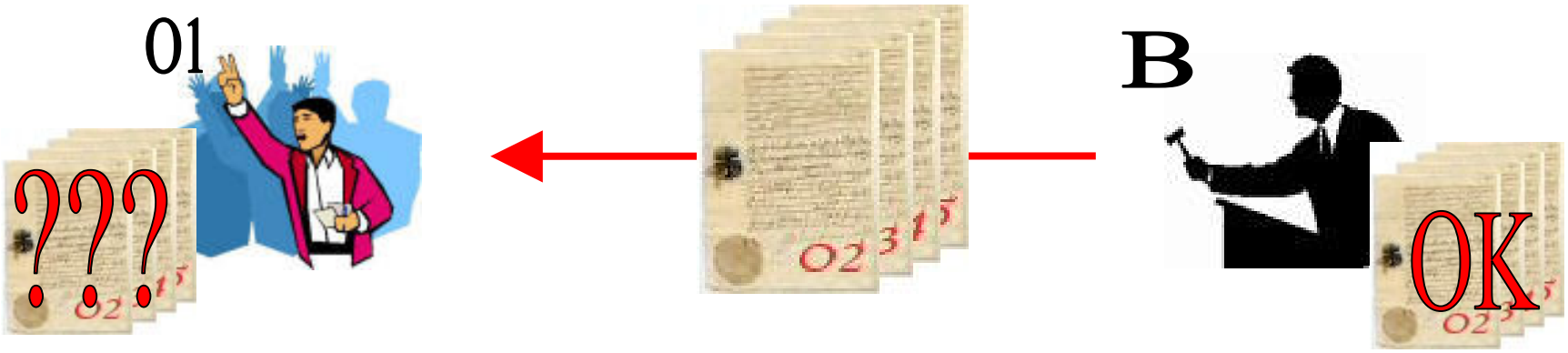
Il meccanismo di collusione tra banditore disonesto e terza parte è bastato sulla ***FIDUCIA***

La fiducia è implementata dalla ***firma digitale*** che non lascia dubbi sull'identità del messaggio e sulla veridicità dell'offerta

Il meccanismo di fiducia potrebbe essere minato dall'introduzione della firma ***NON TRASFERIBILE*** …

… firme *non trasferibili*

Ma cosa si intende per FIRMA NON TRASFERIBILE ????



… è una firma, che sia contemporaneamente:

- **valida** (autentica, non ripudiabile) per il banditore
- **non pubblicamente verificabile** (quindi non valida) per terze parti

SI PUO' REALIZZARE UN MECCANISMO DI FIRMA CON QUESTE CARATTERISTICHE ????

CHAMELEON HASHING

CHAMELEON HASHING

Le ***CHAMELEON*** (o ***TRAPDOOR***) ***HASH FUNCTIONS*** sono particolari funzioni hash, cui è associata una coppia di chiavi:

- **una *chiave pubblica***
- **una *chiave privata* (detta *trapdoor*)**

Una chameleon hash function può essere riconosciuta dalle seguenti tre proprietà:

1. Chiunque conosce la chiave pubblica è in grado di calcolare la funzione hash ad essa associata
2. Per chi non conosce la *trapdoor*, la funzione hash risulta essere ***collision resistant***
3. Chi è a conoscenza della *trapdoor* può facilmente trovare collisioni su un dato message digest

CARATTERISTICHE DI UN HASH CAMALEONTICO

Una chameleon hash function è associata ad un utente destinatario *D;*
D, attraverso un opportuno algoritmo, genera due chiavi:

- $\mathbf{HK_D}$, la chiave pubblica (*hashing key*)
- $\mathbf{CK_D}$, la trapdoor (*collision key*)

CHAM-HASH$_D$(m,r)

m è il messaggio di cui calcolare il chameleon digest

r è una stringa casuale che serve a computare il digest

Denota la trapdoor hash function, che deve avere 3 caratteristiche

RESISTENZA ALLE COLLISIONI

COLLISIONI TRAMITE TRAPDOOR

UNIFORMITA'

CARATTERISTICHE DI UN HASH CAMALEONTICO

RESISTENZA ALLE COLLISIONI

Non esiste un algoritmo efficiente che, preso in input HK_D, riesca a trovare due coppie (m_1,r_1) e (m_2,r_2) con $m_1 \neq m_2$, tale che CHAM-HASH$_D$ (m_1,r_1) = CHAM-HASH$_D$ (m_2,r_2), tranne che per una probabilità trascurabile

