# Crittografia sarai te...

lucha, tas

**Sun-Tzu, *l'Arte della Guerra***

Niente dovrebbe essere considerato con più favore delle informazioni; niente andrebbe ricompensato più generosamente; niente dovrebbe essere così discreto come il lavoro inteso a procurarle.

# Scrivere di nascosto

- steganografia $\rightarrow$ “non esiste nessun messaggio”
- crittografia $\rightarrow$ “questo messaggio è incomprensibile!”

**Attenzione!**

La crittografia non nasconde il messaggio ma il suo significato!

# Scrivere di nascosto

- steganografia $\rightarrow$ “non esiste nessun messaggio”
- crittografia $\rightarrow$ “questo messaggio è incomprensibile!”

**Attenzione!**

La crittografia non nasconde il messaggio ma il suo significato!

# Scrivere di nascosto

- steganografia $\rightarrow$ “non esiste nessun messaggio”
- crittografia $\rightarrow$ “questo messaggio è incomprensibile!”

**Attenzione!**

La crittografia non nasconde il messaggio ma il suo significato!

# Scrivere di nascosto

- steganografia $\rightarrow$ “non esiste nessun messaggio”
- crittografia $\rightarrow$ “questo messaggio è incomprensibile!”

**Attenzione!**

La crittografia non nasconde il messaggio ma il suo significato!

# Trasposizioni

- possibile è ordine frase senza alterare della il significato l'
- trasporre secondo una regola permette a chi riceve di ricostruire il messaggio originale (ma l'attaccante?)

| |
|---|
| ecco ora lo sa anche la stampa che ci dimentichiamo le cose a casa |
| e c o a o a n h l s a p c e i i e t c i m l c s a a a |
| c o r l s a c e a t m a h c d m n i h a o e o e c s |
| ecoaoanhlsapceiietcimlcsaaacorlsaceatmahcdmnihaoeoecs |

# Trasposizioni

- possibile è ordine frase senza alterare della il significato l'
- trasporre secondo una regola permette a chi riceve di ricostruire il messaggio originale (ma l'attaccante?)

ecco ora lo sa anche la stampa che ci dimentichiamo le cose a casa

e c o a o a n h l s a p c e i i e t c i m l c s a a a
c o r l s a c e a t m a h c d m n i h a o e o e c s

ecoaoanhlsapceiietcimlcsaaacorlsaceatmahcdmnihaoeoecs

# Trasposizioni

- possibile è ordine frase senza alterare della il significato l'
- trasporre secondo una regola permette a chi riceve di ricostruire il messaggio originale (ma l'attaccante?)

| |
|---|
| ecco ora lo sa anche la stampa che ci dimentichiamo le cose a casa |
| e c o a o a n h l s a p c e i i e t c i m l c s a a a c o r l s a c e a t m a h c d m n i h a o e o e c s |
| ecoaoanhlsapceiietcimlcsaaacorlsaceatmahcdmnihaoeoecs |

# Trasposizioni

- possibile è ordine frase senza alterare della il significato l'
- trasporre secondo una regola permette a chi riceve di ricostruire il messaggio originale (ma l'attaccante?)

| ecco ora lo sa anche la stampa che ci dimentichiamo le cose a casa |
|---|
| e c o a o a n h l s a p c e i i e t c i m l c s a a a<br>c o r l s a c e a t m a h c d m n i h a o e o e c s |
| ecoaoanhlsapceiietcimlcsaaacorlsaceatmahcdmnihaoeoecs |

# Sostituzioni

*fmivdvmr gm fhxdvh* ovvero...

**cifrario di Cesare**

Sostituiamo ogni lettera con la lettera che si trova *3 posizioni* dopo nell'alfabeto.

```
abcdefghiklmnopqrstux
DEFGHIKLMNOPQRSTVXABC
```

- possiamo spostarci anche di 4, 5, 6, ... posizioni.
- 26 possibili scelte, di cui una poco utile.
- utilizzata dal II secolo d.C. al 2000 circa da diverse Potenze.

# Sostituzioni

*fmivdvmr gm fhxdvh* ovvero...

## cifrario di Cesare

Sostituiamo ogni lettera con la lettera che si trova *3 posizioni* dopo nell'alfabeto.

```
abcdefghiklmnopqrstux
DEFGHIKLMNOPQRSTVXABC
```

- possiamo spostarci anche di 4, 5, 6, ... posizioni.
- 26 possibili scelte - di cui una poco utile
- utilizzata dal II secolo d.C. al 2006 ⇒ pizzini di Provenzano

# Sostituzioni

*fmivdvmr gm fhxdvh* ovvero...

## cifrario di Cesare

Sostituiamo ogni lettera con la lettera che si trova *3 posizioni* dopo nell'alfabeto.

```
abcdefghiklmnopqrstux
DEFGHIKLMNOPQRSTVXABC
```

- possiamo spostarci anche di 4, 5, 6, ... posizioni.
- 26 possibili scelte - di cui una poco utile
- utilizzata dal II secolo d.C. al 2006 $\rightarrow$ pizzini di Provenzano

# Sostituzioni

*fmivdvmr gm fhxdvh* ovvero...

## cifrario di Cesare

Sostituiamo ogni lettera con la lettera che si trova *3 posizioni* dopo nell'alfabeto.

```
abcdefghiklmnopqrstux
DEFGHIKLMNOPQRSTVXABC
```

- possiamo spostarci anche di 4, 5, 6, ... posizioni.
- 26 possibili scelte - di cui una poco utile
- utilizzata dal II secolo d.C. al 2006 $\rightarrow$ pizzini di Provenzano

# Sostituzioni

*fmivdvmr gm fhxdvh* ovvero...

