Mantenere i propri dati segreti: l'utilizzo della crittografia da parte del professionista

di Enrico Zimuel (enrico@enricozimuel.net)

28 Novembre ICLC 2002

Bologna, Starhotel Excelsior, 28-30 novembre 2002

http://www.iclc.org

Note sul copyright (copyfree):

Questa presentazione può essere utilizzata liberamente
a patto di citare la fonte e non stravolgerne il contenuto.

Questa presentazione è stata creata con OpenOffice 1.0
www.openoffice.org

Sommario

- La crittografia come strumento di garanzia della privacy
- Ambiti d'utilizzo della crittografia per la protezione dei dati:
  - La sicurezza del traffico web (IpSec, SSL, TLS)
  - Privacy personale e posta elettronica (PGP, GnuPG)
- La firma digitale e le certification authority
- Il Decreto legislativo 23 gennaio 2002, n. 10
- Esempi d'utilizzo dei software PGP e GnuPG

La crittografia come strumento di garanzia della privacy

- Perchè la crittografia è in grado di garantire la privacy?
- La crittografia è una scienza basata su alcune applicazioni numeriche della matematica. Ciò vuol dire che la sicurezza di un sistema crittografico è affidata, principalmente, all'impossibilità o meglio alla complessità di risolvere problemi di natura matematica.
- Un tipico problema può essere il seguente: Sia *n* un numero con 617 cifre decimali prodotto di due numeri primi *p* e *q*, ossia *n*= *p***q*, calcolare *p* e *q*!
- Rsa Inc. mette in palio $200'000 per chi riesce a calcolare *p* e *q* (http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html).

Ambiti d'utilizzo della crittografia per la protezione dei dati

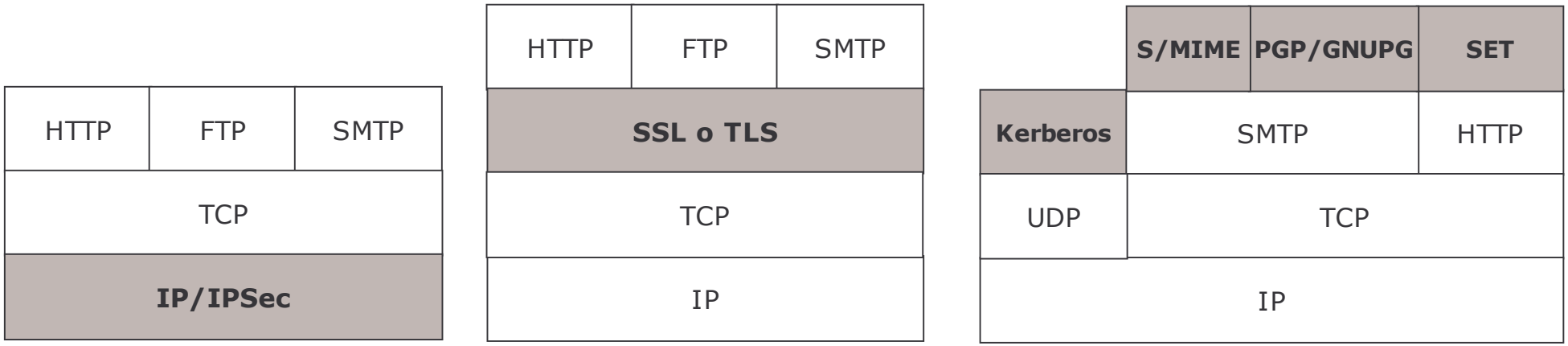
- La crittografia viene utilizzata ormai in molte applicazioni per la protezione dei dati personali, alcuni esempi: la crittografia del GSM (algoritmo A5), le carte di credito (smart card), la protezione della comunicazioni satellitari (SECA2), internet (secure web), e-privacy (cifratura dei documenti informatici, firma digitale).
- Per poter garantire sicurezza in ambito crittografico è necessario imporre la trasparenza dei principi di funzionamento tecnico.
- Principio di Kerckhoffs (1883): *"La sicurezza di un sistema crittografico è basata **esclusivamente** sulla conoscenza della chiave, in pratica si presuppone noto a priori l'algoritmo di cifratura e decifrazione."*

Sicurezza= Trasparenza!

