Crittografia

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

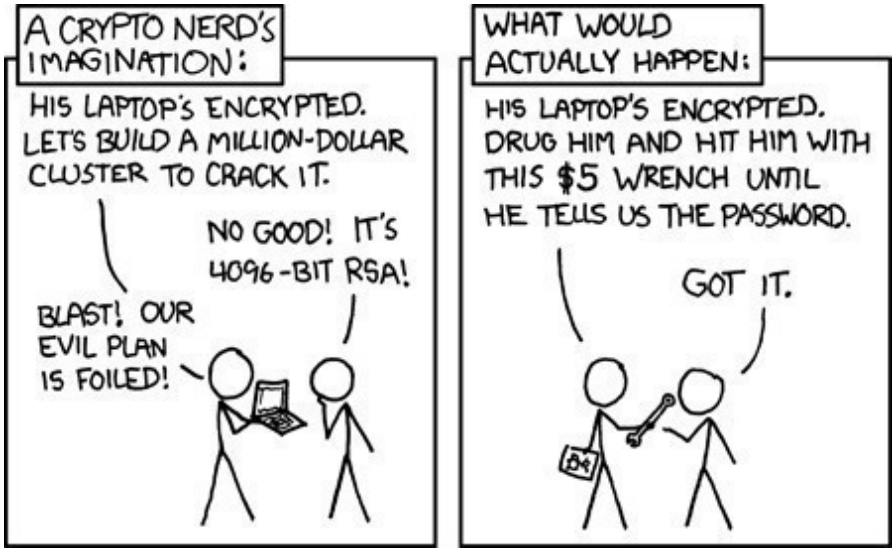
Crittografia

- Crittografia
- Certificati e firma digitale

..

Crittografia

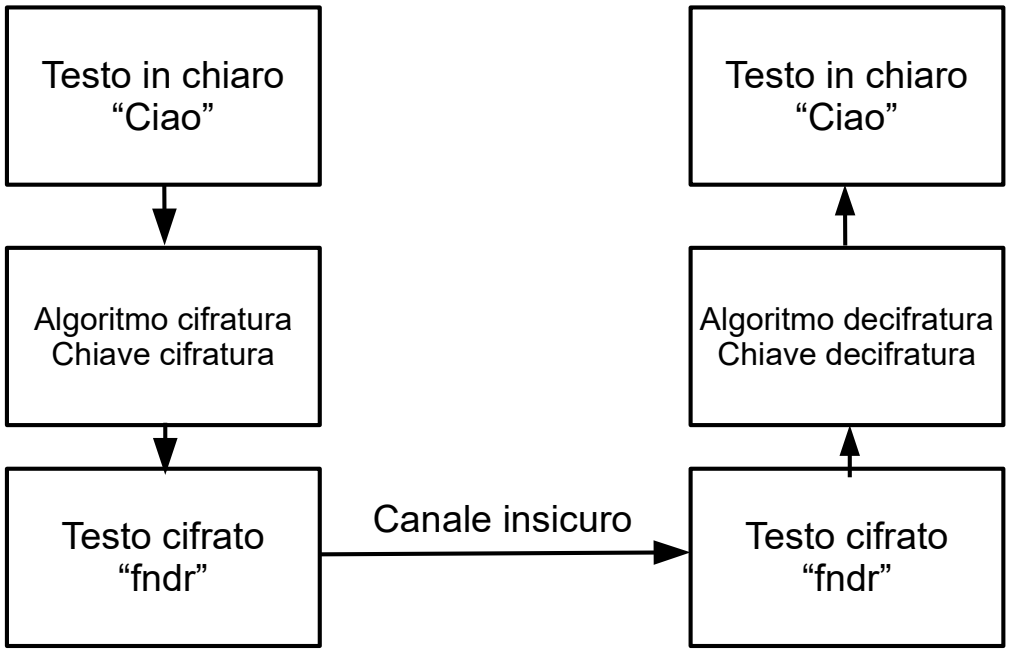
Crittografia



http://xkcd.com/538/

http://xkcd.com/538/

Crittografia



Principio di Kerckhoffs

“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.”