## cifrario di Cesare

Sostituiamo ogni lettera con la lettera che si trova *3 posizioni* dopo nell'alfabeto.

```
abcdefghiklmnopqrstux
DEFGHIKLMNOPQRSTVXABC
```

- possiamo spostarci anche di 4, 5, 6, ... posizioni.
- 26 possibili scelte - di cui una poco utile
- utilizzata dal II secolo d.C. al 2006 $\rightarrow$ pizzini di Provenzano

# Migliorie e attacchi

- attacco: provare tutte le 26 chiavi possibili
- difesa: permutazione invece degli spostamenti $\rightarrow$ 50 miliardi di chiavi
- attacco: Abū Yūsuf ibn Ishāq al-Kindī, *Sulla decifrazione dei messaggi crittati*, IX sec. d.C.
- analisi delle frequenze

| Lettera | frequenza |
|---|---|
| a | 11.74% |
| e | 11.79% |
| f | 0.95% |
| n | 6.88% |
| ... | ... |

- presenza di doppie, frequenza delle sillabe, etc.

# Migliorie e attacchi

- attacco: provare tutte le 26 chiavi possibili
- difesa: permutazione invece degli spostamenti $\rightarrow$ 50 miliardi di chiavi
- attacco: Abū Yūsuf ibn Ishāq al-Kindī, *Sulla decifrazione dei messaggi crittati*, IX sec. d.C.
- analisi delle frequenze

| Lettera | frequenza |
|---|---|
| a | 11.74% |
| e | 11.79% |
| f | 0.95% |
| n | 6.88% |
| ... | ... |

- presenza di doppie, frequenza delle sillabe, etc.

# Migliorie e attacchi

- attacco: provare tutte le 26 chiavi possibili
- difesa: permutazione invece degli spostamenti $\rightarrow$ 50 miliardi di chiavi
- attacco: Abū Yūsuf ibn Ishāq al-Kindī, *Sulla decifrazione dei messaggi crittati*, IX sec. d.C.
- analisi delle frequenze

| Lettera | frequenza |
|---|---|
| a | 11.74% |
| e | 11.79% |
| f | 0.95% |
| n | 6.88% |
| ... | ... |

- presenza di doppie, frequenza delle sillabe, etc.

# Migliorie e attacchi

- attacco: provare tutte le 26 chiavi possibili
- difesa: permutazione invece degli spostamenti $\rightarrow$ 50 miliardi di chiavi
- attacco: Abū Yūsuf ibn Ishāq al-Kindī, *Sulla decifrazione dei messaggi crittati*, IX sec. d.C.
- analisi delle frequenze

| Lettera | frequenza |
|---|---|
| a | 11.74% |
| e | 11.79% |
| f | 0.95% |
| n | 6.88% |
| ... | ... |

- presenza di doppie, frequenza delle sillabe, etc.

# Migliorie e attacchi

- attacco: provare tutte le 26 chiavi possibili
- difesa: permutazione invece degli spostamenti $\rightarrow$ 50 miliardi di chiavi
- attacco: Abū Yūsuf ibn Ishāq al-Kindī, *Sulla decifrazione dei messaggi crittati*, IX sec. d.C.
- analisi delle frequenze

| Lettera | frequenza |
|---|---|
| a | 11.74% |
| e | 11.79% |
| f | 0.95% |
| n | 6.88% |
| ... | ... |

- presenza di doppie, frequenza delle sillabe, etc.

# Le chiffre indéchiffrable

- Leon Battista Alberti: “perché usare *un solo* alfabeto cifrante?”
- nasce la cifratura *polialfabetica*

## Cifrario di Vigenére (XVI sec.)

- si associa ad ogni lettera un alfabeto cifrante
- si concorda una chiave segreta
- si utilizza un alfabeto diverso per ogni lettera, corrispondente ad una diversa lettera della chiave
- quando la chiave termina, si riutilizza dall'inizio

# Le chiffre indéchiffrable

- Leon Battista Alberti: “perché usare *un solo* alfabeto cifrante?”
- nasce la cifratura *polialfabetica*

## Cifrario di Vigenére (XVI sec.)

- si associa ad ogni lettera un alfabeto cifrante
- si concorda una chiave segreta
- si utilizza un alfabeto diverso per ogni lettera, corrispondente ad una diversa lettera della chiave
- quando la chiave termina, si riutilizza dall'inizio

# Le chiffre indéchiffrable

- Leon Battista Alberti: “perché usare *un solo* alfabeto cifrante?”
- nasce la cifratura *polialfabetica*

## Cifrario di Vigenére (XVI sec.)

- si associa ad ogni lettera un alfabeto cifrante
- si concorda una chiave segreta
- si utilizza un alfabeto diverso per ogni lettera, corrispondente ad una diversa lettera della chiave
- quando la chiave termina, si riutilizza dall’inizio

# Le chiffre indéchiffrable

- Leon Battista Alberti: “perché usare *un solo* alfabeto cifrante?”
- nasce la cifratura *polialfabetica*

## Cifrario di Vigenére (XVI sec.)

- si associa ad ogni lettera un alfabeto cifrante
- si concorda una chiave segreta
- si utilizza un alfabeto diverso per ogni lettera, corrispondente ad una diversa lettera della chiave
- quando la chiave termina, si riutilizza dall’inizio

# Le chiffre indéchiffrable

- Leon Battista Alberti: “perché usare *un solo* alfabeto cifrante?”
- nasce la cifratura *polialfabetica*

## Cifrario di Vigenére (XVI sec.)

- si associa ad ogni lettera un alfabeto cifrante
- si concorda una chiave segreta
- si utilizza un alfabeto diverso per ogni lettera, corrispondente ad una diversa lettera della chiave
- quando la chiave termina, si riutilizza dall’inizio

# Le chiffre indéchiffrable

- Leon Battista Alberti: “perché usare *un solo* alfabeto cifrante?”
- nasce la cifratura *polialfabetica*

## Cifrario di Vigenére (XVI sec.)

- si associa ad ogni lettera un alfabeto cifrante
- si concorda una chiave segreta
- si utilizza un alfabeto diverso per ogni lettera, corrispondente ad una diversa lettera della chiave
- quando la chiave termina, si riutilizza dall’inizio