- "*Se un sistema è veramente sicuro, lo è anche quando i dettagli divengono pubblici*" Bruce Schneier
- Questa apparente contraddizione può essere spiegata solo grazie all'ausilio della matematica come base teorica della crittografia.
- Sicurezza teorica = Sicurezza pratica? Purtroppo NO, i problemi sorgono in fase di applicazione dei concetti teorici (ad esempio esiste un algoritmo teoricamente sicuro, l'algoritmo di Vernam, ma non può essere implementato correttamente).
- Conoscenza algoritmo = libera distribuzione codici sorgenti = standard aperti = uno dei principi fondamentali dell'open source!

Sicurezza del traffico web

- Per fornire sicurezza del traffico web esistono diversi approcci simili dal punto di vista delle funzionalità ma differenti per quanto concerne l'ambito di applicabilità ed il loro posizionamento all'interno della pila del protocollo TCP/IP.

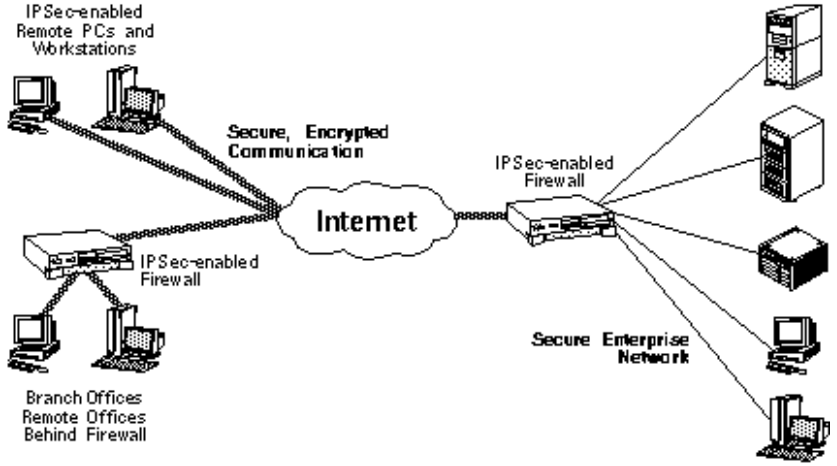


Sicurezza IP

- Il protocollo di comunicazione attualmente utilizzato su Internet Ipv4 non prevede la cifratura dei messaggi dati (nell'IPv6 si), chiunque può "sniffare" ossia intercettare dalla rete un pacchetto dati e ricostruire il messaggio originario.
- La sicurezza IP (IPSec, *IP Security*) nasce da una precisa esigenza: proteggere le comunicazioni IP da attacchi di tipo IP spoofing (falsificazione degli indirizzi IP) e di tipo IP sniffing (intercettazione dei pacchetti dati).
- La protezione avviene tramite encryption dei pacchetti IP.
- IPSec fornisce la possibilità di rendere sicure le comunicazioni su LAN, su WAN private e pubbliche e su Internet.
- IPSec fornisce un insieme di servizi di sicurezza a livello IP: controllo dell'accesso, integrità in assenza di connessione, autenticazione della sorgente dati, rifiuto di pacchetti originati da un attacco di replay, riservatezza (cifratura), parziale riservatezza del flusso di traffico.

Sicurezza IP

- Alcuni esempi d'utilizzo di IPSec:
  - Connettività sicura di filiali su Internet;
  - Accessi remoti sicuri su Internet;
  - Possibilità di stabilire connettività extranet e intranet con i partner;
  - Miglioramento della sicurezza del commercio elettronico;
- La caratteristica più importante di IPSec è che può cifrare e/o autenticare tutto il traffico a livello IP, adattandosi quindi a una notevole gamma di applicazioni.