http://en.wikipedia.org/wiki/Kerckhoffs's_principle

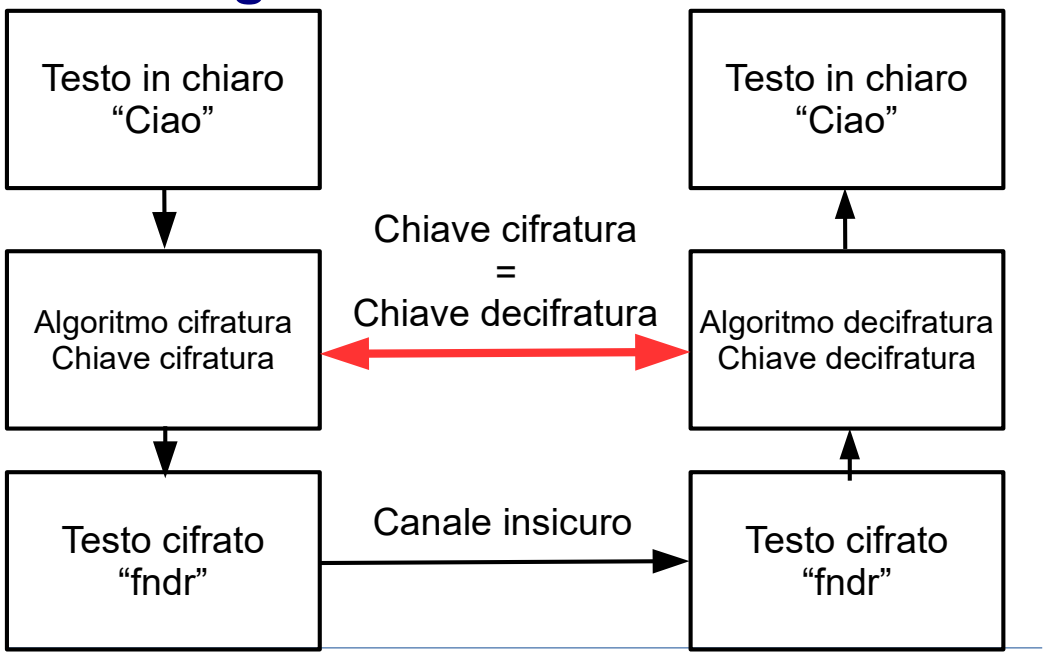
“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”

“It should not require secrecy, and it should not be a problem if it falls into enemy hands”

Auguste Kerckhoffs, "La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.

Il contrario di “Security by Obscurity”

Crittografia a chiave simmetrica



https://en.wikipedia.org/wiki/Symmetric-key_algorithm

Crittografia a chiave simmetrica

Vantaggi

- Algoritmi anche molto complessi ma veloci e con basso consumo di risorse
- Spazio delle chiavi molto ampio quindi più robusto
- Algoritmo di decifratura simmetrico a cifratura
- Sicurezza dipende solo dalla chiave
- Numero di chiavi cresce in modo esponenziale

