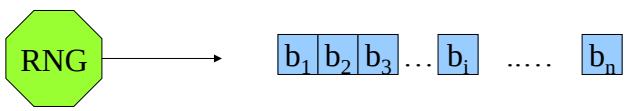
MECCANISMI DI BASE:
•Generatori di bit casuali

Random Number/Bit Generator



Proprietà di casualità dei bit:
• indipendenza statistica
• valori equiprobabili

Test statistici (FIPS 140-2): $\chi 2$
•Monobit: *numero* di 1 e di 0
•Pocker: *sequenze* di M bit
•Run: *block* (1) e *gap* (0)
•Long Run: *block* più lungo

Altri test statistici:
•Autocor.: *differenze* dopo shift
•TdF: *distanza* pattern ripetitivi
•Compressione LZ: *lunghezza*
• ...

True Random Number Generator

•Fenomeni fisici:

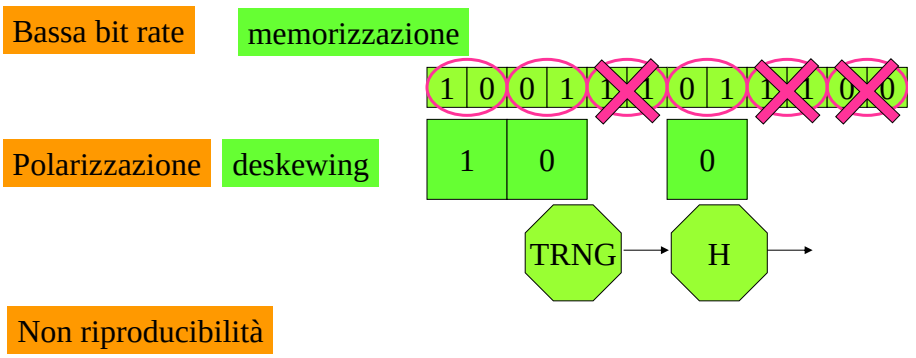
Decadimento radioattivo, rumore termico, turbolenza di un fluido

•Segnali di apparati elettronici:

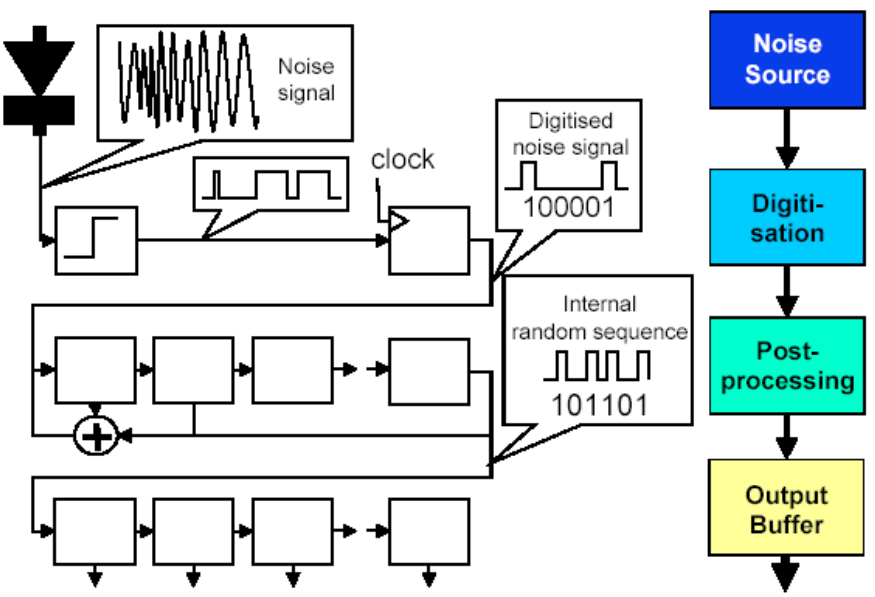
Microfono, telecamera, oscillatore

•Programmi di estrazione di rumore dal funzionamento del computer

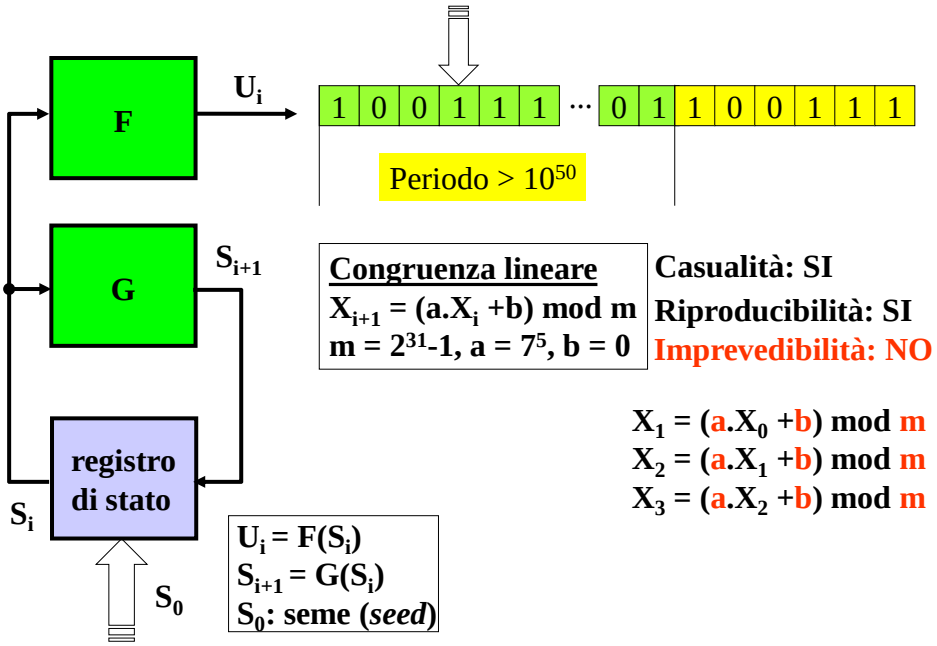
Tastiera, Mouse, n° di processi attivi, traffico di rete



Elaborazione del rumore



Pseudo Random Number Generator



Congruenza lineare
$X_{i+1} = (a.X_i + b) \bmod m$
$m = 2^{31}-1,\ a = 7^5,\ b = 0$

Casualità: SI
Riproducibilità: SI
Imprevedibilità: NO

$X_1 = (a.X_0 + b) \bmod m$
$X_2 = (a.X_1 + b) \bmod m$
$X_3 = (a.X_2 + b) \bmod m$

$U_i = F(S_i)$
$S_{i+1} = G(S_i)$
S_0: seme (*seed*)

Cryptographically Secure PseudoRandom Bit Generator

casualità dell'uscita — Test statistici

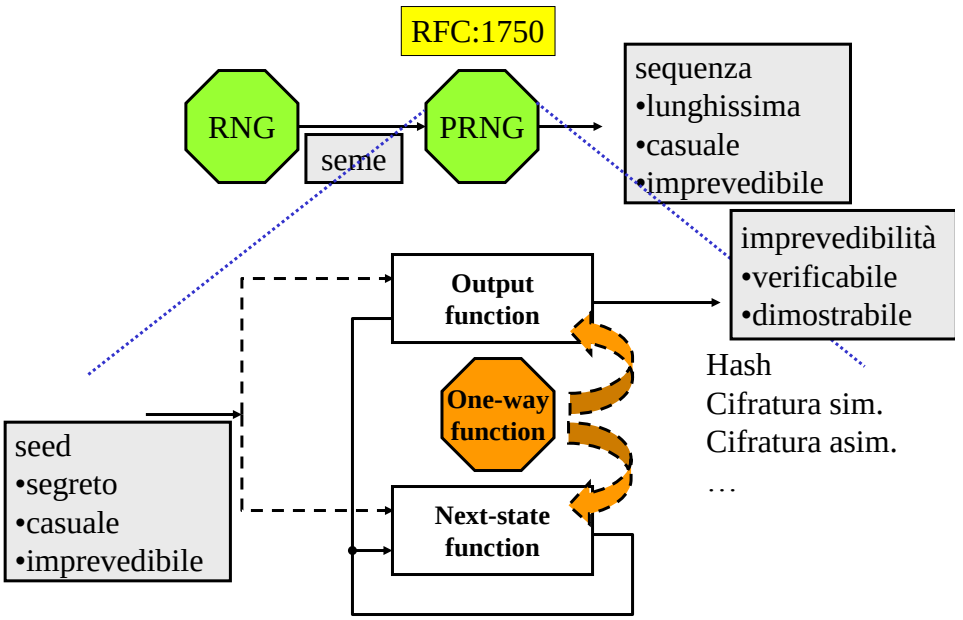
imprevedibilità dell'uscita — **Next-bit test**: dati L bit della stringa d'uscita non deve esistere un algoritmo polinomiale in grado di predire il bit L+1-esimo con probabilità > 0,5

indeducibilità del seed — One-way function

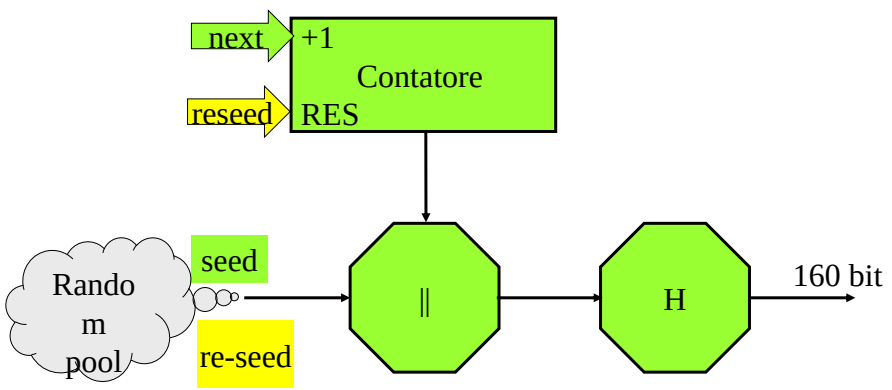
Crittografia simmetrica:
- verifica sperimentale
- alta velocità