I protocolli SSL e TLS

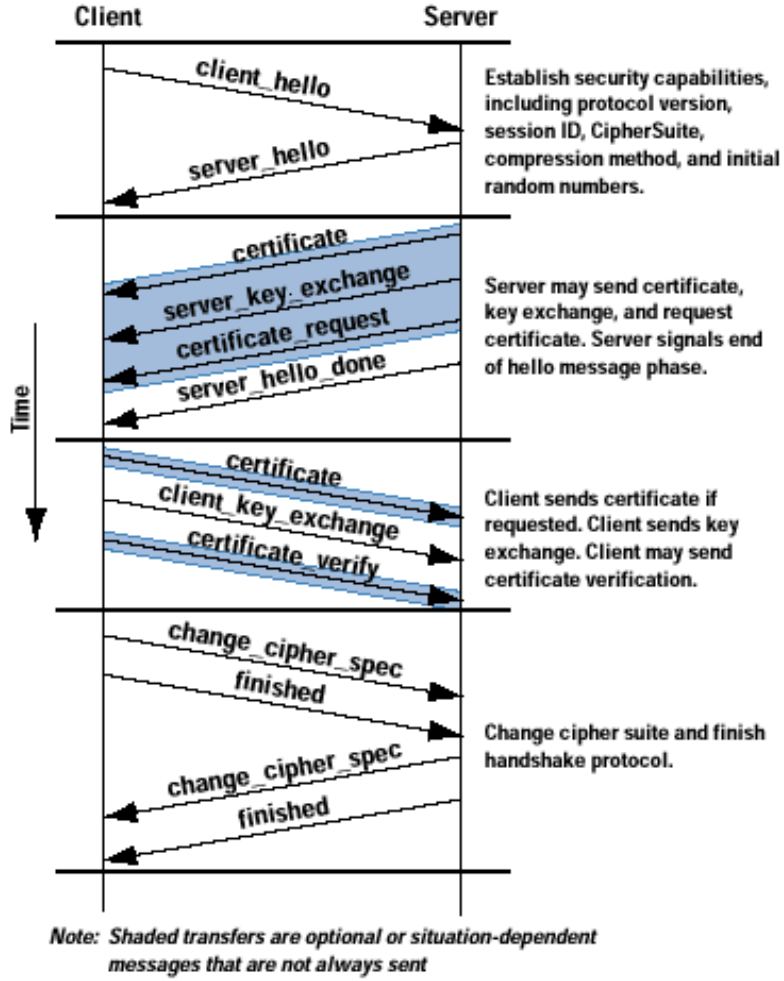
- SSL (Secure Socket Layer) è stato creato dalla Netscape nel 1994, la versione 3.0 è del 1995.
- Successivamente il progetto è stato sottoposto al processo di standardizzazione Internet, all'interno di IETF () si costituì il gruppo di lavoro TLS (Transport Layer Security).
- La prima versione del TLS può essere considerata come un SSL 3.1, in pratica lo standard TLS è l'evoluzione del protocollo SSL.
- SSL è progettato per fare uso del protocollo TCP al fine di fornire un servizio di sicurezza end-to-end affidabile.
- Viene utilizzato per proteggere le transazioni via web di dati sensibili (https): acquisti legati all'e-commerce, numeri di carte di credito, informazioni aziendali, etc.

I protocolli SSL e TLS

- SSL è costituito da due livelli di protocolli: l'SSL **Record** e l'SSL **Handshake**; il primo viene utilizzato per il trasposto dei messaggi fornendo servizi di riservatezza ed integrità dei dati, il secondo fornisce il processo di autenticazione tra client e server per la creazione di un canale sicuro di comunicazione per l'utilizzo dell'SSL Record.
- La cifratura delle transazioni via web è variabile per ogni sessione di collegamento.
- Gli algoritmi di cifratura utilizzati dal protocollo SSL sono: IDEA, RC2-40, DES-40,DES, 3DES, Fortezza, RC4-40, RC4-128.
- Gli algoritmi di autenticazione per lo scambio delle chiavi temporali utilizzati dal protocollo SSL sono: RSA,DSS, MD5, SHA-1, Diffie-Hellman.