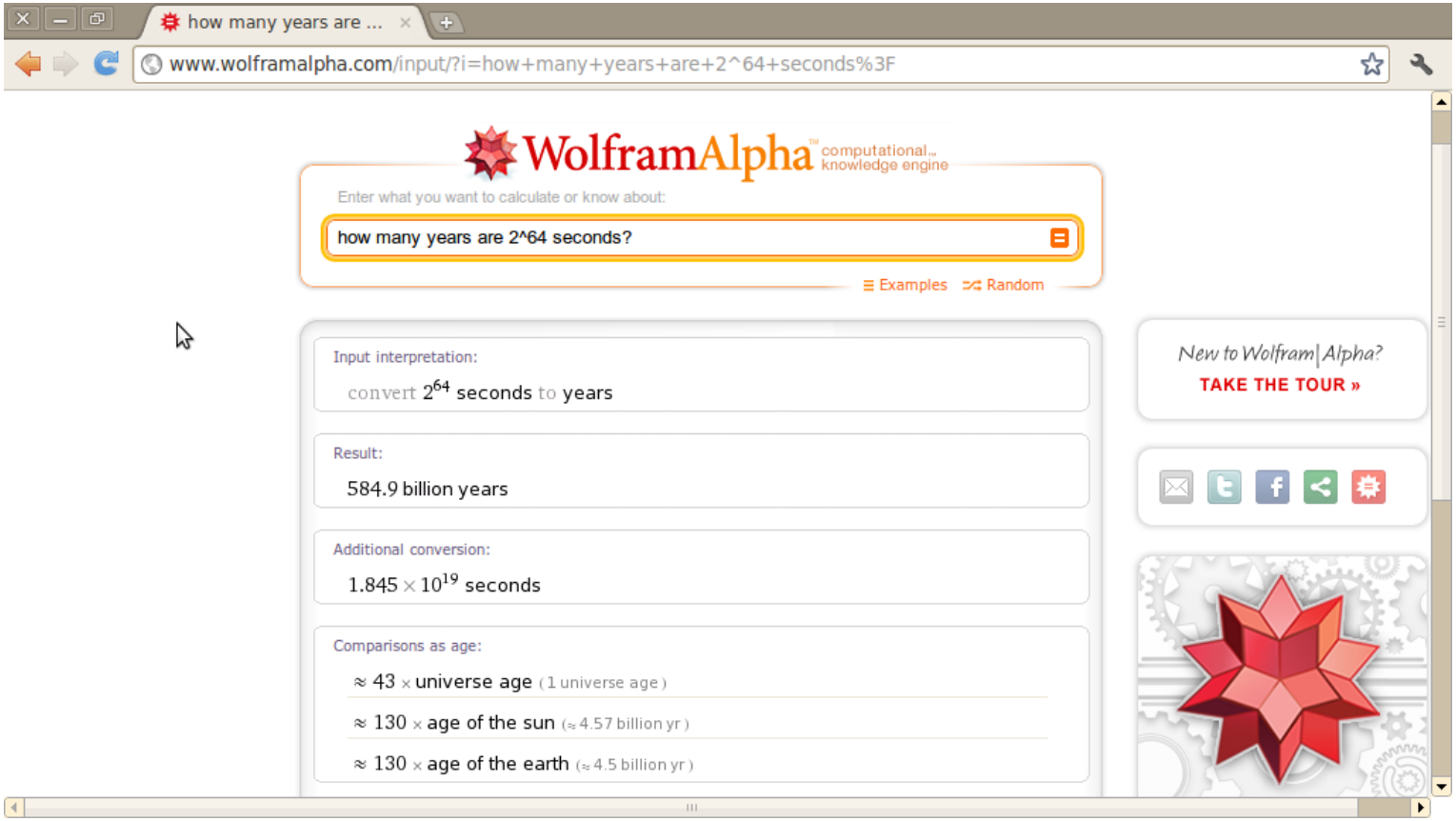
# Esempio di cifratura di Vigenére

**chiave segreta**

HACK

| | |
|---|---|
| parola chiave: | `HACKHACK HA CKH ACKHA` |
| testo chiaro: | `qualcuno ha una tenda?` |
| testo cifrato: | `xucvjupy oa wxh tgxka?` |

- scarso successo a causa della sua scarsa agilità


how many years are ...
www.wolframalpha.com/input/?i=how+many+years+are+2^64+seconds%3F
WolframAlpha computational knowledge engine
Enter what you want to calculate or know about:
how many years are 2^64 seconds?
Examples
Random
Input interpretation:
convert 2^64 seconds to years
Result:
584.9 billion years
Additional conversion:
1.845 × 10^19 seconds
Comparisons as age:
≈ 43 × universe age (1 universe age)
≈ 130 × age of the sun (≈ 4.57 billion yr)
≈ 130 × age of the earth (≈ 4.5 billion yr)
New to Wolfram|Alpha?
TAKE THE TOUR »

# Arriva il vapore, il capitale e a ragion di Stato...

- Charles Babbage riesce a rompere il cifrario di Vigenére se la chiave non e' troppo lunga
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni

**Soluzione**

Utilizzare una chiave *lunga quanto il messaggio* e che sia *casuale*, ovvero la cosiddetta cifratura *one-time pad*

# Arriva il vapore, il capitale e a ragion di Stato...

- Charles Babbage riesce a rompere il cifrario di Vigenére se la chiave non e' troppo lunga
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni

**Soluzione**

Utilizzare una chiave *lunga quanto il messaggio* e che sia *casuale*, ovvero la cosiddetta cifratura *one-time pad*

# Arriva il vapore, il capitale e a ragion di Stato...

- Charles Babbage riesce a rompere il cifrario di Vigenére se la chiave non e' troppo lunga
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni

**Soluzione**

Utilizzare una chiave *lunga quanto il messaggio* e che sia *casuale*, ovvero la cosiddetta cifratura *one-time pad*

# Arriva il vapore, il capitale e a ragion di Stato...

- Charles Babbage riesce a rompere il cifrario di Vigenére se la chiave non e' troppo lunga
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni

**Soluzione**

Utilizzare una chiave *lunga quanto il messaggio* e che sia *casuale*, ovvero la cosiddetta cifratura *one-time pad*

# Arriva il vapore, il capitale e a ragion di Stato...

- Charles Babbage riesce a rompere il cifrario di Vigenére se la chiave non e' troppo lunga
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni

**Soluzione**

Utilizzare una chiave *lunga quanto il messaggio* e che sia *casuale*, ovvero la cosiddetta cifratura *one-time pad*

# Arriva il vapore, il capitale e a ragion di Stato...

- Charles Babbage riesce a rompere il cifrario di Vigenére se la chiave non e' troppo lunga
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni
- la colpa è delle ripetizioni

**Soluzione**

Utilizzare una chiave *lunga quanto il messaggio* e che sia *casuale*, ovvero la cosiddetta cifratura *one-time pad*

# One-time pad

## l'argoritmo perfetto

Un lancio casuale + una frase fissa = un lancio casuale.
L'attacante non distingue il messaggio cifrato da una possibile chiave.