Crittografia asimmetrica:
- dimostrazione teorica
- bassa velocità

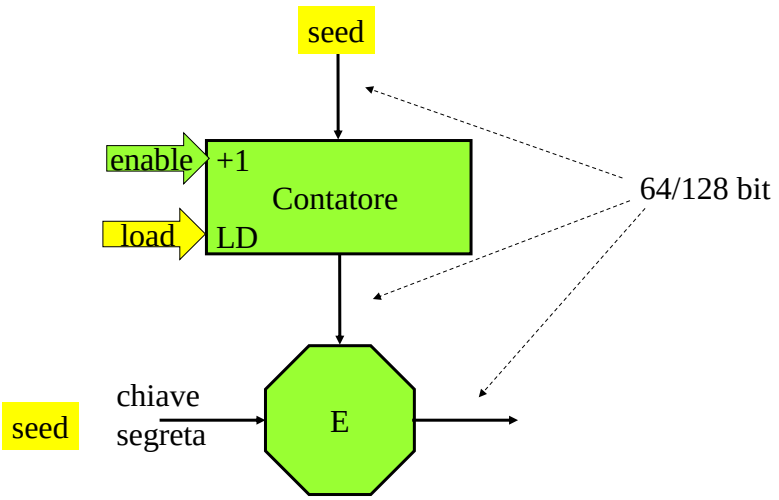
PRNG crittografico



Secure Random di Java

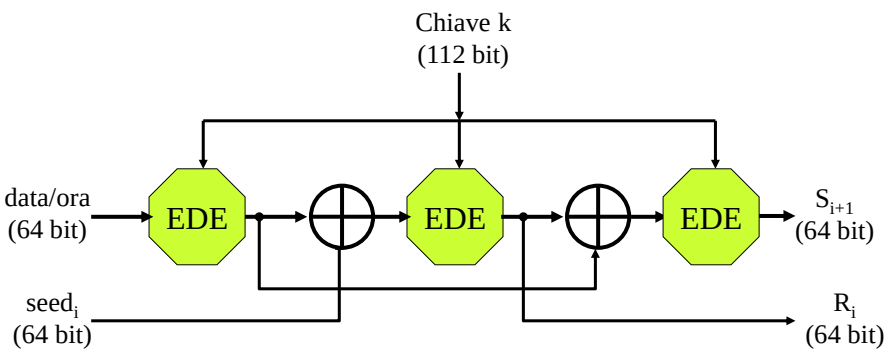


PRNG con cifratura di un contatore



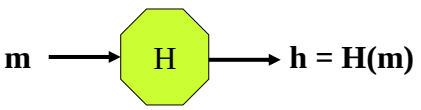
PRNG X9.17

Obiettivo: chiavi e vettori di inizializzazione per il DES
Meccanismo: TDES a due chiavi



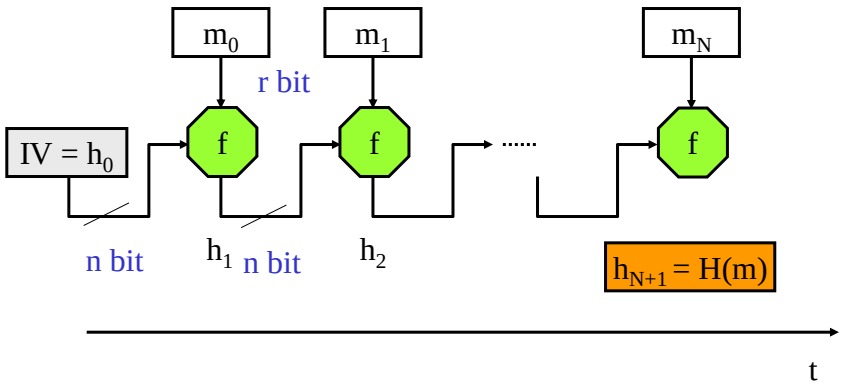
MECCANISMI DI BASE:
•Algoritmi di hash

Algoritmi di hash: proprietà

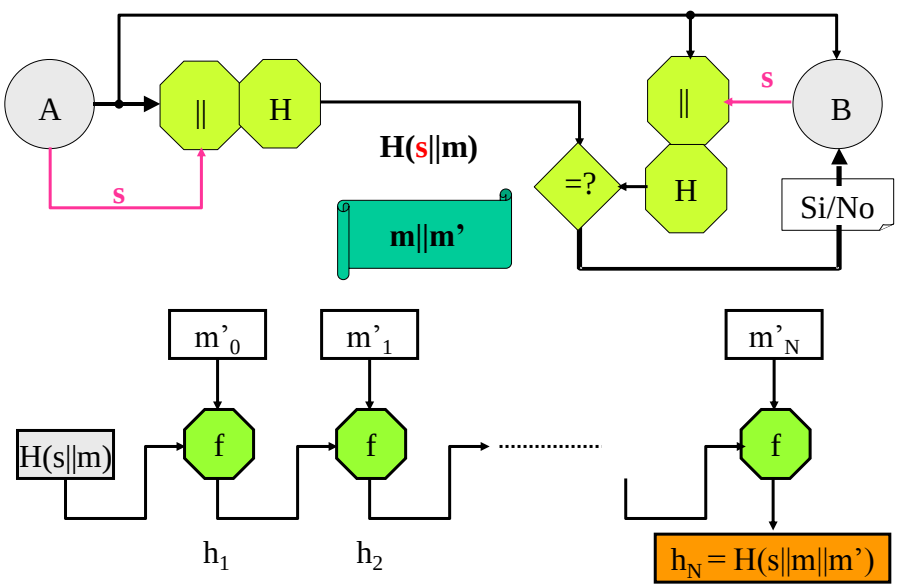


- R18(efficienza: "*il calcolo di H(x) deve essere facile per ogni x*"
- R19 (robustezza debole alle collisioni): "*per ogni x deve essere infattibile trovare un y ≠x tale che H(y) = H(x)*"
- R20 (robustezza forte alle collisioni): "*deve essere infattibile trovare una qualsiasi coppia y, x tale che H(y) = H(x)*"
- R21 (unidirezionalità): "*per ogni h deve essere infattibile trovare un x tale che H(x) = h*"