Il protocollo di autenticazione SSL: l'Handshake

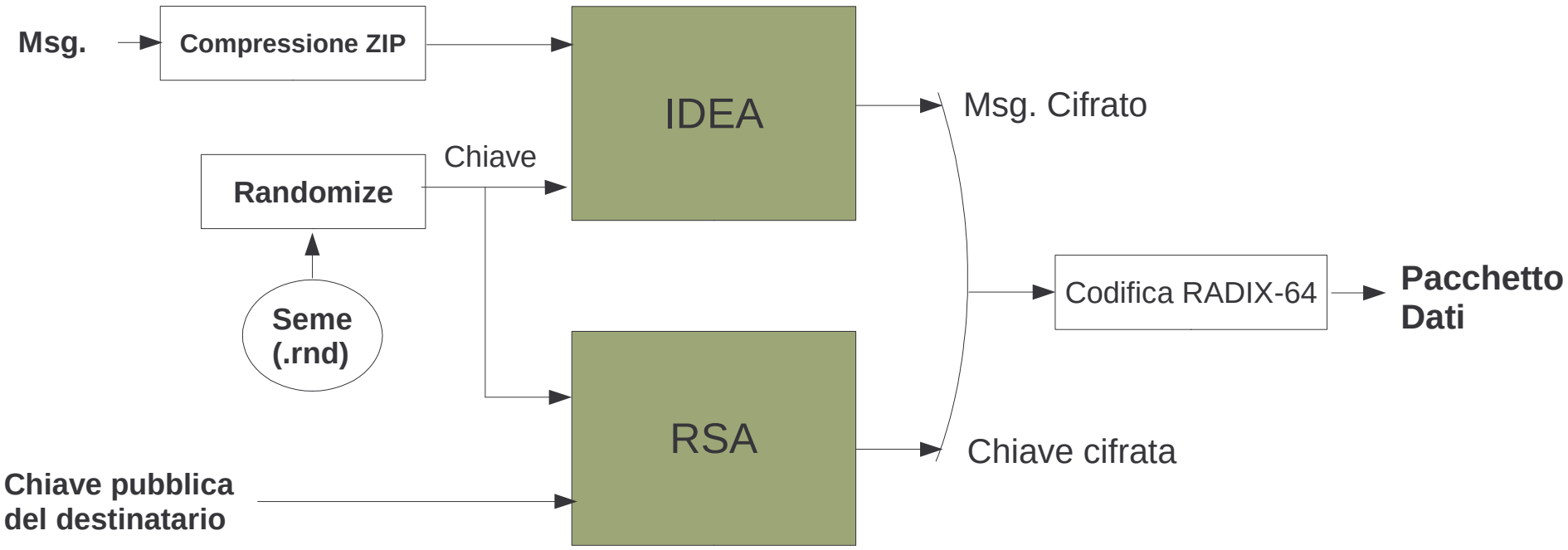
- I passi principali dell'SSL Handshake possono essere così schematizzati:
  - Utente: client hello
  - Server: server hello
  - Server: invio del certificato
  - Server: server hello done
  - Utente: autenticazione del sistema
  - Utente: invio del pre-master secret e costruzione del master secret
  - Server: ricezione del pre-master secret e costruzione del master secret.
  - Utente: invio del certificato (opzionale)
  - Utente/Server: messaggio finished



Sicurezza della posta elettronica: PGP

- PGP (Pretty Good Privacy) è un software di pubblico dominio creato da Phil Zimmermann nel 1991.
- E' un software per la privacy personale: protezione delle email, dei files, firma digitale.
- Utilizza gli algoritmi di crittografia a chiave pubblica RSA, Diffie-Hellman, DSA e gli algoritmi simmetrici IDEA, CAST, 3-DES.
- E' basato su di un sistema di crittografia "ibrido" nel senso che utilizza crittografia simmetrica per le operazioni di encryption sui dati generando delle chiavi di sessione pseudo-casuali cifrate con un algoritmo a chiave pubblica.
- Attualmente il progetto PGP è risorto con la nuova società PGP Corporation, l'ultima versione rilasciata in beta è la 8.0.

Il funzionamento del PGP (esempio di encryption di un messaggio)



Sicurezza della posta elettronica: GNUPG

- Il progetto tedesco GnuPG (GNU Privacy Guard) nasce nel 1997 per opera di Werner Koch, sviluppatore indipendente interessato alla crittografia OpenSource.
- L'obiettivo del progetto è la realizzazione di un engine crittografico, alternativo al Pgp, totalmente open source basato su algoritmi crittografici standard e non proprietari.
- Disponibile in più versioni: Gnu/Linux, Ms Windows, FreeBSD, OpenBSD, AIX, Sun Os, BSDI, IRIX, etc.
- Disponbili vari front-end per sistemi GUI: Gnome, KDE, Ms Windows, etc.
- Supporto algoritmi crittografici ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 e TIGER
- La versione attuale è la 1.2.1 rilasciata il 25 Ottobre 2002

Il confronto con il PGP

• **PGP:**
Architettura crittografica chiusa (DSS, RSA, IDEA...).
Software proprietario della PGP Corporation Inc. - ex NAI Inc.
Presenza di features “poco trasparenti” vedi bug sulle ADK e discussioni sul rilascio dei codici sorgenti con la nuova release 8.0.

• **GNUPG:**
Architettura aperta (algoritmi modulari)
Software non proprietario (libero), licenza GPL.
Ottimizzazione del codice, engine leggero, features essenziali

Lo standard OpenPGP (RFC 2440)

• Primo standard crittografico completo di stampo open source.