Svantaggi

- Scambio della chiave

Esempi

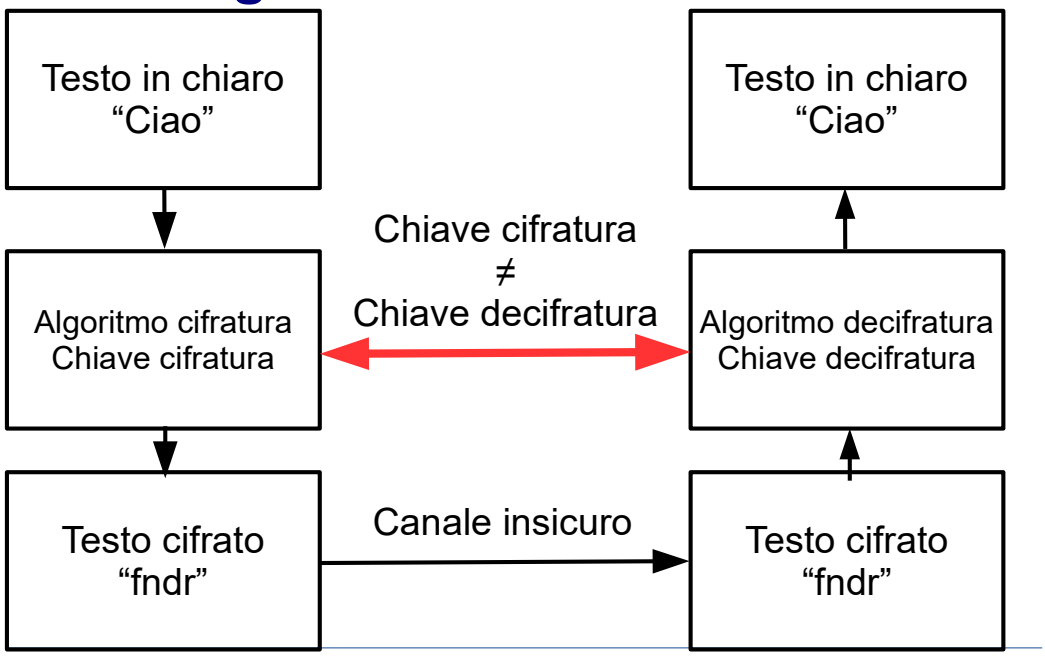
- Blowfish, 3DES

https://en.wikipedia.org/wiki/Blowfish_(cipher)

https://en.wikipedia.org/wiki/Triple_DES

20 colloqui = 19 chiavi per ogni utente = 190 chiavi da gestire (20*19/2)

Crittografia a chiave asimmetrica



https://en.wikipedia.org/wiki/Public-key_cryptography

Crittografia a chiave asimmetrica

Svantaggi

- Algoritmi molto complessi e lenti
- Spazio delle chiavi meno ampio
- Algoritmo di decifratura asimmetrico rispetto a quello di cifratura
- Introduce un ente terzo (CA)
- Numero di chiavi cresce linearmente

Vantaggi

- Lo scambio della chiave non è più un problema

Esempi

- RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

20 colloqui = 20 chiavi pubbliche e 20 chiavi private = 40 chiavi

Quindi come ne esco ?

Uso l'algoritmo asimmetrico a chiave pubblica per scambiarmi la chiave segreta dell'algoritmo simmetrico, poi uso l'algoritmo simmetrico per la cifratura del resto.

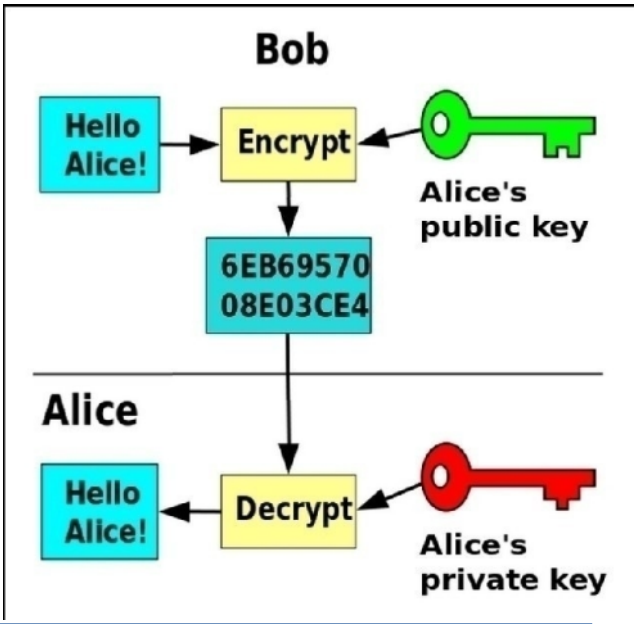
Ma si capisce meglio con un esempio dal vero ...

Esempio con scatola di legno e due lucchetti

Crittografia

Crittografia a chiave asimmetrica

- Coppia di chiavi
- Tecniche matematiche



http://en.wikipedia.org/wiki/Public-key_cryptography

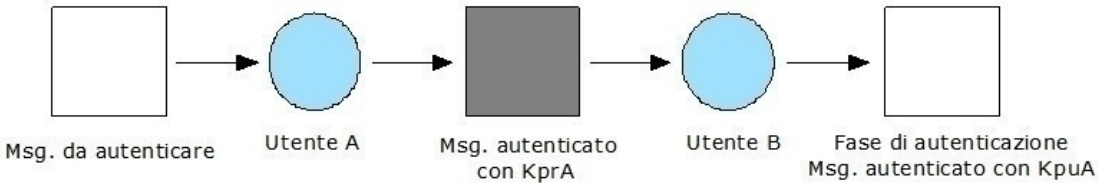
Coppia di chiavi: chiave pubblica (public key) per encryption e chiave privata (private key) per decryption

Utilizza tecniche di tipo matematico basate sulla teoria dei numeri, sulla teoria delle curve ellittiche, sull'asimmetria di alcune operazioni matematiche (es. fattorizzazione 127*157=19939) etc.