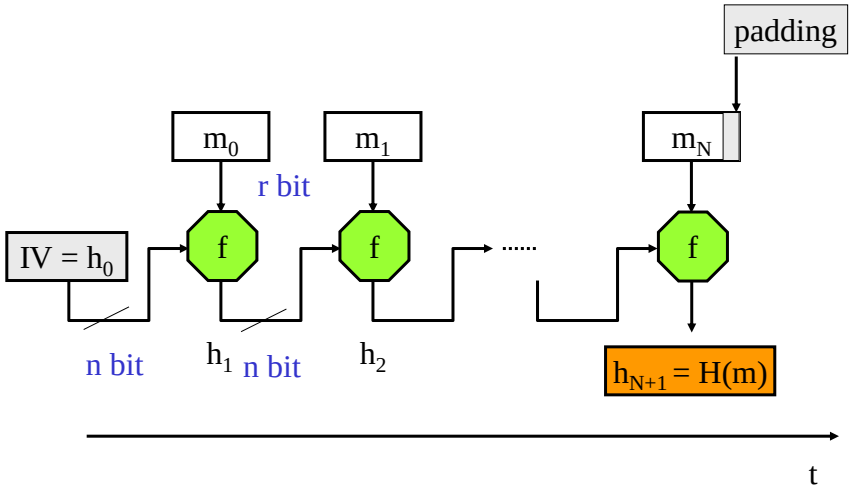
Efficienza: compressione iterata



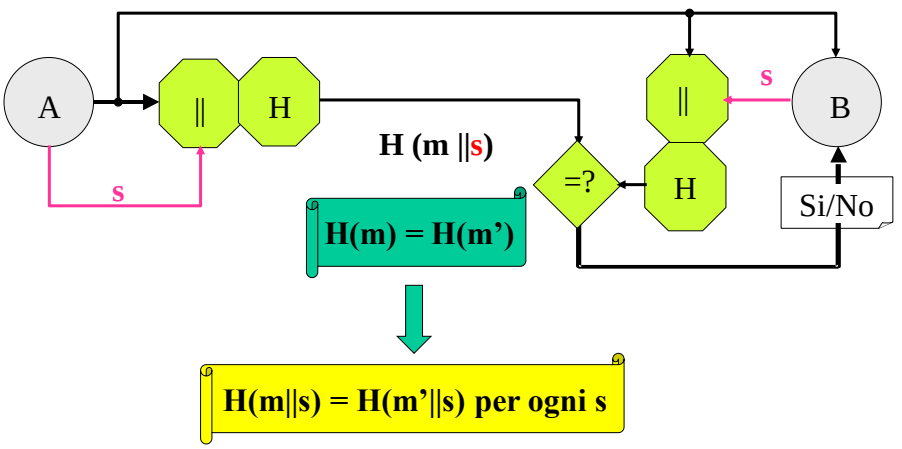
Attacco con lenght extension



Efficienza: compressione iterata



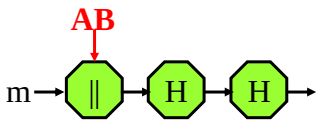
Attacco al segreto con una collisione



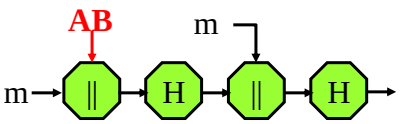
Contromisura: impronta di un'impronta

m messaggio
AB segreto condiviso da A e da B

- H(H(AB||m))

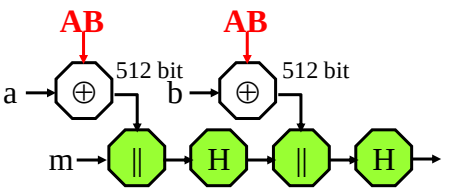


- H(H(AB||m)||m)

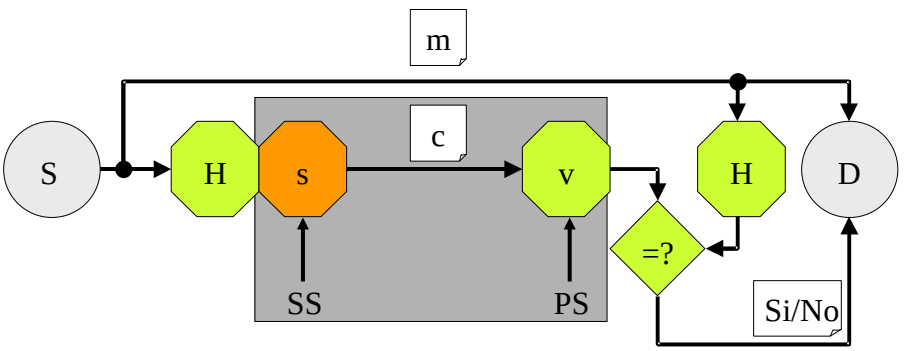


- HMAC(AB, m)

RFC(2104)



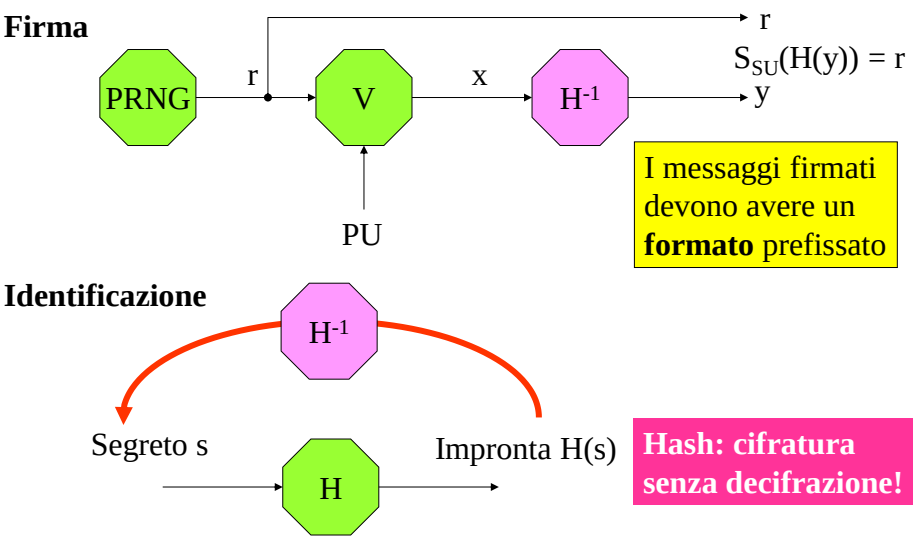
Resistenza alle collisioni e firma digitale



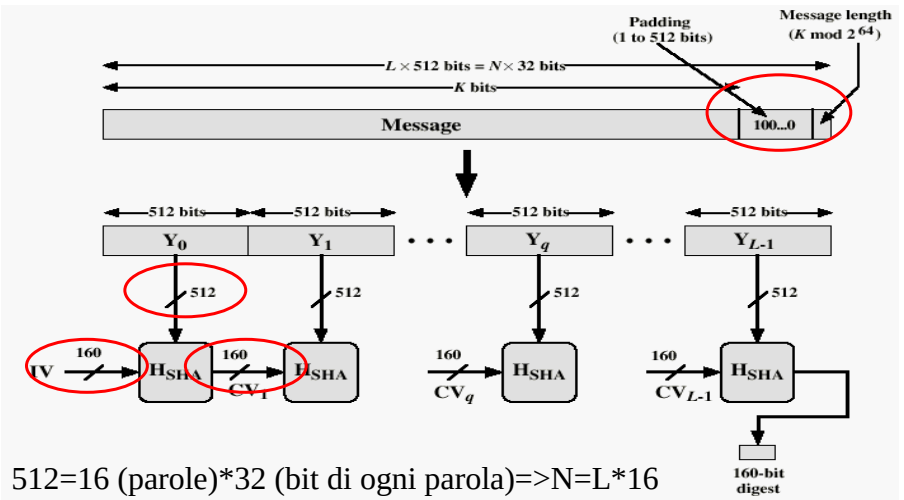
Quando valgono R19, R20 l'impronta **H(m) identifica m**

Con la firma di H(m) si ottiene:
•efficienza
•individuazione di modifiche a **m** e/o a **c** apportate dall'intruso
•S non può sostenere di aver inviato **m*** e non **m**
•D non può sostenere di aver ricevuto da S un **m*** da lui inventato

R21: unidirezionalità (non invertibilità)



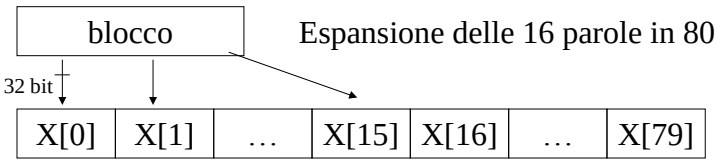
Message Digest Generation Using SHA-1



512=16 (parole)*32 (bit di ogni parola)=>N=L*16

SHA-1

512 bit (16 parole di 32 bit)

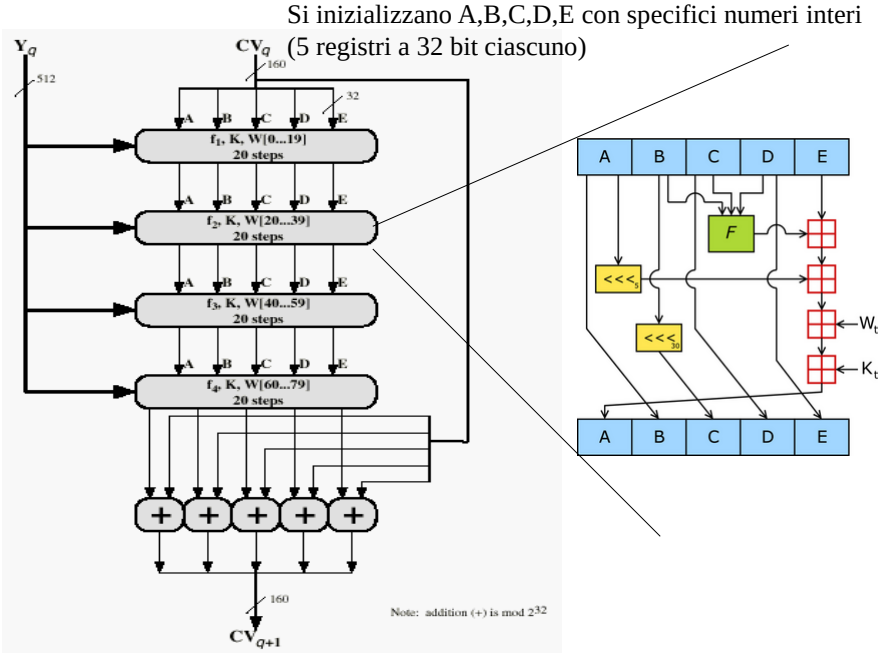


Espansione delle 16 parole in 80 parole

Espansione tramite operazioni di X-or tra
parole precedenti e operazioni scorrimento

SHA-1

Si inizializzano A,B,C,D,E con specifici numeri interi
(5 registri a 32 bit ciascuno)



Secure HASH functions

Algoritmi di hash più noti ed usati	**MD5 1991**	**SHA-1 1994**	**RIPEMD-160 1996**
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
Number of steps	64 (4 rounds of 16)	80 (4 rounds of 20)	160 (5 paired rounds of 16)
Maximum message size	∞	2^{64}-1 bits	∞

Tiger (1996)
192 bit

NIST 2002:
SHA-256
SHA-384
SHA-512

Whirlpool (2002)
512 bit

SHA-3 (2015)

Funzione Hash crittografica: dimensionamento dell'impronta

Quanti bit deve avere un'impronta per essere sicura?