COLLISIONI TRAMITE TRAPDOOR

Esiste un algoritmo efficiente che, presi in input CK_D, un qualsiasi coppia (m_1,r_1) e un ulteriore messaggio m_2, trova un valore r_2 per cui si verifica l'uguaglianza: CHAM-HASH$_D$ (m_1,r_1) = CHAM-HASH$_D$ (m_2,r_2)

UNIFORMITA'

Tutti i messaggi m sono uniformemente distribuiti sullo spazio degli output della funzione hash camaleontica CHAM-HASH$_D$ (m,r), con r scelto uniformemente a caso. In altri termini, per r scelto a caso, non può essere "svelato" niente riguardo al messaggio m semplicemente studiando l'output (il chameleon digest)

chameleon hashing

Princìpi matematici

Costruzione generale di una *trapdoor hash function* mediante claw-free permutation

($f_0(x)$,$f_1(x)$) è una coppia di permutazioni *claw-free* se è computazionalmente difficile trovare valori x,y del loro dominio t.c. $f_0(x) = f_1(y)$

GENERAZIONE CHIAVI →

$$HK_D = (f_0, f_1)$$
$$CK_D = (f_0^{-1}, f_1^{-1})$$

Coppia di permutazioni claw-free con le rispettive inverse

FUNZIONE CHAM-HASH →

$$ChamHash_{(f_0,f_1)}(m,r) = f_{m[k]}(...(f_{m[2]}(f_{m[1]}(r)))...)$$

- **m[i]**=i-mo bit di m; **k** = lunghezza di *m* (in numero di bits);

FUNZIONE PER TROVARE COLLISIONI SU UN DIGEST →

$$r_2 = f_{m_2[1]}^{-1}(f_{m_2[2]}^{-1}(...(f_{m_2[k]}^{-1}(ChamHash_{(f_0,f_1)}(m_1,r_1)))...))$$

chameleon hashing

Princìpi matematici

Generare coppie di permutazioni claw-free non è affatto banale; lo si può fare, però, per mezzo di implementazioni semplificate basate sulla

intrattabilità della fattorizzazione

- si scelgono due numeri primi ***p***, ***q*** tali che $p \equiv 3 \bmod 8$ $q \equiv 7 \bmod 8$
- si calcola $\boldsymbol{n = pq}$
- si dimostra allora che la coppia di permutazioni

$$f_0(x) = x^2 \bmod n$$
$$f_1(x) = 4x^2 \bmod n$$

$$con\ x \in \left\{ Z_n^* \mid \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1 \right\}$$

è *claw-free*

chameleon hashing

Princìpi matematici

Si possono generare trapdoor hash function anche a partire da una base differente da quella delle permutazioni *claw-free*, ovvero il ***LOGARITMO DISCRETO***:

GENERAZIONE CHIAVI →

- si scelgono $\boldsymbol{p}$, $\boldsymbol{q}$ primi tali che $p=kq+1$, e un elemento $\boldsymbol{g}$ di ordine q in Z_p^*
- $\boldsymbol{CK_D} = x \in Z_q^*$
- $\boldsymbol{HK_D} = y = g^x \bmod p$

FUNZIONE CHAM-HASH → $ChamHash_y(m,r) = g^m y^r \bmod p$ *con* $m \in Z_q^*$ (messaggio), $r \in Z_q^*$ (# random)

FUNZIONE PER TROVARE COLLISIONI SU UN DIGEST →

per trovare il valore random $\boldsymbol{r_2}$ della coppia $(\boldsymbol{m_2},\boldsymbol{r_2})$ il cui digest collide con $(\boldsymbol{m_1},\boldsymbol{r_1})$, si deve risolvere l'equazione

$$m_1 + xr_1 = m_2 + xr_2 \bmod q$$

CHAMELEON SIGNATURES

CHAMELEON SIGNATURES

definizione

Una ***firma digitale camaleontica*** (o *chameleon signature*) è il risultato della applicazione di un algoritmo di firma digitale standard (RSA,DSS,…) ad un message digest calcolato grazie ad una

trapdoor hash function

CHAMELEON SIGNATURES

Una *chameleon signature* ha delle caratteristiche innovative rispetto agli standard conosciuti