(ecco chi sono Alice e Bob, https://en.wikipedia.org/wiki/Alice_and_Bob)

Crittografia a chiave asimmetrica

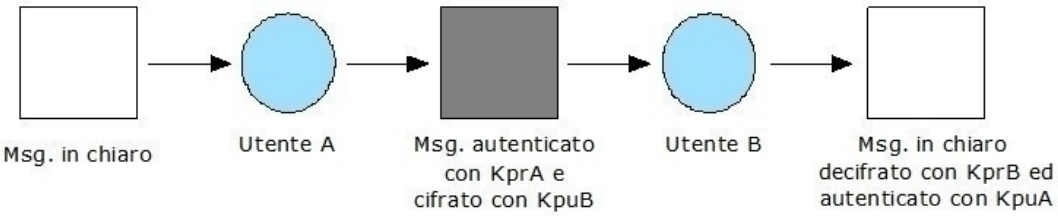
Posso usarla anche per fare autenticazione



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A

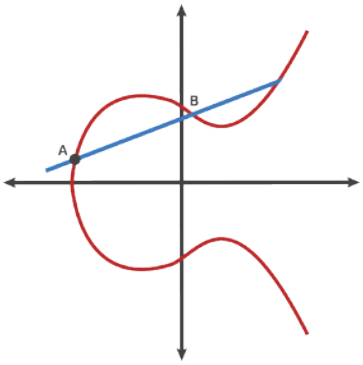
Crittografia a chiave asimmetrica

Oppure per fare autenticazione e crittografia



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A
KprB = chiave privata dell'utente B
KpuB = chiave pubblica dell'utente B

Crittografia ellittica



Crittografia ellittica (in inglese Elliptic Curve Cryptography o anche ECC). Asimmetrica.
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

A 256 bit key in ECC offers about the same security as 3072 bit key using RSA.
Starting at A:
A dot B = -C (Draw a line from A to B and it intersects at -C) Reflect across the X axis from -C to C
A dot C = -D (Draw a line from A to C and it intersects -D) Reflect across the X axis from -D to D
A dot D = -E (Draw a line from A to D and it intersects -E) Reflect across the X axis from -E to E

Public Key: Starting Point A, Ending Point E
Private Key: Number of hops from A to E
https://blog.goodaudience.com/very-basic-elliptic-curve-cryptography-16c4f6c349ed

Attacchi alla crittografia

Attacco esaustivo (o “brute force”)
→ numero tentativi pari a

$$2^N$$

Con N= lunghezza della chiave crittografica in bit.
Lunghezze ritenute “***sicure***” ***oggi***:

- Chiavi simmetriche: 192-256 bit
- Chiavi asimmetriche: 2048 bit

“Sicure” si intende a fronte di un attacco “normale” (no governi, servizi segreti, criminalità organizzata internazionale ecc.)

“Oggi” perché con i miglioramenti di hardware e software domattina potrebbe non essere più vero.

Utilizzo di GPU come potenza di calcolo per attacchi forza bruta.