Complessità del calcolo di una collisione

IPOTESI: una funzione hash sottoposta ad ingressi scelti a caso restituisce, con eguale probabilità, uno dei suoi 2^n valori d'uscita.

Problema: individuare un ingresso che fornisca un'impronta assegnata

un tentativo: probabilità di successo $\mathbf{P_1(2^n, 1) = 2^{-n}}$,
probabilità di insuccesso $\mathbf{1 - 2^{-n}}$.

k tentativi: probabilità di successo $\mathbf{P_1(2^n, k) = 1 - (1 - 2^{-n})^k}$

Teorema binomiale: $(b+a)^n = \sum_{i=0}^{n} \binom{n}{i} b^i a^{n-i}$

$$\mathbf{(1- 2^{-n})^k = 1- k\,2^{-n} + k(k-1)\,2^{-2n}/2! - k(k-1)(k-2)\,2^{-3n}/3! + ..}$$

$\mathbf{P_1(2^n, k)} = \mathbf{k.\,2^{-n} - k.(k-1).\,2^{-2n}/2 + k.(k-1).(k-2).\,2^{-3n}/6 - ..}$ ecc.

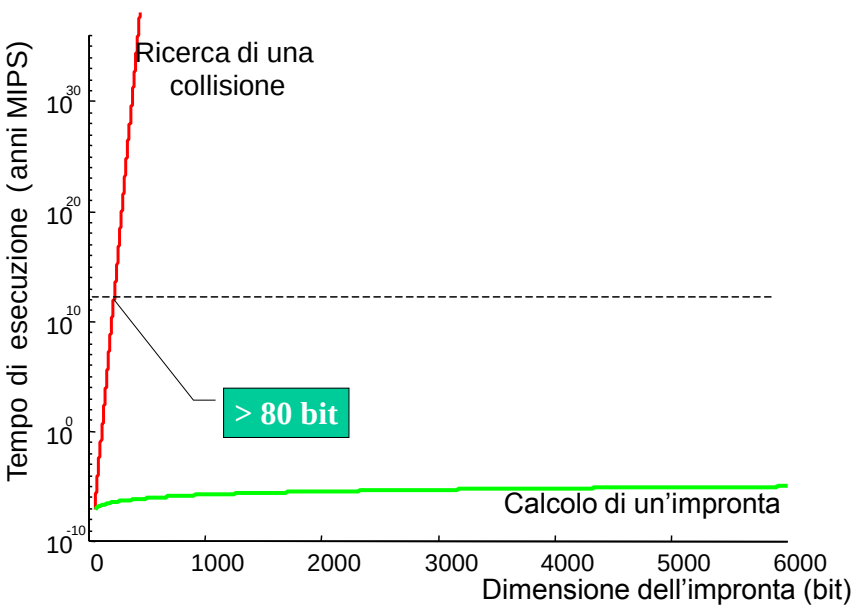
$\cong \mathbf{k.\,2^{-n}}$ quando $\mathbf{2^{-n}}$ è molto piccolo

S: probabilità di successo desiderata

$\mathbf{S = P_1(2^n, k) \rightarrow k = S.2^n}$

O(exp(n))

Robustezza debole alle collisioni



Un Possibile Attacco in assenza di Resistenza debole

L'intruso prepara 2 versioni di un contratto M ed M´
a) M è favorevole ad Alice
b) M´ è sfavorevole ad Alice
modifica M´ a caso (piccoli cambiamenti come aggiunta spazi) finchè h(M) = h(M´)

Alice firma M ⇒ $Firma_{kpriv}(h(M))$

L'intruso ha quindi la firma di M´ ⇒ $Firma_{kpriv}(h(M'))$

Un Possibile Attacco in assenza di Resistenza debole

Cara Alice,

ti { scrivo / sto scrivendo

Il paradosso del giorno del compleanno

Birthday paradox

Nell'ipotesi che le date di nascita siano equiprobabili, è sufficiente scegliere a caso **253** persone per avere una probabilità > 0,5 che una di queste compia gli anni in un dato giorno.

Sono invece sufficienti **23** persone scelte a caso per avere una probabilità > 0,5 che due o più compiano gli anni nello stesso giorno.

Calcolo di due input in collisioni

$P_2(2^n, k)$ probabilità di due uscite identiche con **$k \leq 2^n$** ingressi scelti a caso

- sequenze d'uscita possibili: **$(2^n)^k$** differenti
- sequenze con valori tutti diversi: **$2^n! / (2^n - k)!$**

$$P_2(2^n, k) = 1 - \frac{(2^n! / (2^n - k)!)}{(2^n)^k} \quad \begin{matrix} \text{tutti diversi} \\ \text{tutti} \end{matrix}$$

$$= 1 - (2^n \times (2^n-1) \times (2^n-2) \times \ldots \times (2^n-k+1)) / 2^{n\,k}$$

$$= 1 - (1-1/2^n)(1-2/2^n) \ldots (1-(k-1)/2^n)$$

N.B. $(1-x) \leq e^{-x}$ *è valida per* $x \geq 0$,

e^{-x} *è una buona approssimazione di* $(1-x)$ *per* $x < 0{,}3$

$$P_2(2^n, k) \cong 1-\exp[-2^{-n}(1+2+\ldots+(k-1))]$$

$$= 1 - \exp[-2^{-n}(k(k-1)/2)] \text{ e per k grande}$$

$$\cong 1 - \exp[-2^{-n}(k^2/2)]$$

IPOTESI: $P_2 = ½$

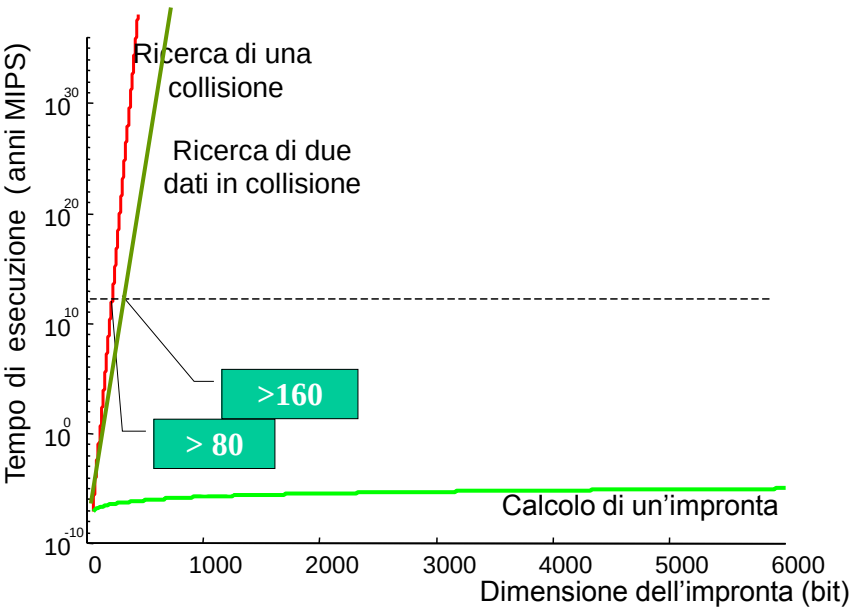
$$1 - ½ = \exp[-2^{-n}(k^2/2)]$$

$$\ln 2 = 2^{-n} \times (k^2/2)$$

$$k = \lceil 2 \times (\ln 2) \rceil^{1/2} \times 2^{n/2} = 1{,}18 \times 2^{n/2}$$

Paradosso del compleanno: $k = (2.\ln(2))^{1/2}.(365)^{1/2} = 22{,}54$.