1. Come per le firme digitali standard, il firmatario **F** di un messaggio non può ripudiare una firma da lui emessa
2. Il destinatario **D** di un messaggio così firmato non è in grado di dimostrare ad una terza parte che una firma di F corrisponde ad un dato messaggio, visto che D possiede gli strumenti per generare una firma del tutto simile a quella di F
3. Le firme sono *recipient-specific* cioè se uno stesso messaggio ha due destinazioni differenti (destinatari distinti) allora deve essere firmato due volte

La caratteristica ***2*** prende il nome di ***NON - TRASFERIBILITA'***

componenti per la realizzazione di uno schema di
FIRMA DIGITALE CAMALEONTICA

gli attori

- ***F***, chi firma il messaggio
- ***D***, il destinatario del messaggio
- ***G***, un giudice: un'entità imparziale per la valutazione in caso di dispute sulla validità della firma

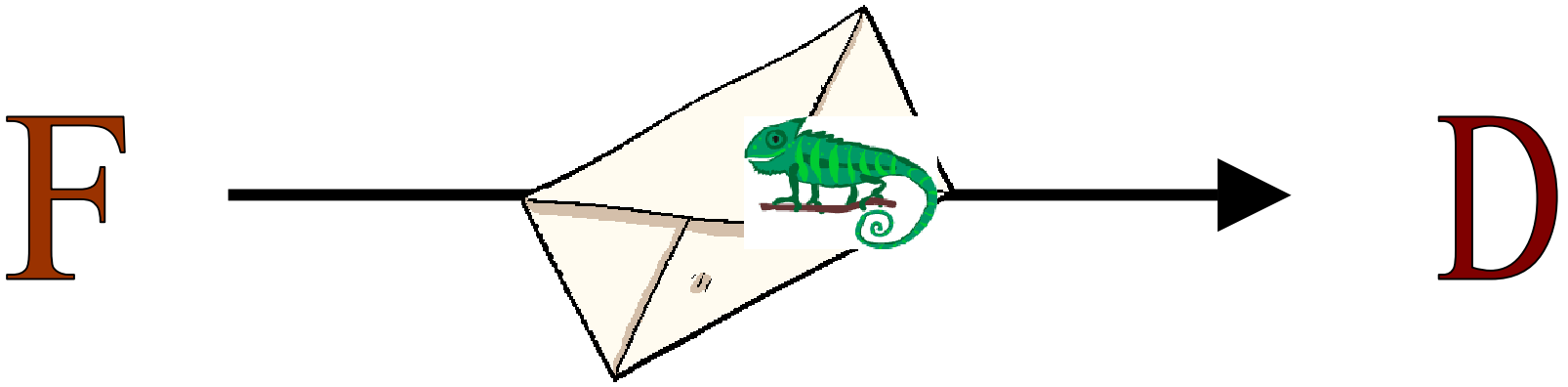
le funzioni

- uno ***schema standard di firma digitale*** (RSA, DSS …) con le chiavi (pubblica e privata), nonché relative funzioni per la firma (**SIGN**) e la verifica (**VERIFY**)
- una ***trapdoor hash function*** con le relative chiavi (pubblica e trapdoor) e la funzione per il calcolo del digest camaleontico (**CHAM-HASH$_D$**)

le chiavi

- per la firma digitale standard: $\boldsymbol{SK_F}$ è la chiave privata (*signing key*) di *F*, mentre $\boldsymbol{VK_F}$ è la corrispondente chiave pubblica (*verifying key*)
- per il digest camaleontico: $\boldsymbol{HK_D}$ è la chiave pubblica (*hashing key*) di *D*, mentre $\boldsymbol{CK_D}$ è la trapdoor information (*collision key*)

lo schema di FIRMA



$$SIG(m) = (m, r, SIGN_F(hash))$$

E' il ***messaggio originale*** allegato ***in chiaro*** a tutto il pacchetto spedito

E' il ***numero random*** necessario per calcolare il digest camaleontico con la funzione designata