Computer quantistici

Algoritmo di fattorizzazione di Shor

Fattorizzazione di un numero di 230 cifre

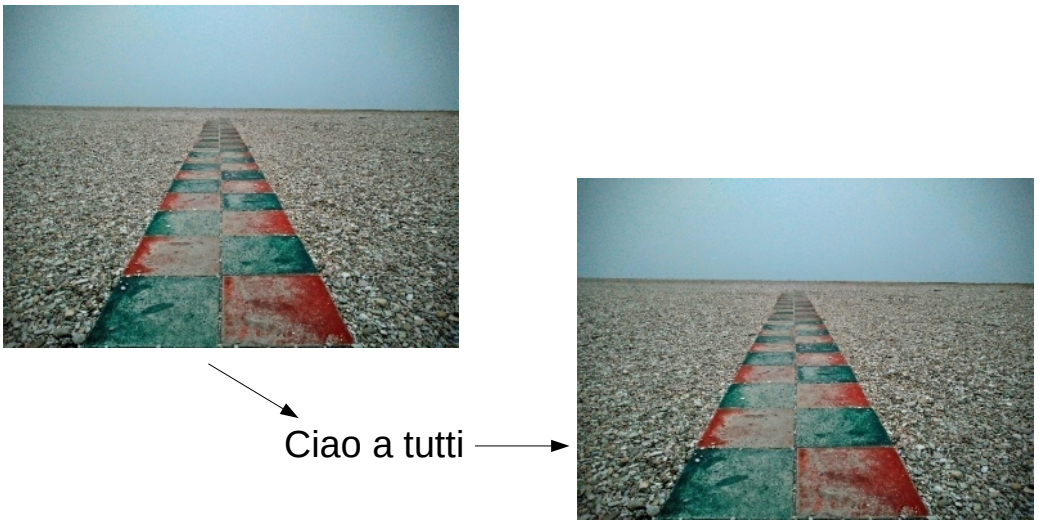
Computer tradizionale=1,68 anni

Computer quantistico=5,32 picosecondi

Computer quantistici in grado di cambiare completamente le carte in tavola. (descrizione out-of-scope).
Aumento esponenziale velocità con piccole operazioni altamente parallelizzabili.
Algoritmi specifici per sfruttarli al massimo: algoritmo di fattorizzazione di Shor
https://en.wikipedia.org/wiki/Shor%27s_algorithm
Servono nuovi algoritmi di crittografia: crittografia post-quantistica
https://en.wikipedia.org/wiki/Post-quantum_cryptography

Crittografia

Steganografia



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo 18

https://en.wikipedia.org/wiki/Steganography

Steganografia è la crittografia nascosta. Se vedo un messaggio cifrato lo riconosco, obiettivo della steganografia è nascondere il fatto che ci sia un messaggio nascosto.

Affonda le radici nella storia (uovo, capelli).

Più recentemente applicata alle immagini sfruttando piccole modifiche ai bit di colore, indistinguibili all'occhio umano ma in grado di codificare un messaggio. In questo caso la chiave è l'immagine originale da cui, per differenze, ricavo il messaggio.

(immagine modificata usando OpenStego http://www.openstego.com/)

Steganografia

https://en.wikipedia.org/wiki/Steganography

Non solo immagini come vettore di trasporto, anche audio, video, pdf ecc.

https://www.darknet.org.uk/2017/07/openpuff-professional-steganography-tool/

Posso crittografare i dati prima di nasconderli, posso lavorare a più livelli (nascondo un messaggio non troppo segreto sopra ad uno più segreto in modo da fermare la ricerca dell'attaccante).

Steganografia

Document fingerprinting
(watermark nascosto)

Queste tre stringhe sono diverse
Queste tre stringhe sono diverse
Queste tre stringhe sono diverse

Posso usare la steganografia anche per fare un watermarking nascosto dei documenti (in caso di fuga dei documenti posso distinguere le diverse copie anche se apparentemente sono uguali, impronte digitali dei documenti).

Tecniche steganografiche sulle immagini, uso di “spazi di lunghezza zero” (seconda riga dopo “queste”) oppure di caratteri di alfabeti non latini (terza riga seconda e) nei testi.

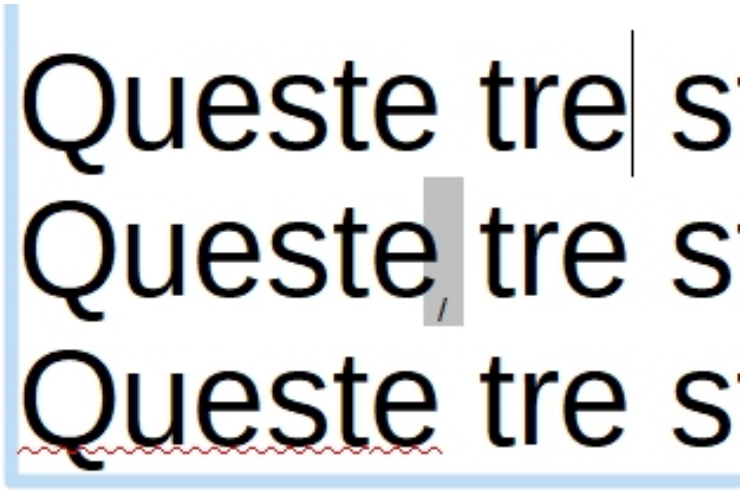
https://www.zachaysan.com/writing/2017-12-30-zero-width-characters

https://www.researchgate.net/publication/308044170_Content-preserving_Text_Watermarking_through_Unicode_Homoglyph_Substitution

http://blog.fastforwardlabs.com/2017/06/23/fingerprinting-documents-with-steganography.html