Robustezza forte alle collisioni



Birthday attack

Nello schema di firma digitale, l'intruso (anche chi firma o chi verifica) non deve poter individuare una coppia m, m' in collisione (R20)

L'attaccante che vuole due messaggi con la stessa impronta

1. genera $2^{n/2}$ piccole varianti del primo messaggio
2. calcola e memorizza gli hash
3. Modifica lievemente il secondo messaggio, calcola l'hash e controlla se è in memoria; in caso contrario ripete. Dopo $2^{n/2}$ iterazioni puo' aspettarsi di trovare una coincidenza

Problema: data una variabile casuale con distribuzione uniforme tra 1 e n e due insiemi di k istanze della variabile (k<=n) qual è la probabilità che vi sia un valore presente in entrambi gli insiemi?

Problema: si applica H a un insieme di istanze K per produrre l'insieme X, e nuovamente ad altri k casuali per produrre l'insieme Y. Quale deve essere il valore di k tale che vi sia almeno una corrispondenza nei due insiemi? K= 2^n

Birthday attack

Nello schema di firma digitale, l'intruso (anche chi firma o chi verifica) non deve poter individuare una coppia m, m' in collisione (R20)

L'attaccante che vuole due messaggi con la stessa impronta

1. genera $2^{n/2}$ piccole varianti del primo messaggio (valido)
2. calcola e memorizza gli hash
3. Modifica lievemente il secondo messaggio (fraudolento), calcola l'hash e controlla se è in memoria; in caso contrario ripete. Dopo $2^{n/2}$ iterazioni puo' aspettarsi di trovare una coincidenza

O(exp(n/2))

spazi
punteggiatura
sinonimi

Dear Anthony,

{This letter is / I am writing} to introduce {you to / to you} {Mr. / --} Alfred {P. / --}

Barton, the {new / newly appointed} {chief / senior} jewellery buyer for {our / the}

Northern {European / Europe} {area / division}. He {will take / has taken} over {the / --}

responsibility for {all / the whole of} our interests in {watches and jewellery / jewellery and watches}

in the {area / region}. Please {afford / give} him {every / all the} help he {may need / needs}

to {seek out / find} the most {modern / up to date} lines for the {top / high} end of the

market. He is {empowered / authorized} to receive on our behalf {samples / specimens} of the

{latest / newest} {watch and jewellery / jewellery and watch} products, {up / subject} to a {limit / maximum}

of ten thousand dollars. He will {carry / hold} a signed copy of this {letter / document}

as proof of identity. An order with his signature, which is {appended / attached}

{authorizes / allows} you to charge the cost to this company at the {above / head office}

address. We {fully / --} expect that our {level / volume} of orders will increase in

the {following / next} year and {trust / hope} that the new appointment will {be / prove}

{advantageous / an advantage} to both our companies.

Obiettivi

1. Se le entità in gioco (A e B) sono fidate B deve poter completare il protocollo di identificazione certo dell’identità di A
2. (*transferability*) B non può riutilizzare lo scambio di identificazione con A per impersonare illegittimamente A presso un’altra entità
3. (*impersonation*) Deve essere irrilevante la probabilità che un’entità C che esegue il protocollo spacciandosi per A possa indurre B a completare con successo il protocollo accettando l’identità di C come se fosse quella di A
4. Tutti gli obiettivi precedenti devono rimanere validi se: un numero elevato di autenticazioni tra A e B sono state osservate; l’avversario C è stato precedentemente coinvolto in protocolli di identificazione con A e/o B anche in presenza di simultanee sessioni di identificazioni

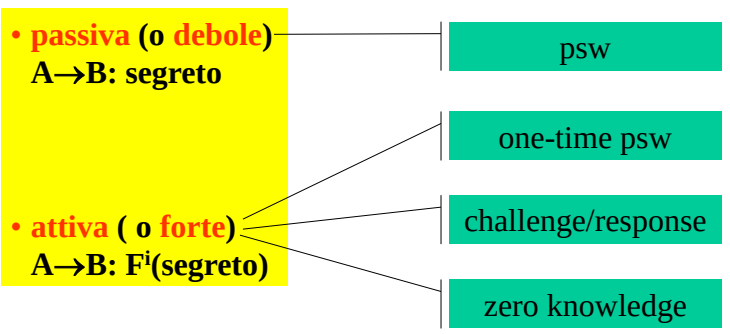
Proprietà

1. *Identificazione unilaterale o reciproca*
2. *Efficienza computazionale*
3. *Overhead di comunicazione*

In aggiunta:

4. *presenza real-time di una terza parte* (ad esempio che distribuisce chiavi simmetriche da utilizzare nella costruzione di prove di identificazione)
5. *Natura della terza parte* (terza parte che fa il bnding tra una chaive e un'identità, o terza parte che conosce una chiave di identificazione)
6. *Memorizzazione dei segreti*

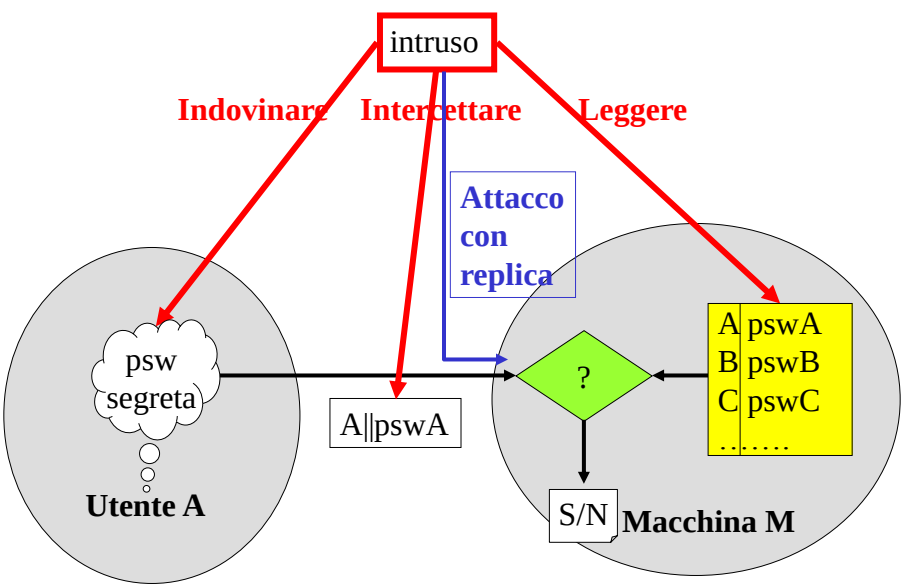
Dimostrazione di conoscenza



identificazione	unilaterale	reciproca
passiva	SI	NO
attiva	SI	SI

Identificazione passiva

La password



Difesa della password

1 - Scelta

lunga stringa casuale
utente, sistema, passphrase

R22: almeno 8 simboli casuali
L.196/03

2 - Memorizzazione

imparare
a memoria

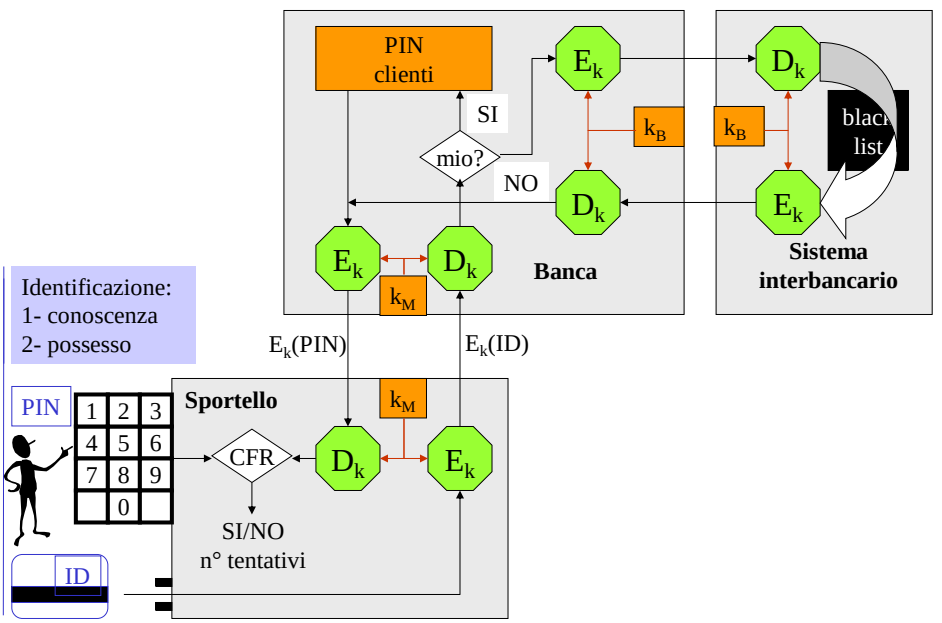
File di password cifrate

3-Comunicazione

A prova d'intercettazione
"eco", sportello, inaccessibilità fisica

N.B. la cifratura è inutile!