- e' *molto* importante non riusare mai la stessa chiave più volte!

## Problema

Volevamo trasmettere un messaggio, e ci siamo ridotti al problema di trasmettere una chiave *della stessa lunghezza*!

# One-time pad

## l'argoritmo perfetto

Un lancio casuale + una frase fissa = un lancio casuale.
L'attacante non distingue il messaggio cifrato da una possibile chiave.

- e' *molto* importante non riusare mai la stessa chiave più volte!

## Problema

Volevamo trasmettere un messaggio, e ci siamo ridotti al problema di trasmettere una chiave *della stessa lunghezza*!

# One-time pad

## l'argoritmo perfetto

Un lancio casuale + una frase fissa = un lancio casuale.
L'attacante non distingue il messaggio cifrato da una possibile chiave.

- e' *molto* importante non riusare mai la stessa chiave più volte!

## Problema

Volevamo trasmettere un messaggio, e ci siamo ridotti al problema di trasmettere una chiave *della stessa lunghezza*!

# Dell'arte di scambiarsi le chiavi

Diffie-Hellman 1976 propongono uno scambio a tre.

1. Alice prende una chiave e la mette in una scatola. Chiude la scatola con un lucchetto.
2. Bob riceva la scatola, non può aprirla e quindi ci aggiunge un lucchetto.
3. Alice riceve la scatola, neanche lei può più aprirla: per cui toglie il suo lucchetto.
4. Bob riceve la scatola: ora può aprirla, togliendo il suo lucchetto, e dentro la scatola recuperare la chiave che aveva scelto Alice.

Abbiamo risolto il problema di scambiarci le chiavi, ma con una comunicazione un po' laboriosa!

# Dell'arte di scambiarsi le chiavi

Diffie-Hellman 1976 propongono uno scambio a tre.

1. Alice prende una chiave e la mette in una scatola. Chiude la scatola con un lucchetto.
2. Bob riceva la scatola, non può aprirla e quindi ci aggiunge un lucchetto.
3. Alice riceve la scatola, neanche lei può più aprirla: per cui toglie il suo lucchetto.
4. Bob riceve la scatola: ora può aprirla, togliendo il suo lucchetto, e dentro la scatola recuperare la chiave che aveva scelto Alice.

Abbiamo risolto il problema di scambiarci le chiavi, ma con una comunicazione un po' laboriosa!

# Dell'arte di scambiarsi le chiavi

Diffie-Hellman 1976 propongono uno scambio a tre.

1. Alice prende una chiave e la mette in una scatola. Chiude la scatola con un lucchetto.
2. Bob riceva la scatola, non può aprirla e quindi ci aggiunge un lucchetto.
3. Alice riceve la scatola, neanche lei può più aprirla: per cui toglie il suo lucchetto.
4. Bob riceve la scatola: ora può aprirla, togliendo il suo lucchetto, e dentro la scatola recuperare la chiave che aveva scelto Alice.

Abbiamo risolto il problema di scambiarci le chiavi, ma con una comunicazione un po' laboriosa!

# Dell'arte di scambiarsi le chiavi

Diffie-Hellman 1976 propongono uno scambio a tre.

1. Alice prende una chiave e la mette in una scatola. Chiude la scatola con un lucchetto.
2. Bob riceva la scatola, non può aprirla e quindi ci aggiunge un lucchetto.
3. Alice riceve la scatola, neanche lei può più aprirla: per cui toglie il suo lucchetto.
4. Bob riceve la scatola: ora può aprirla, togliendo il suo lucchetto, e dentro la scatola recuperare la chiave che aveva scelto Alice.

Abbiamo risolto il problema di scambiarci le chiavi, ma con una comunicazione un po' laboriosa!

# Dell'arte di scambiarsi le chiavi

Diffie-Hellman 1976 propongono uno scambio a tre.

1. Alice prende una chiave e la mette in una scatola. Chiude la scatola con un lucchetto.
2. Bob riceva la scatola, non può aprirla e quindi ci aggiunge un lucchetto.
3. Alice riceve la scatola, neanche lei può più aprirla: per cui toglie il suo lucchetto.
4. Bob riceve la scatola: ora può aprirla, togliendo il suo lucchetto, e dentro la scatola recuperare la chiave che aveva scelto Alice.

Abbiamo risolto il problema di scambiarci le chiavi, ma con una comunicazione un po' laboriosa!

# Dell'arte di scambiarsi le chiavi

Diffie-Hellman 1976 propongono uno scambio a tre.

1. Alice prende una chiave e la mette in una scatola. Chiude la scatola con un lucchetto.
2. Bob riceva la scatola, non può aprirla e quindi ci aggiunge un lucchetto.
3. Alice riceve la scatola, neanche lei può più aprirla: per cui toglie il suo lucchetto.
4. Bob riceve la scatola: ora può aprirla, togliendo il suo lucchetto, e dentro la scatola recuperare la chiave che aveva scelto Alice.

Abbiamo risolto il problema di scambiarci le chiavi, ma con una comunicazione un po' laboriosa!