Crittografia

Steganografia



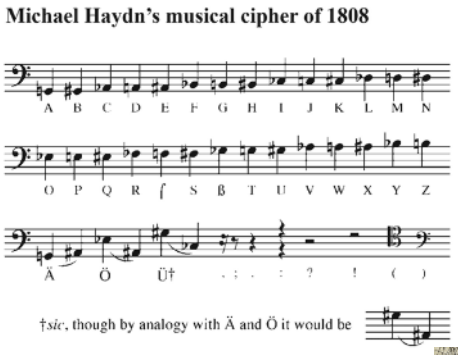
Posso usare la steganografia anche per fare un watermarking nascosto dei documenti (in caso di fuga dei documenti posso distinguere le diverse copie anche se apparentemente sono uguali).

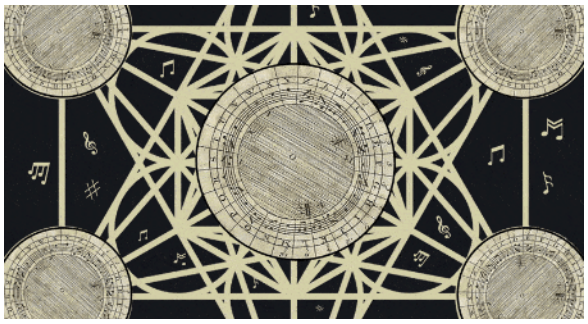
Tecniche steganografiche sulle immagini, uso di “spazi di lunghezza zero” (seconda riga dopo “queste”) oppure di caratteri di alfabeti non latini (terza riga seconda e) nei testi.

In alternativa posso usare minime perturbazioni della forma dei caratteri
https://www.youtube.com/watch?v=dejrBf9jW24

Demo su internet
https://www.umpox.com/zero-width-detection/

Crittografia





Steganografia dal passato , nascondere il messaggio nella musica. Uso codifiche con note musicali
https://www.atlasobscura.com/articles/musical-cryptography-codes

Create il vostro messaggio sonoro cifrato:
https://wmich.edu/mus-theo/solfa-cipher/

Certificazione della chiave pubblica

Certificato digitale

http://en.wikipedia.org/wiki/Public_key_certificate
- Certificazione della chiave pubblica o più semplicemente “certificato digitale”.

E' l'associazione della chiave pubblica dell'utente alla sua identità fisica.

Unisce il mondo online con quello offline (non sempre, potrei anche certificare un'identità digitale o un indirizzo IP).

Serve un garante delle identità: Certification Authority

Le Certification Authority debbono avere una gerarchia.

Un certificato può essere revocato (CRL) sia dall'emettitore che dal richiedente.

Deve avere una scadenza temporale.

Formato dei certificati
X.509

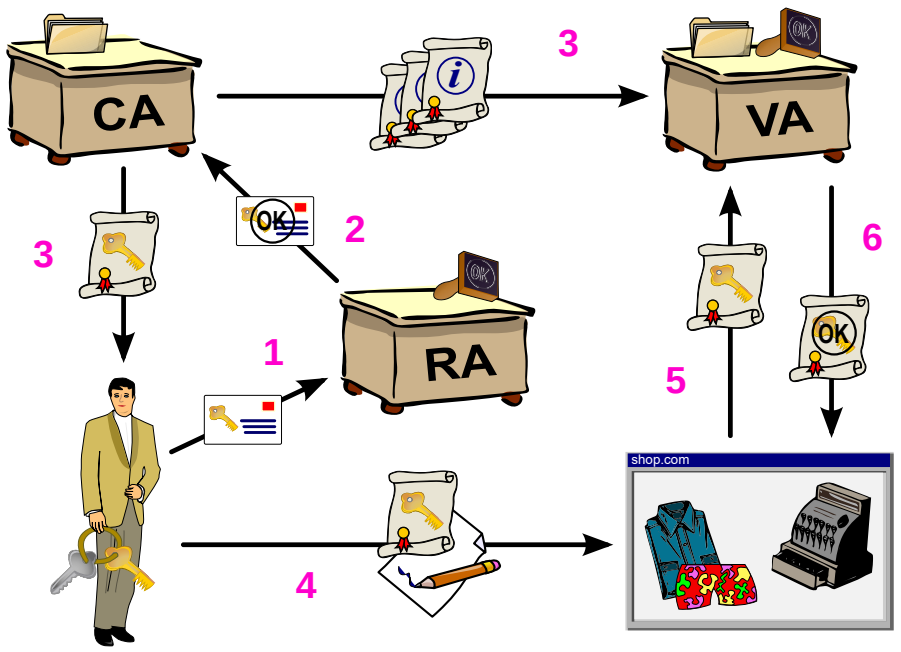
Formato standard dei certificati: X.509
http://en.wikipedia.org/wiki/X.509
Deve contenere:

- Periodo di validità
- Soggetto
- Nome dell'autorità emittente
- Chiave pubblica
- Firma digitale dell'autorità emittente

Più altri campi opzionali:

- Scopi di uso del certificato (validare sito web ecc.)
- Nomi alternativi del soggetto (esempio metto mail, IP, URL ecc.)
- Estensioni private utilizzabili, ad esempio, a livello di azienda

Certificati e firma digitale



PKI (Public Key Infrastructure)
https://en.wikipedia.org/wiki/Public_key_infrastructure
Certificate Authority (CA) Genera i certificati, garantendo la corrispondenza tra una chiave pubblica e un soggetto.
Registration Authority (RA):identifica il soggetto
Validation Authority (VA): valida il certificato al client

By Chris 論 - [1] and OpenCliparts.org, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2501151

Certificati e firma digitale

CA riconosciute nel browser.
Certificato a pagamento, dipende dal tipo, qualche centinaio di Euro/anno.
Certificati gratis per siti web: https://letsencrypt.org/
"Let's Encrypt is a free, automated, and open certificate authority brought to you by the non-profit Internet Security Research Group (ISRG)."

Motivi di revoca di un certificato prima della scadenza:
- Azienda non esiste più
• Compromissione di chiave privata
• Persa la passphrase associata alla chiave privata
• Cambio di informazioni nel certificato

Vedere errori di certificato:
https://badssl.com/

Certificati e firma digitale

HACKING DEFCON 23'S IOT VILLAGE SAMSUNG FRIDGE

Posted on Tuesday, August 18th, 2015 by Pedro Venda.

pwned?

As well as running the Village this year (more challenge:

"Can you own our #IoT

As a team we're doing opportunity to work on

It was a full-on team ef here.

Se non controllo che il certificato presentato sia valido … il nemico può annidarsi ovunque … il tuo frigorifero può rivelare le tue credenziali Gmail con un attacco "Man in the Middle".

http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

Funzioni di hash

- Da testo a stringa di lunghezza fissa
- Algoritmi unidirezionali
- Variazione produce modifica non correlabile
- Basso costo computazionale
- Non ci debbono essere collisioni
- Distribuzione uniforme dell'hash
- Usato per verificare che un testo non sia stato modificato
- MD5 - SHA-*

http://en.wikipedia.org/wiki/Cryptographic_hash_function

Trasformano un testo in una stringa di lunghezza fissa (message digest o riassunto)
Algoritmi unidirezionali (è praticamente impossibile risalire dalla stringa al testo originale)
Una piccola variazione al testo originale produce una modifica non facilmente correlabile alla stringa
Basso costo computazionale
Non ci debbono essere collisioni
Distribuzione uniforme hash riduce rischio collisioni
Usato per verificare che un messaggio/documento non sia stato modificato
Esempio: MD5 http://en.wikipedia.org/wiki/MD5
SHA-1 (old) SHA-3 (Ethereum) SHA-256 (bitcoin)
https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
https://medium.com/@rauljordan/the-state-of-hashing-algorithms-the-why-the-how-and-the-future-b21d5c0440de

Funzioni di hash

Utilizzate per salvare le password sul server (meglio aggiungere un po' di sale)

Utente scrive la password, il server calcola hash della password e lo confronta con quello che ha memorizzato. Se uguali autenticazione OK. Se hash non è reversibile e non ha collisioni posso fare autenticazione sicura senza memorizzare la password in chiaro.