Bancomat: identificazione del cliente



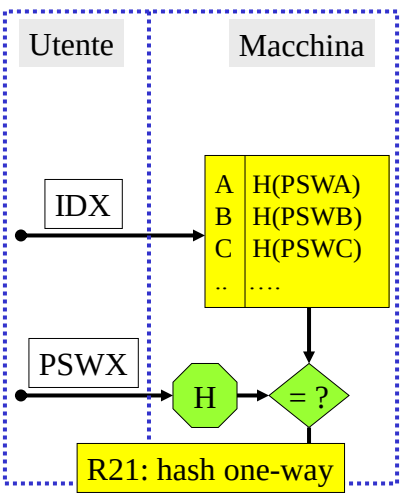
Difesa del file delle password

R14bis: "*L'accesso in scrittura al file delle psw deve essere consentito solo all'amministratore del servizio*"

R15bis: "*L'accesso in lettura al file delle psw deve restituire all'intruso dati non utilizzabili per farsi identificare come utente legittimo*"

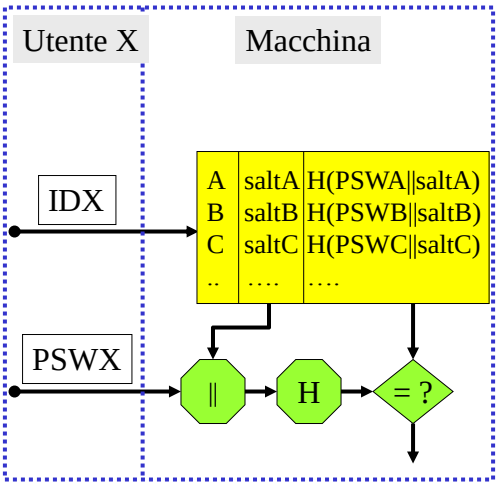
Hash della password: forma di cifratura per cui non esiste decifrazione!

hash delle password

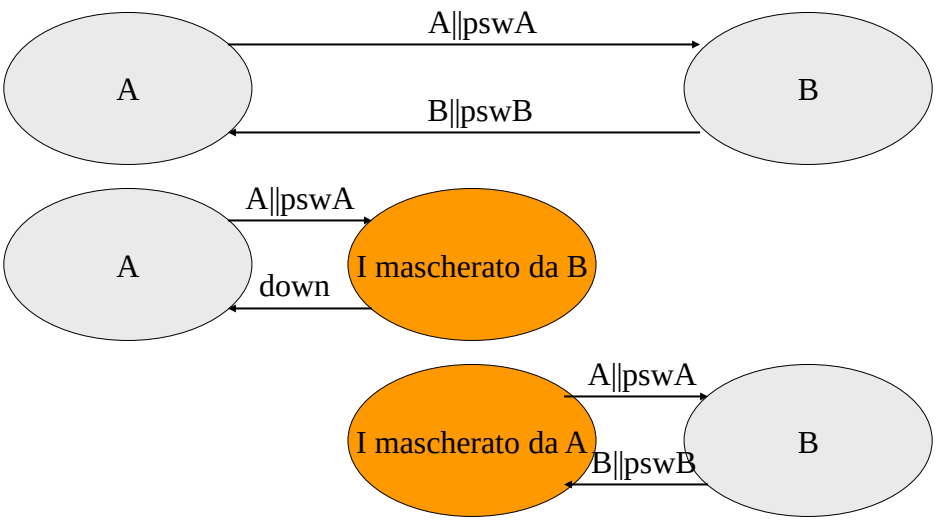


Attacco con dizionario

hash delle password e dei salt



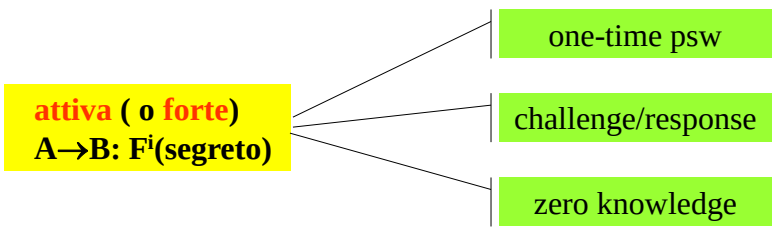
Identificazione unilaterale e reciproca



Solo l'identificazione attiva può essere anche mutua

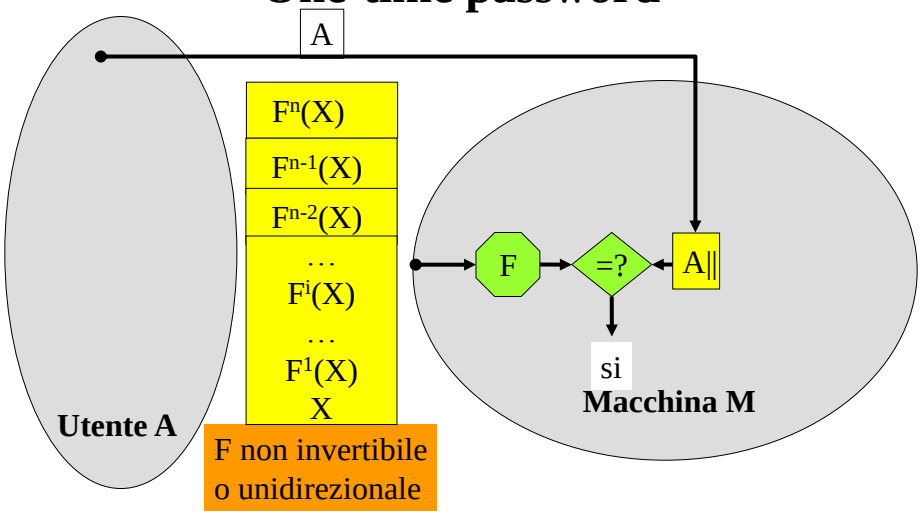
Identificazione attiva

La prova di conoscenza sempre diversa

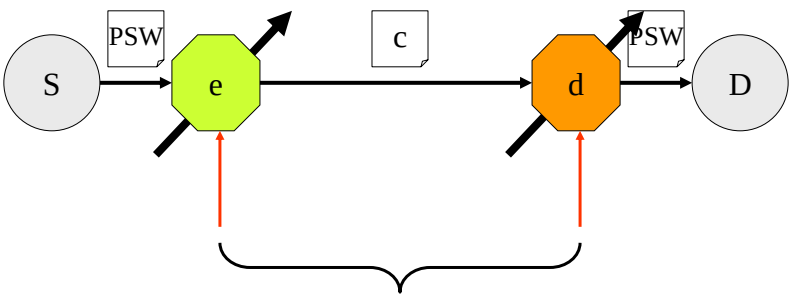


R23: "*Il calcolo della prova d'identità da fornire* ***di volta in volta*** *deve essere facile per chi conosce un'informazione segreta, difficile per chi dispone solo delle prove inviate in precedenza*"

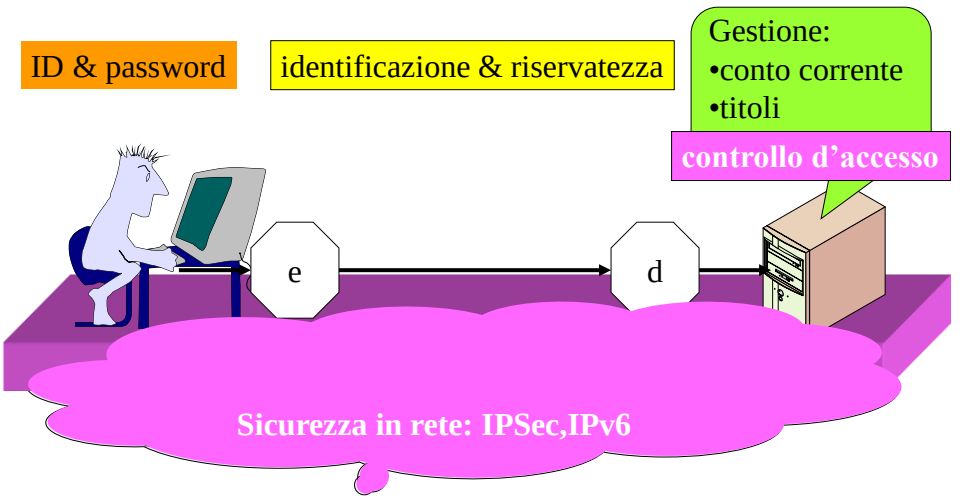
One-time password



Cifratura one-time

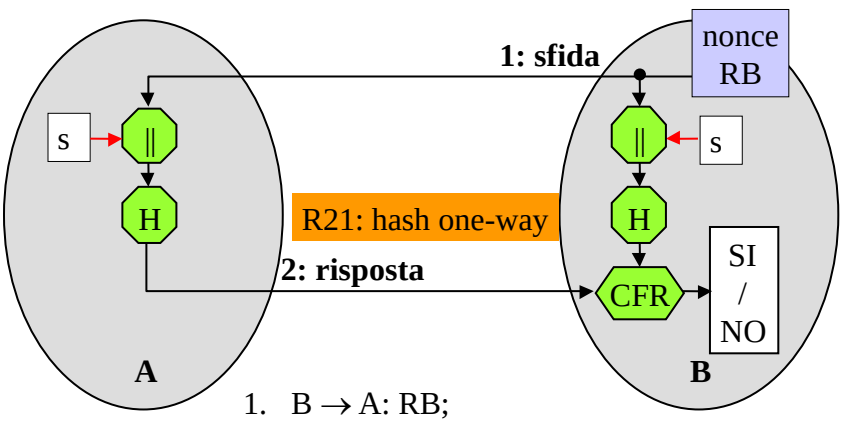


Home banking (1)