• Standard aperto per la cifratura/decifratura dei dati, firma digitale, autenticazione, gestione delle chiavi pubbliche/private

• Tentativo di affermare uno standard libero per applicazioni crittografiche in un ottica di difesa delle libertà digitali

• Perchè solo le istituzioni o grandi aziende possono utilizzare strong encryption?

• Per maggiori info: www.openpgp.org

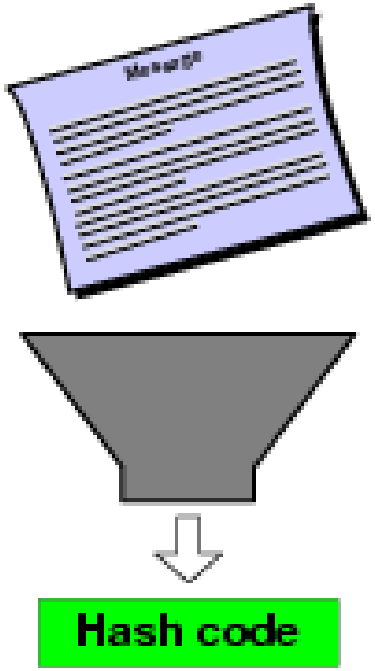
OpenPGP ALLIANCE

La firma digitale e le funzioni hash sicure

- Nasce come applicazione dei sistemi a chiave pubblica.
- Viene utilizzata per autenticare la paternità di un documento informatico e la sua integrità.
- Si utilizza un cifrario a chiave pubblica e si “cifra” un documento (file) con la propria chiave segreta. Chiunque può verificare la paternità del documento utilizzando la chiave pubblica dell'utente firmatario.
- Problema: per l'autenticazione di un documento di grandi dimensioni con un algoritmo a chiave pubblica occorre molto tempo.
- Soluzione: posso autenticare solo un “riassunto” del documento tramite l'utilizzo di una funzione hash sicura.

Le funzioni hash sicure

- Vengono utilizzate per generare un sorta di "riassunto" di un documento informatico (file).
- Una funzione hash accetta in ingresso un messaggio di lunghezza variabile M e produce in uscita un digest di messaggio H(M) di lunghezza fissa.
- Questo digest (impronta digitale, targa, riassunto) è strettamente legato al messaggio M, ogni messaggio M genera un H(M) univoco.
- Anche considerando due messaggi M ed M' differenti solo per un carattere le loro funzioni hash H(M) e H(M') saranno diverse.



Requisiti di una funzione hash sicura H(x):

- H può essere applicata a un blocco di dati di qualsiasi dimensione;
- H produce in uscita un risultato di lunghezza fissa (ad esempio 160 bit);
- Per qualunque codice h il calcolo di x tale che H(x)=h deve avere una complessità computazionale improponibile;
- Per qualunque blocco di dati x deve essere il calcolo di y≠x tale che H(x)=H(y) deve avere una complessità computazionale improponibile.
- Ai fini pratici H(x) deve essere relativamente semplice da calcolare.

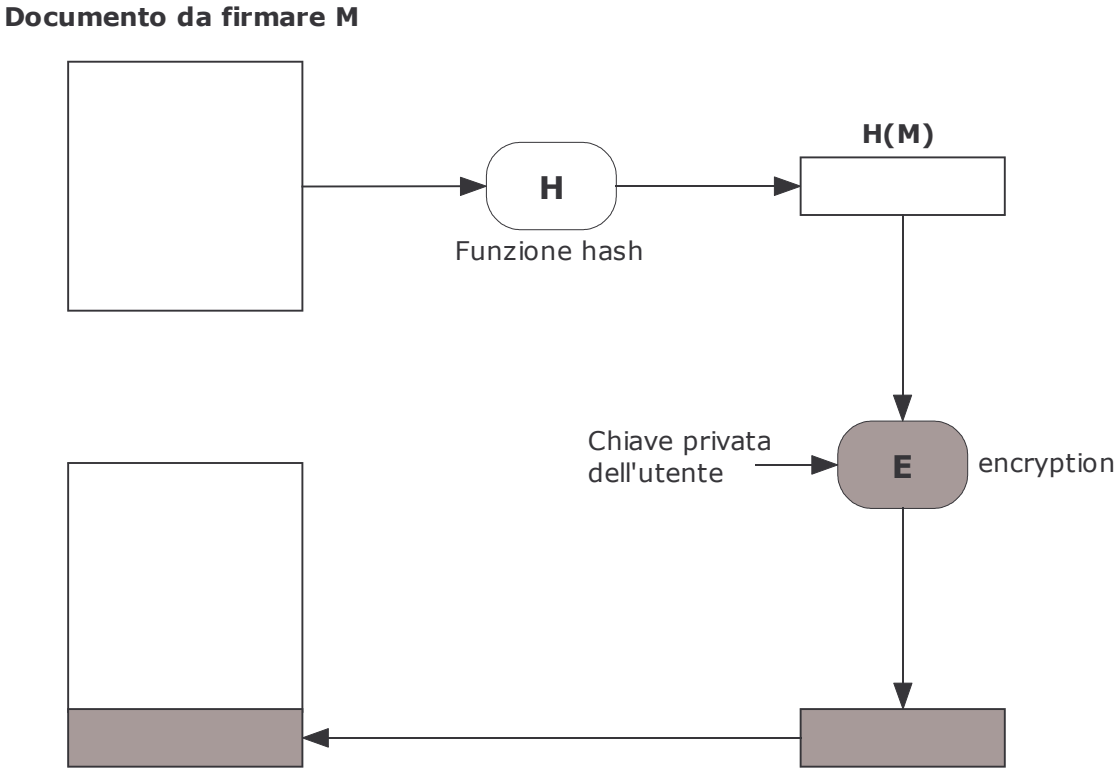
Esempio di funzione hash:

- Tutte le funzioni hash operano sulla base del seguente principio: i dati in ingresso sono considerati come una sequenza di blocchi di n bit, essi vengono elaborati un blocco alla volta iterativamente per produrre una funzione hash di n bit.
- Una delle più semplici funzioni hash è quella che esegue lo XOR (+) bit a bit di ciascun blocco, ossia:

$$C_i = b_{i1} + b_{i2} + \ldots + b_{im}$$

- Dove C_i rappresenta l'i-esimo bit del codice hash, m il numero di blocchi di n bit, b_{ij} l'i-esimo bit all'interno del j-esimo blocco e l'operatore + l'operazione di XOR.
- La probabilità che un errore nei dati produca lo stesso valore hash è 2^{-n}, con n=128 bit $2^{-128} \approx 2{,}9387*10^{-39}$.

Esempio di firma digitale di un documento:



Documento firmato:
Il ricevente può verificare
la firma utilizzando la
chiave pubblica dell'utente firmatario
e riapplicando la funzione hash

La nascita delle Certification Authority (CA)

- Dove trovo le chiavi pubbliche dei miei destinatari?
- Creazione di "archivi di chiavi pubbliche", i public key server.
- Ma chi mi garantisce la corrispondenza delle chiavi pubbliche con i legittimi proprietari?
- Nascita delle Certification Authority (CA).
- DPR 10 Novembre 1997, n. 513 (Capo I, Principi Generali, Art.1, Definizioni): *"Certificazione, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni; "*

Requisiti dei certificatori (DPR 10 novembre 1997, n.513)

- forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;

- possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;

- affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 3;

- Qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

Elenco pubblico dei certificatori in Italia

- In Italia esistono attualmente 15 entità di certificazione legalmente riconosciute dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) secondo l'articolo 27 comma 3 del DPR 28 dicembre 2000 n.445 specificato nel DPCM 8 febbraio 1999, esse sono:
- S.I.A. S.p.A., SSB S.p.A., BNL Multiservizi SpA, Infocamere SC.p.A., Finital S.p.A., Saritel SpA, Postecom S.p.A., Seceti S.p.A., Centro Tecnico per la RUPA, In.Te.S.A. S.p.A., ENEL.IT S.p.A., Trust Italia S.p.A. , Cedacrinord S.p.A., Actalis SpA, Consiglio Nazionale del Notariato.
- L'elenco è disponibile su internet all'indirizzo www.aipa.it

Il Decreto legislativo 23 gennaio 2002, n. 10

- **"Firma elettronica"** l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
- **"Firma digitale"** il risultato della procedura informatica (validazione) basata su di un sistema di chiavi asimmetriche a coppia, una pubblica e l'altra privata, che consente al sottoscrittore, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico...
- "**Firma elettronica avanzata**" la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

Il Decreto legislativo 23 gennaio 2002, n. 10

- Il documento informatico, quando è sottoscritto con **firma digitale** o con un altro tipo di **firma elettronica avanzata**, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.
- Al documento informatico, sottoscritto con **firma elettronica**, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

Esempi pratici d'utilizzo del software PGP e GnuPg