# Crittografia a chiave pubblica

- Ora sappiamo come costruire un canale sicuro...
- ... se riusciamo a scambiarci le chiavi su un canale non sicuro!
- Ci viene in soccorso la *crittografia a chiave pubblica*
- L'utente non deve più comunicare la sua chiave
- Le chiavi diventano due: una *pubblica* ed una *privata*
- Si cifra con la chiave pubblica che *tutti* devono conoscere
- Si decifra con la chiave privata, che solo l'utente conosce

# Debolezze e difetti della chiave pubblica

- è lenta
- ci vogliono tanti conti
- chissà se si sono detti proprio questo...
- chosen chypertext

# RSA

- ideato da Rivest, Shaamir e Adleman nel 1978
- si basa sulla difficoltà di scomporre (fattorizzare) un numero molto grande in un prodotto di numeri primi

# funzionamento di RSA

1. si scelgono due numeri primi molto grandi $p$ e $q$.
2. si calcola $n = p \times q$.
3. si sceglie un numero $e < \Phi(n)$ e primo con esso.
4. si calcola $d = e^{-1} \mod \Phi(n)$.
5. $k^+ =< e, n >$, $k^- =< d >$.

# funzionamento di RSA

## messaggi

i messaggi sono numeri naturali più piccoli di $n$.

## cifratura

dato un messaggio $m$, il messaggio cifrato è $c = m^e \mod n$.

## decifrazione

dato un crittogramma $c$, si ottiene il messaggio originale $m = c^d \mod n$.

# Firma digitale

Cosa mi garantisce?

- come una firma vera!
- l'hai scritto tu!
- l'ho scritto io ed era proprio così!
- È vero l'hai scritto tu!
- possiamo garantire solo sul mittente.

# Firma digitale

Come si può fare?

- protocollo di firma Diffie-Hellman
- serve un cifrario asimettrico
- per firmare il mittente decifra il messaggio con la sua chiave privata ottenendo $f$
- per verificare la firma il destinatario cifra $f$ con la chiave pubblica del mittente

# Firma digitale

Dunque ora siamo al sicuro? Ovviamente *NO!*

- Come facciamo ad essere sicuri che la chiave pubblica in nostro possesso sia davvero quella del destinatario col quale noi vogliamo comunicare?
- Verifica diretta $\rightarrow$ Web of trust
- Certification Authority

# Firma digitale

Dunque ora siamo al sicuro? Ovviamente *NO!*

- Come facciamo ad essere sicuri che la chiave pubblica in nostro possesso sia davvero quella del destinatario col quale noi vogliamo comunicare?
- Verifica diretta $\rightarrow$ Web of trust
- Certification Authority

# SSL

## Secure Socket Layer

È un protocollo di cifratura che si aggiunge *sopra* una comunicazione già esistente.

Esempio: `https`

1. `mi collego ad un server che supporta SSL`
2. `ci mettiamo d'accordo su un protocollo`
3. `verifico l'identità del server tramite firma/certificato`
4. `via crittografia asimettrica ci scambiamo una chiave`
5. `inizio la comunicazione cifrando il canale con la chiave (simmetrica!) che ci siamo scambiati`