HTTPS: Cilma & Multitel

Sfida/Risposta (Hash)

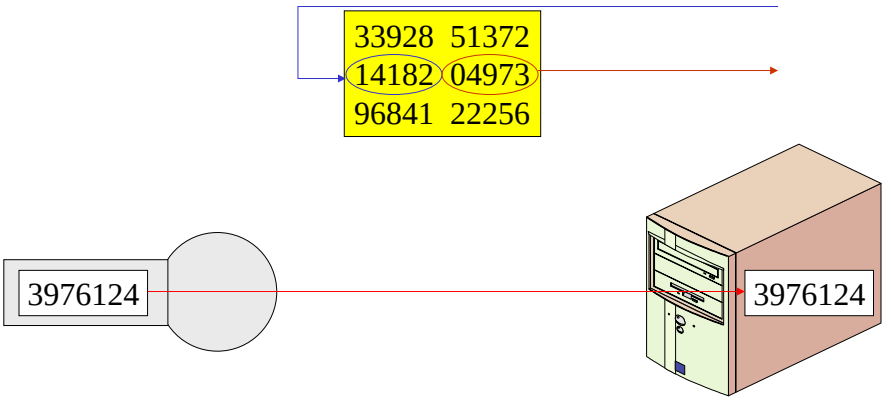


1. B → A: RB;
2. A → B: cA = H(RB || s).

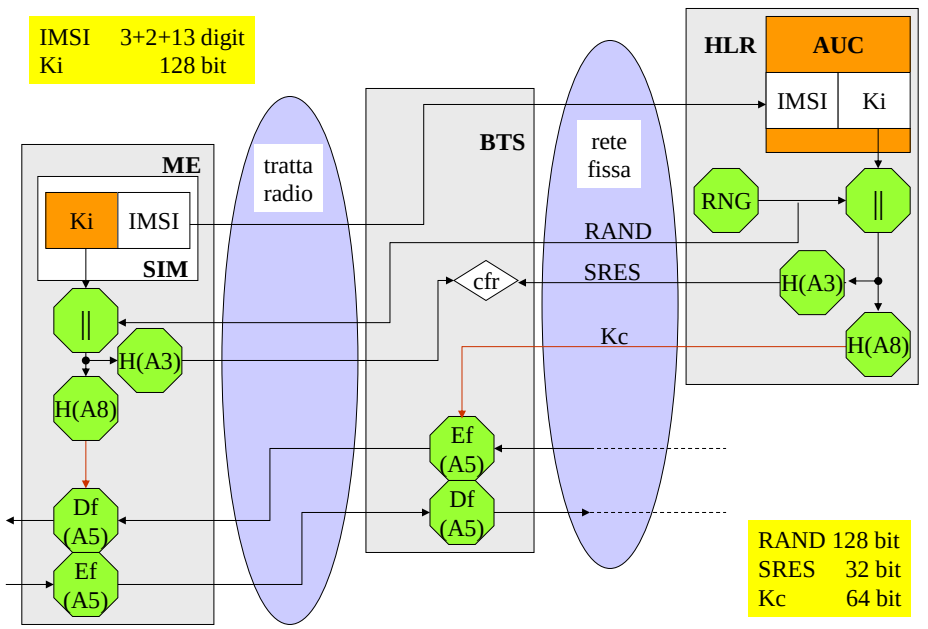
Home banking (2)

ID & password & token

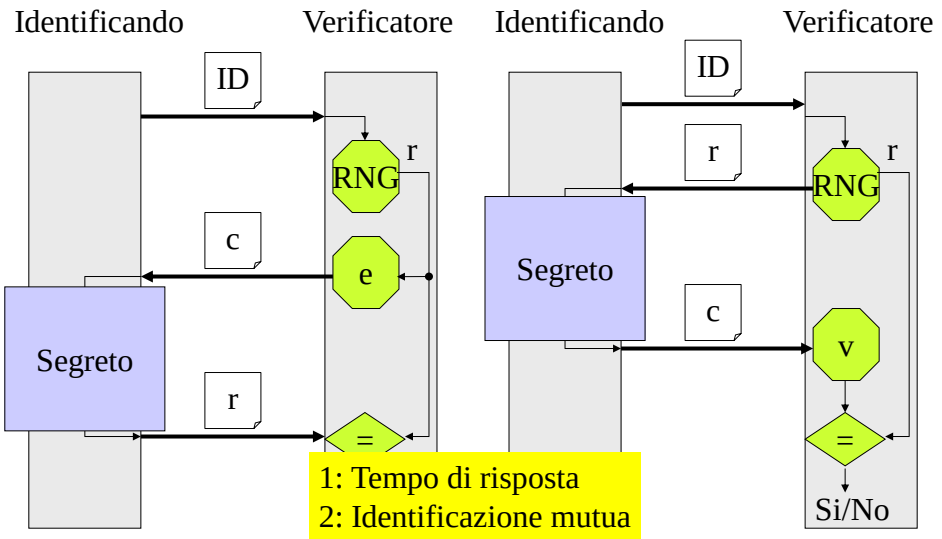
sfida/risposta: Unicredit, Sanpaolo, ..



GSM: identificazione e riservatezza



Il protocollo sfida/risposta (Cifrario, Firma digitale)



Identificazione mutua

1. B → A: RB;
2. A → B: cA = RA || H(RB|| s);
3. B → A: cB = H(RA|| s).

Robusto????

Attacchi su Protocolli di Identificazione

- ***impersonation**:* a deception whereby one entity purports to be another.
- ***replay attack**:* an impersonation or other deception involving use of information from a single previous protocol execution, on the same or a different verifier.
- ***interleaving attack**:* an impersonation or other deception involving selective combination of information from one or more previous or simultaneously ongoing protocol executions (*parallel sessions*), including possible origination of one or more protocol executions by an adversary itself.
- ***reflection attack:*** an interleaving attack involving sending information from an ongoing protocol execution back to the originator of such information.
- ***forced delay**:* a forced delay occurs when an adversary intercepts a message (typically containing a sequence number), and relays it at some later point in time. Note the delayed message is not a replay.
- ***chosen-text attack**:* an attack on a challenge-response protocol wherein an adversary strategically chooses challenges in an attempt to extract information about the claimant's long-term key.

Il problema del Gran Maestro di Scacchi

A vuole spacciarsi
per un grande esperto di scacchi pur non conoscendo il gioco.
A sfida due Gran Maestri B e C, che sistema, senza che se ne accorgano,
in due camere contigue: a B assegna i "bianchi", a C i "neri".
Preso nota della prima mossa di B, A corre nell'altra stanza e la riproduce sulla scacchiera di C. Successivamente prende nota della contromossa di C e corre a riprodurla sulla scacchiera di B.
Continuando così ottiene o due patte o un'incredibile vittoria.

C tenta di impersonare B, è sfidato (a dimostrare di essere B) da A, ed è in grado di inviare in tempo reale senza troppo ritardo e inganno pretendendo di essere A la sfida al vero B, riceve una risposta giusta da B a la passa indietro ad A

ATTACCO di INTERLEAVING

Attacco di Reflection

L’attacco richiede di attivare due copie del protocollo contemporaneamente tra A e C.