E' la ***firma digitale*** (tramite algoritmo noto) del firmatario *F*; è applicata allo hash camaleontico calcolato con $\boldsymbol{HK_D}$ tramite ***m*** ed ***r***, ovvero

$$hash := \textbf{CHAM-HASH}_{\mathbf{D}}(m,r)$$

Io schema di VERIFICA

Quando *D* riceve il "pacchetto camaleontico" **SIG(m)** deve verificare se contiene una firma valida e se il digest camaleontico del messaggio è corretto

- grazie al messaggio ***m***, e al numero random ***r***, è in grado di calcolare il digest camaleontico (tramite la chiave pubblica della sua funzione, HK_D):

$$\textbf{CHAM-HASH}_{\textbf{D}}(m,r)$$

- per mezzo della chiave pubblica VK_F del firmatario *F* può decifrare (*verificare*) il valore $\textbf{SIGN}_{\textbf{F}}(hash)$ trovando il testo in chiaro, ***hash***

- a questo punto se $\text{CHAM-HASH}_D(m,r) = hash$ allora il destinatario *D* può ritenere la firma di *F* valida a tutti gli effetti (come fosse una firma digitale standard), altrimenti la firma non è ritenuta autentica

… perché la firma camaleontica è NON TRASFERIBILE ???

Si noti che *D*, qualora volesse, avrebbe la capacità di produrre una valore *hash* identico a quello prodotto da *F*, ma a partire da un messaggio *m* e un numero random *r* diversi da quelli "confezionati" da *F*, grazie alla formula vista:

$$r_2 = f^{-1}_{m_2[k]}(f^{-1}_{m_2[k-1]}(...(f^{-1}_{m_2[1]}(hash))...))$$

Qui la funzione inversa rappresenta la trapdoor CK_D, che solo *D* possiede; il valore *r2* è tale che $\underline{\text{CHAM-HASH}_D(m_2,r_2)} = \underline{hash}$

Questa capacità di generare un digest identico a partire da un messaggio (un'offerta, nell'esempio dell'asta on line) e da un numero casuale ***DIVERSI***, rende del tutto INATTENDIBILE ogni informazione divulgata da *D*

Quindi la firma prodotta da *F* è ***NON - TRASFERIBILE***

… e in caso di DISPUTA?

Nonostante la firma non sia trasferibile, cioè universalmente verificabile, esiste ancora il *NON-RIPUDIO* della firma stessa da parte del firmatario

Se il destinatario *D* ha dubbi sulla veridicità della firma, può ricorrere all'intervento di *un giudice* ***G***, una terza parte affidabile e super partes che è in grado di verificarla.

G preleverà da *D* la firma incriminata SIG(m), e chiederà a *F* di fornire due valori *m* e *r* che producano lo stesso chameleon digest di SIG(m):

- qualora *F* non fornisca i valori corretti oppure si rifiuti di fornirne, la firma sarebbe dichiarata *non valida*
- nel caso contrario, ovvero qualora i valori siano corretti, così sarà la firma

Rivelerebbe però la trapdoor -violazione della confidenzialità di *F*-: le implementazioni più recenti delle chameleon signatures risolvono anche questo problema
(***exposure-freeness***)

Caratteristiche di sicurezza delle chameleon signatures

NON RIPUDIO	il firmatario non può negare di aver firmato un documento
NON TRASFERIBILITA'	solo il destinatario designato può verificare la firma
NON INTERATTIVITA'	non c'è bisogno di scambio multiplo (asincrono) di messaggi tra il firmatario e il destinatario del messaggio
SICUREZZA SEMANTICA	il digest camaleontico non rivela informazioni sul messaggio firmato
PRATICITA' ED EFFICIENZA	i costi dell'algoritmo nella sua interezza sono bassi, comparabili ad un algoritmo standard di firma digitale
CONVERTIBILITA'	una variante delle chameleon signatures può essere trasformata in una firma digitale standard, all'occorrenza

CONCLUSIONI

1. Le FD sono utili ma, in alcuni contesti, troppo "forti";
2. Le firme camaleontiche:
   - Indeboliscono la FD;
   - Preservano l'imputabilità,
3. Un paradigma promettente, sia per l'accademia che per il settore ICT.

Riferimenti bibliografici

- H. Krawczyk, T. Rabin.
  Chameleon Hashing and Signatures, NDSS.
- G. Ateniese, B. de Medeiros.
  Identity-based Hash and Applications
- Tsudik, Ateniese
  Sanitizable signatures, ESORICS 2006