# Il panico di Firefox

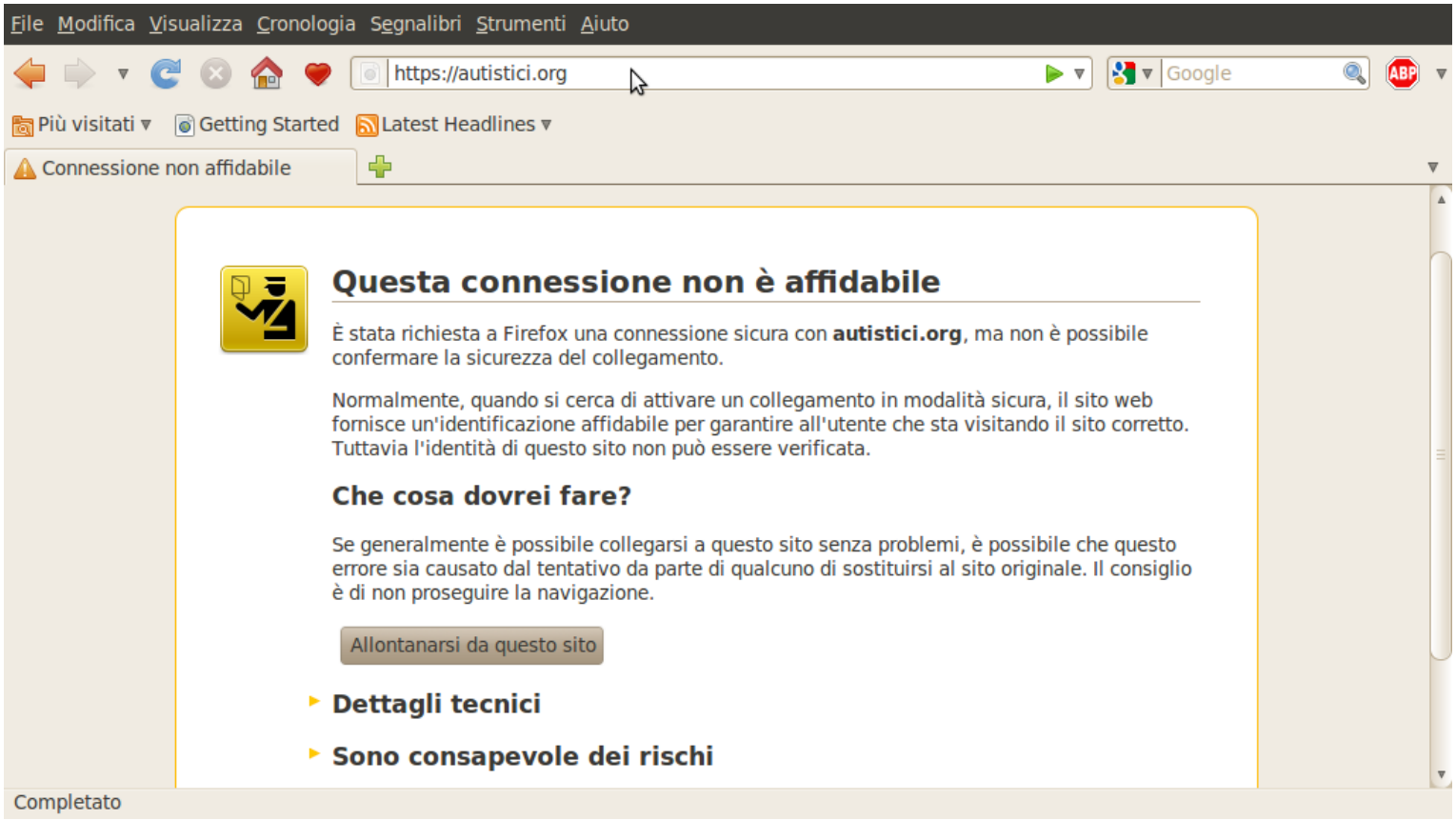
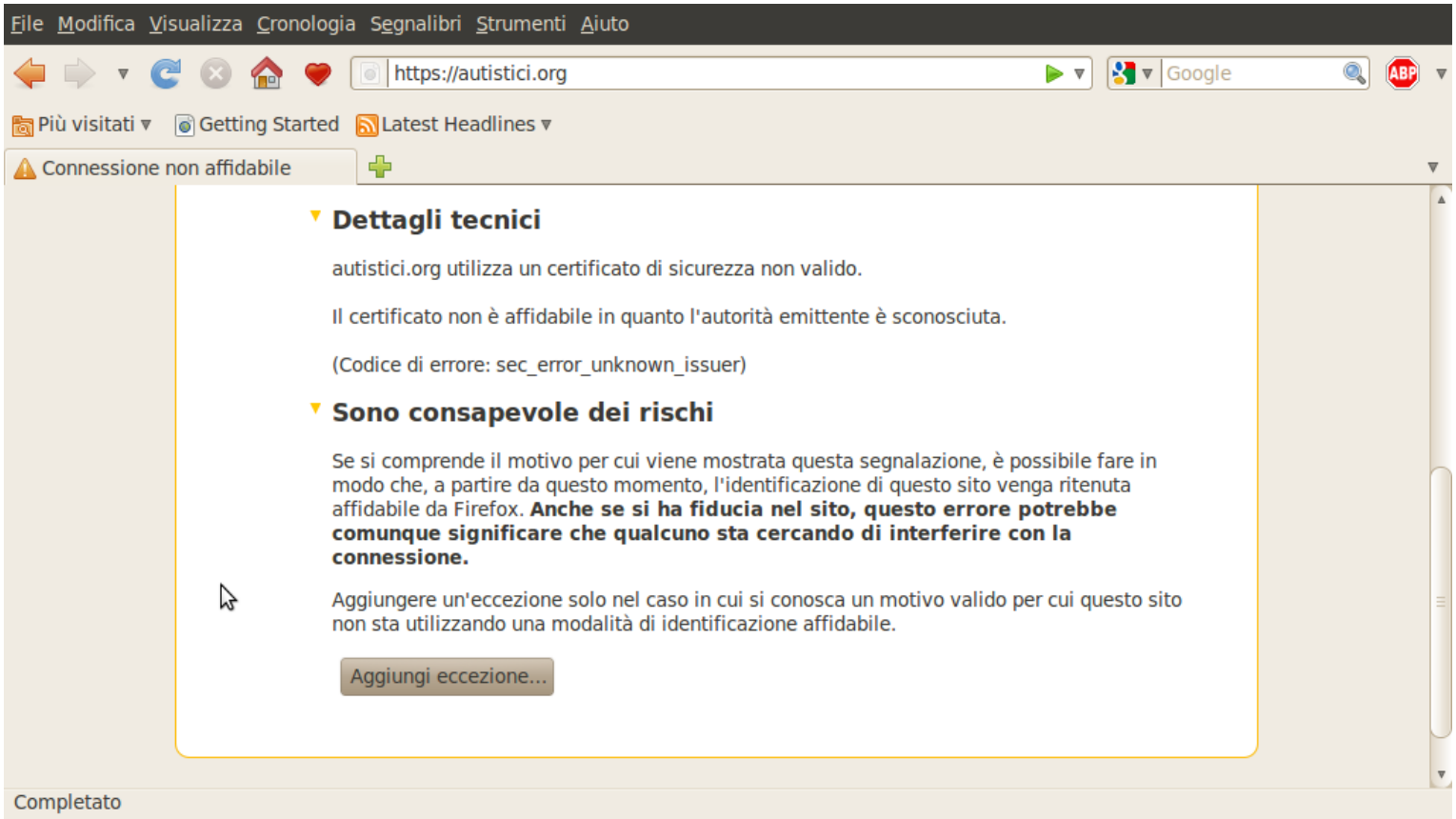
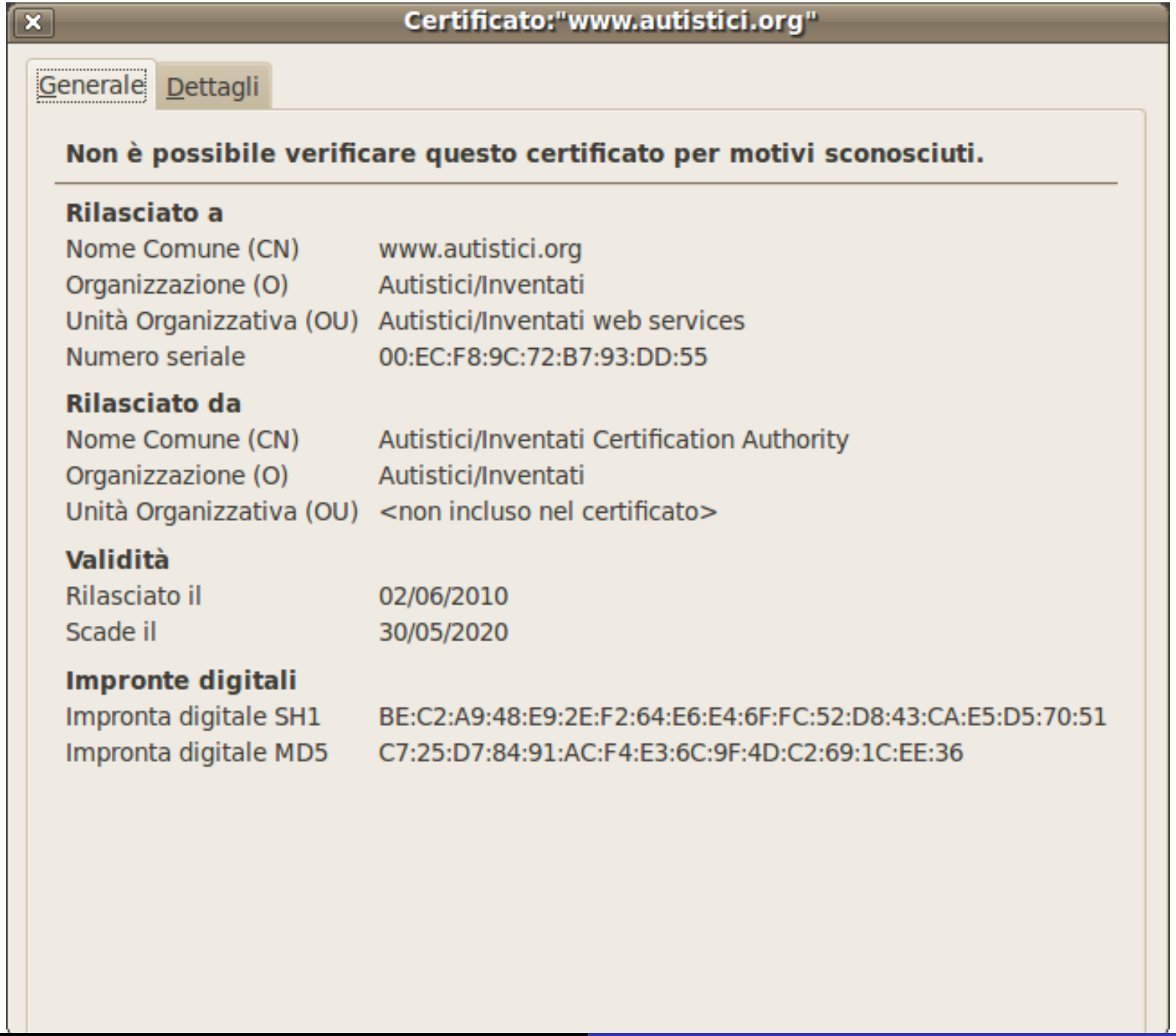