L’attacco di reflection prevede di rimbalzare indietro informazioni scambiate in sessioni diverse

Attacco di Reflection

L’attacco richiede di attivare due copie del protocollo contemporaneamente. A inizia il protocollo inviando la sfida RA a C, C avvia un’altra copia del protocollo ma nell’opposta direzione inviando la sfida RA ad A pretendendo di essere B

Identificazione mutua

Resistente all'attacco di
reflection

1. B → A: RB;
2. A → B: cA = RA || H(**RA** || RB || **B** || s);
3. B → A: cB = H(RA || **RB** || **A** || s).

Eliminazione di simmetria di messaggi, linking
tra i vari messaggi tramite numeri random,
inserimento dell'identificatore del target

Marca temporale (time stamp)

Numero di sequenza

Contromisure

Numeri random, timestamp,
numeri di sequenza

Type of attack	Principles to avoid attack
replay	use of challenge-response techniques; use of nonces; embed target identity in response
interleaving	linking together all messages from a protocol run (e.g., using chained nonces)
reflection	embed identifier of target party in challenge responses; construct protocols with each message of different form (avoid message symmetries); use of uni-directional keys
chosen-text	use of zero-knowledge techniques; embed in each challenge response a self-chosen random number (*confounder*)
forced delay	combined use of random numbers with short response time-outs; timestamps plus appropriate additional techniques

***Disadvantages of random numbers*:**

1. cryptographically secure (i.e., unpredictable) random numbers.
2. when random numbers are used in challenge-response mechanisms in place of timestamps, typically the protocol involves one additional message, and the challenger must temporarily maintain state information, but only until the response is verified.

Disadvantages of sequence numbers:

1. each claimant must record and maintain long-term pairwise state information for each possible verifier, sufficient to determine previously used and/or still valid sequence numbers.
2. special procedures (e.g., for resetting sequence numbers) may be necessary following circumstances disrupting normal sequencing (e.g., system failures). As a consequence of the overhead and synchronization necessary, sequence numbers are most appropriate for smaller, closed groups.

Disadvantages of timestamps:

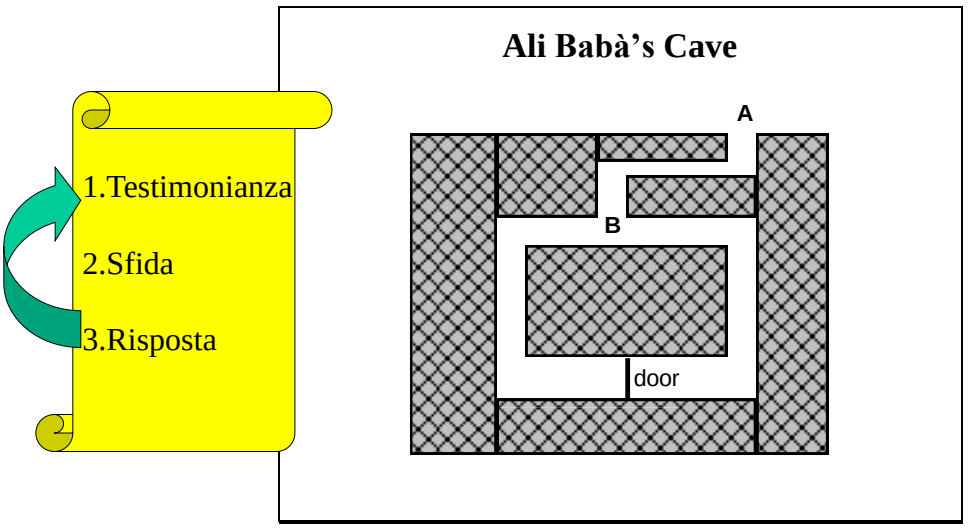
1. timestamp-based protocols require that timeclocks be both synchronized and secured.
2. the preclusion of adversarial modification of local timeclocks is difficult to guarantee in many distributed environments
3. while technical solutions exist for synchronizing distributed clocks, if synchronization is accomplished via network protocols, such protocols themselves must be secure, which typically requires authentication; this leads to a circular security argument if such authentication is itself timestamp-based.

Protocollo di identificazione = processo real-time, i.e., fornisce la prova che l'entità che si deve identificare è in quell'istante operativa; si fornisce certezza solo nel momento in cui il protocollo si completa

Se occorre mantenere autenticità nel tempo (ad esempio nel corso di un'intera sessione) occorre affiancare al protocollo di identificazione altre misure, ad esempio di autenticazione del messaggio

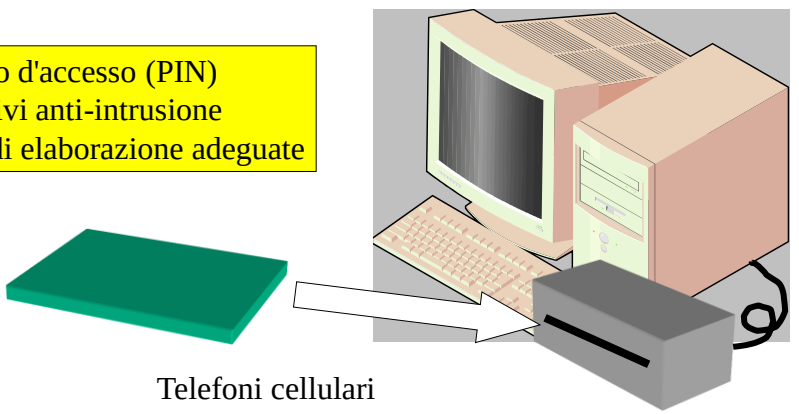
Zero-knowledge protocols

Principio: dare solo una testimonianza di saper risolvere facilmente un problema da tutti ritenuto difficile



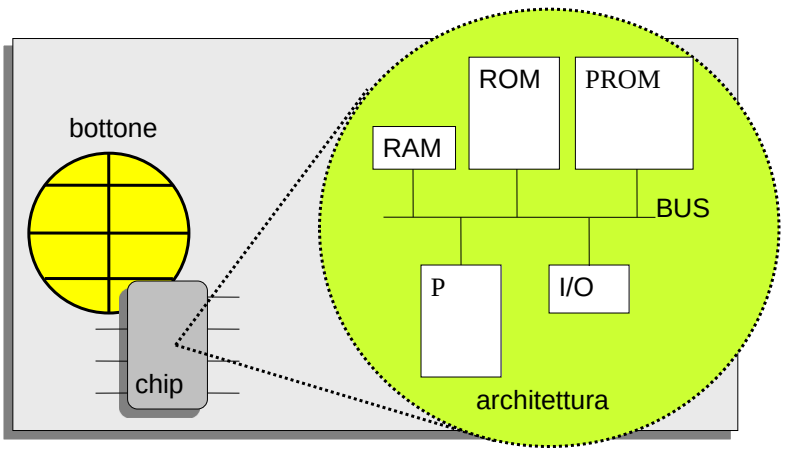
Il calcolatore portatile e personale

controllo d'accesso (PIN)
dispositivi anti-intrusione
risorse di elaborazione adeguate



Telefoni cellulari
Home banking
Carta d'identità
Passaporto europeo
….
Registrazione esami

Smart card a contatto

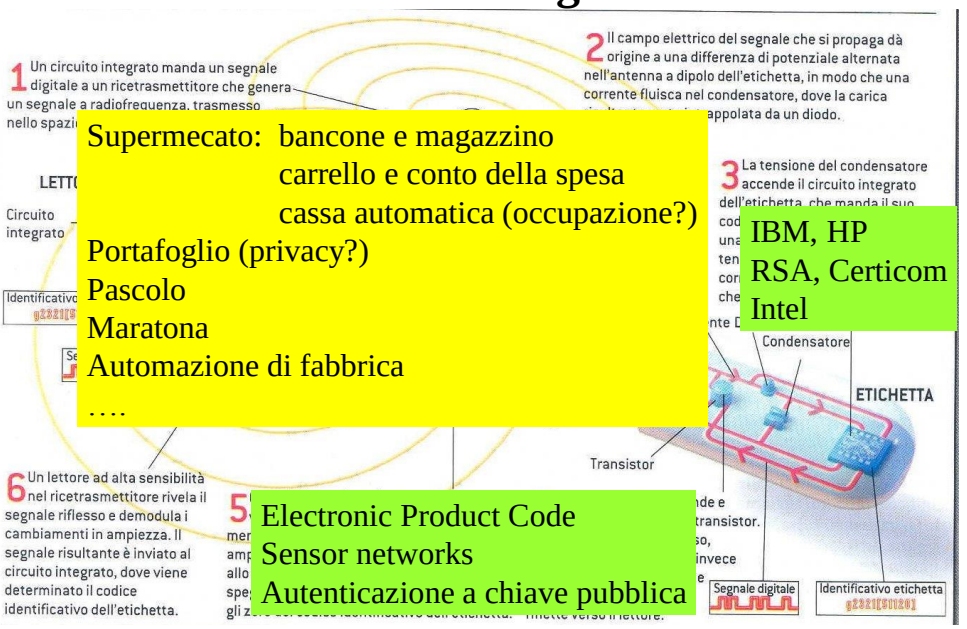


Tipi e Standard

- a contatto
- senza contatto
- a prossimità

- ISO 7816
- Microsoft Crypto API
- PKCS#11
- PKCS#15
- PC/SC Workgroup

Smart tag



Supermecato: bancone e magazzino
carrello e conto della spesa
cassa automatica (occupazione?)
Portafoglio (privacy?)
Pascolo
Maratona
Automazione di fabbrica
….

IBM, HP
RSA, Certicom
Intel

Electronic Product Code
Sensor networks
Autenticazione a chiave pubblica