Se algoritmo di hash noto posso fare attacco a dizionario o a tabella (conosco tutti gli hash di quell'algoritmo).

Per evitare aggiungo un valore alla password (salt).

Per ogni utente genero un salt diverso (lungo e con caratteri poco usati). Calcolo hash=(password + salt). Memorizzo sul server: utente, hash, salt. Faccio stesso calcolo per verificare password. Password uguali hanno hash-salted diverso. Rende molto più difficili gli attacchi dizionario.

https://en.wikipedia.org/wiki/Salt_(cryptography)

Funzioni di hash

Varianti specifiche per la protezione delle password: bcrypt, PBKDF2

AMD Radeon HD 7970, 500$
258.7M SHA1 Hash per second

Con l'aumento delle velocità di crack gli algoritmi tradizionali (MD5, SHA*) sono diventati attaccabili anche con salt.

Meglio passare ad algoritmi più lenti da applicare ma anche molto più lenti da attaccare.

https://en.wikipedia.org/wiki/Bcrypt

https://www.troyhunt.com/our-password-hashing-has-no-clothes/

Posso usare tempo GPU in cloud.

20 Hours, $18, and 11 Million Passwords Cracked

I ran Hashcat on a Nvidia Tesla K80 — a GPU with 4992 cores that you can rent on AWS for $0.90 per hour (P2.xlarge).

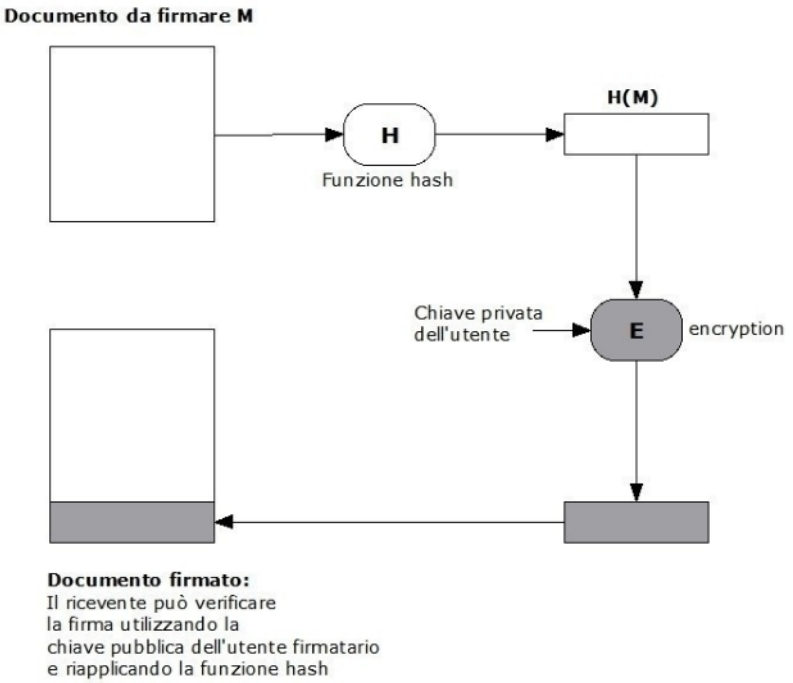
https://medium.com/hackernoon/20-hours-18-and-11-million-passwords-cracked-c4513f61fdb1

Firma digitale

http://en.wikipedia.org/wiki/Digital_signature

Uso crittografia asimmetrica, certificati digitali e funzioni di hash per firmare digitalmente un documento.

Certificati e firma digitale



Chiave privata su dispositivo di firma sicuro a garanzia dell'"Identità digitale" (ad esempio smart card protetta da PIN).

Il documento non è crittografato, viene nascosto solo l'hash.

Decodificando l'hash con la chiave pubblica del mittente ne verifico l'identità.

Confrontando l'hash decodificato con quello calcolato verifico l'integrità del documento.

Vale anche come "non ripudio" (con tutte le cautele giuridiche del caso: volontà della firma, consapevolezza della firma).

Time stamp Protocol

Uso crittografia asimmetrica, certificati digitali e funzioni di hash + un servizio di time stamp online (TSA Time Stamping Authority, Marca temporale) per datare digitalmente un documento (ad esempio per poterne stabilire in seguito la paternità).

“La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell’Amministrazione Digitale Dlgs 82/2005).”

https://www.pec.it/marche-temporali.aspx