Figura: errore di Firefox

# Come comportarsi

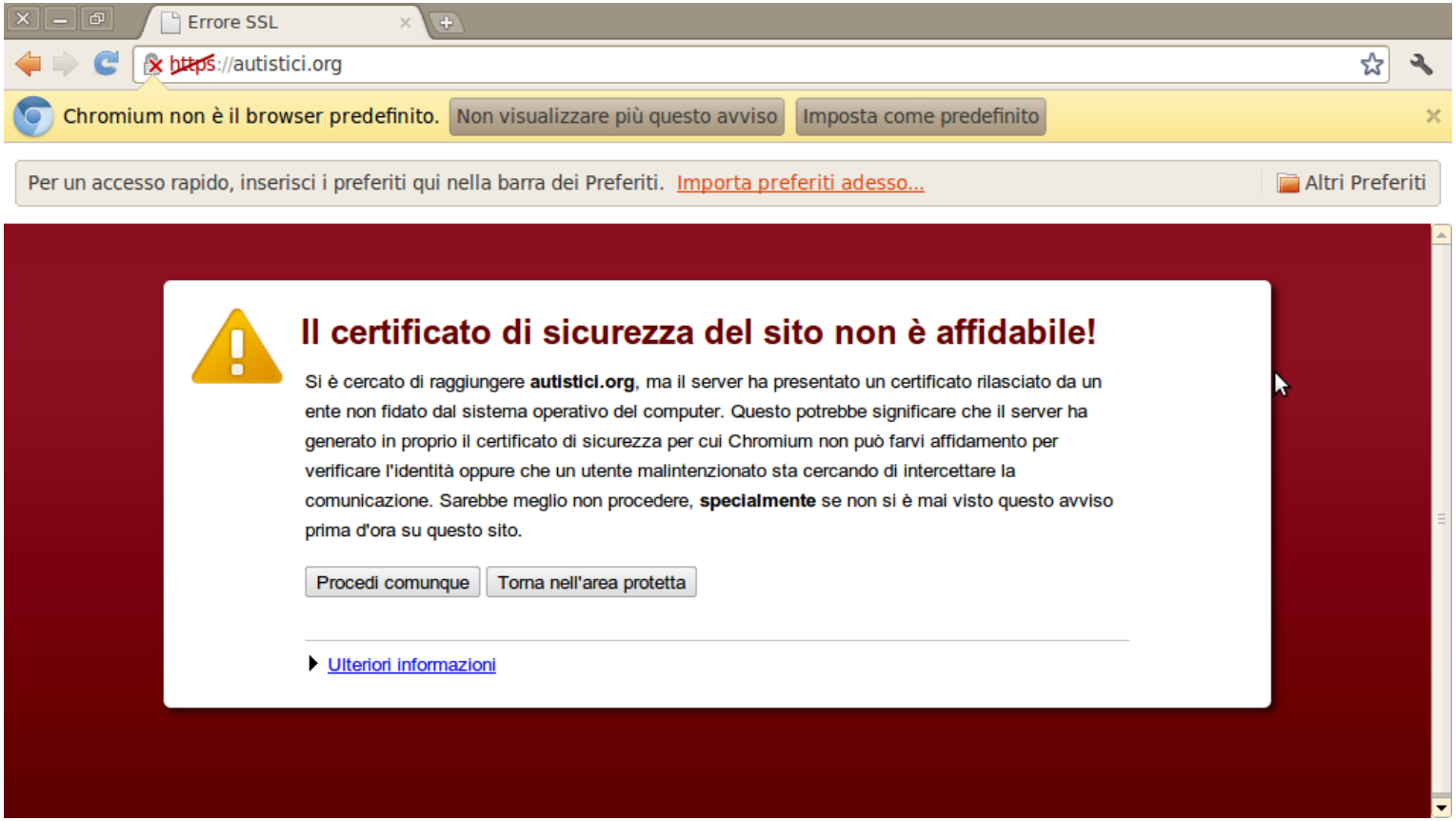



Aggiungi eccezione di sicurezza
Si sta per modificare il modo in cui Firefox identifica questo sito.
Banche, negozi e altri siti pubblici affidabili non ti chiederanno di fare questa operazione.
Server
Indirizzo:
https://autistici.org/
Acquisisci certificato
Stato del certificato
Il sito ha cercato di identificarsi fornendo informazioni non valide.
Visualizza...
Identità sconosciuta
Il certificato non è affidabile in quanto non è stato verificato da un'autorità riconosciuta.
Salva eccezione in modo permanente


Certificato:"www.autistici.org"
Generale
Dettagli
Non è possibile verificare questo certificato per motivi sconosciuti.
Rilasciato a
Nome Comune (CN) www.autistici.org
Organizzazione (O) Autistici/Inventati
Unità Organizzativa (OU) Autistici/Inventati web services
Numero seriale 00:EC:F8:9C:72:B7:93:DD:55
Rilasciato da
Nome Comune (CN) Autistici/Inventati Certification Authority
Organizzazione (O) Autistici/Inventati
Unità Organizzativa (OU) <non incluso nel certificato>
Validità
Rilasciato il 02/06/2010
Scade il 30/05/2020
Impronte digitali
Impronta digitale SH1 BE:C2:A9:48:E9:2E:F2:64:E6:E4:6F:FC:52:D8:43:CA:E5:D5:70:51
Impronta digitale MD5 C7:25:D7:84:91:AC:F4:E3:6C:9F:4D:C2:69:1C:EE:36


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
http://ca.autistici.org/
Google
Più visitati
Getting Started
Latest Headlines
Autistici/Inventati Certification ...
Autistici/Inventati
Certification Authority
Da questa pagina puoi scaricare il certificato della CA di Autistici/Inventati, per installarlo nel tuo computer così da verificare l'autenticità delle tue connessioni con i nostri servizi.
scarica il certificato: formato DER - PEM
A meno che non sappiate di avere bisogno espressamente del formato PEM, scaricate il DER.
guide all'installazione: Mac OS X, Windows, Linux
CRL (v1)
C=IT, O=Autistici/Inventati,
CN=Autistici/Inventati Certification Authority
MD5 Fingerprint
Completato


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
autistici.org https://www.autistici.org/it/
Wikipedia (en)
A/I :: Home
A/I :: [ it en pt ] :: Home /
email:
password:
chi siamo
-manifesto
-il collettivo
-infrastruttura
-ma quanto ci costa?
-policy
-L'associazione Investici
servizi
-posta
-blog e siti web
-instant messaging e chat
-radio
-forum, liste e bookmark
-anonimato
materiali
-manuali per gli utenti
-manuali per amministratori
-archivio storico
-propaganda
people
-il nostro blog
-mailing-list ospitate
-siti ospitati
-progetti amici
join the crew
-richiedi un servizio
-partecipa ad A/I
-contattaci
-fai una donazione
-sviluppo
-adotta un server TOR
don't panic
-FAQ
-forum di AutoAiuto
-supporto tecnico
-password
-stato della rete
La polizia spara nel mucchio: colpirne cento per educarne uno!
È la logica di chi non sa bene che pesci pigliare. Nel dubbio spara nel mucchio, capace che prenderai anche il tuo bersaglio. O quella dei rastrellamenti per cui si buttano all'aria intere strade per cercare magari qualcosa che non c'è. La polizia (postale) italiana ha la brutta abitudine di frugare nei dati di centinaia, migliaia di persone anche solo per trovare un e-mail. È successo di nuovo al server che A/I ha in Norvegia: i dischi sono stati clonati per intero per una indagine di cui non ci hanno ancora detto nulla. Anche se non siamo direttamente coinvolti in una eventuale inchiesta resta il fatto che i dati dei nostri utenti (nella maggior parte dei casi crittati) sono comunque stati acquisiti da qualcuno che al massimo aveva il mandato per cercare una specifica cosa.
In Evidenza
PAURA DEL BUIO?
Il babau é l'ultima frontiera nella politica dell'ansia. Semplice e primordiale paura. Qualcosa di ancora diverso dal terrore, qualcosa di più simile alla goccia che ti cade in testa e piano piano ti porta incosapevolmente alla pazzia. Il nostro buffo mondo sta prendendo coscienza dell'esistenza del babau. L'ansia di sicurezza, la paura del proprio simile, il rancore confuso e convulso che trasudano da ogni dove in questi anni difficili, trovano la propria
Completato


Errore SSL
https://autistici.org
Chromium non è il browser predefinito.
Non visualizzare più questo avviso
Imposta come predefinito
Per un accesso rapido, inserisci i preferiti qui nella barra dei Preferiti.
Importa preferiti adesso...
Altri Preferiti
Il certificato di sicurezza del sito non è affidabile!
Si è cercato di raggiungere autistici.org, ma il server ha presentato un certificato rilasciato da un ente non fidato dal sistema operativo del computer. Questo potrebbe significare che il server ha generato in proprio il certificato di sicurezza per cui Chromium non può farvi affidamento per verificare l'identità oppure che un utente malintenzionato sta cercando di intercettare la comunicazione. Sarebbe meglio non procedere, specialmente se non si è mai visto questo avviso prima d'ora su questo sito.
Procedi comunque
Torna nell'area protetta
Ulteriori informazioni

# Bibliografia


- Simon Sing, *Codici e segreti*, Rizzoli, 2003.
- Paolo Ferragina e Fabrizio Luccio, *Crittografia, principi, algoritmi, applicazioni*, Boringhieri, 2007.
- Joe Lametta, *Kriptonite*, Nautilus, 1998.
- AA.VV., *Handbook of applied cryptography*, CRC Press, 1996.
- Wikipedia