http://www.olografix.org
info@olografix.org
metro olografix
associazione culturale telematica

METRO OLOGRAFIX CRYPTO MEETING

Gpg, Kgpg, Kmail

Crittografia con sofware libero

Pescara, Sala dei Marmi

Silvano Tuccella

docente Informatica ITC "R. De Sterlich"

certificazioni:

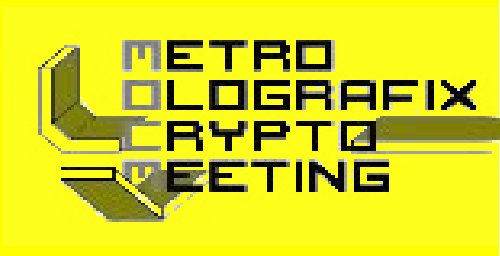
Cisco CCNA

ECDL Advanced

tentuc@alice.it

http://www.olografix.org
info@olografix.org
metro olografix
associazione culturale telematica

Indice



Steganografia e crittografia

dalle parole greche

- steganós, che significa coperto e
- gráphein, che significa scrivere

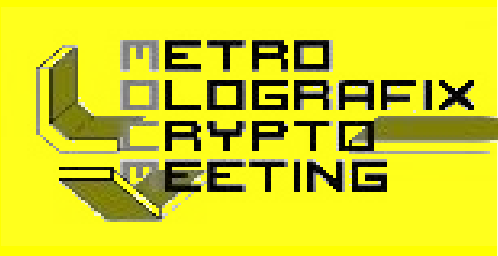
- quindi OCCULTARE messaggio.
  - kryptós, che significa nascosto

- nascondere non il messaggio ma il suo significato.

Steganografia e crittografia

vantaggio della crittografia

se il messaggio viene intercettato risulta incomprensibile e quindi inutilizzabile.



Steganografia e crittografia

Esempio nell'antica Persia:

a)rasare testa schiavo

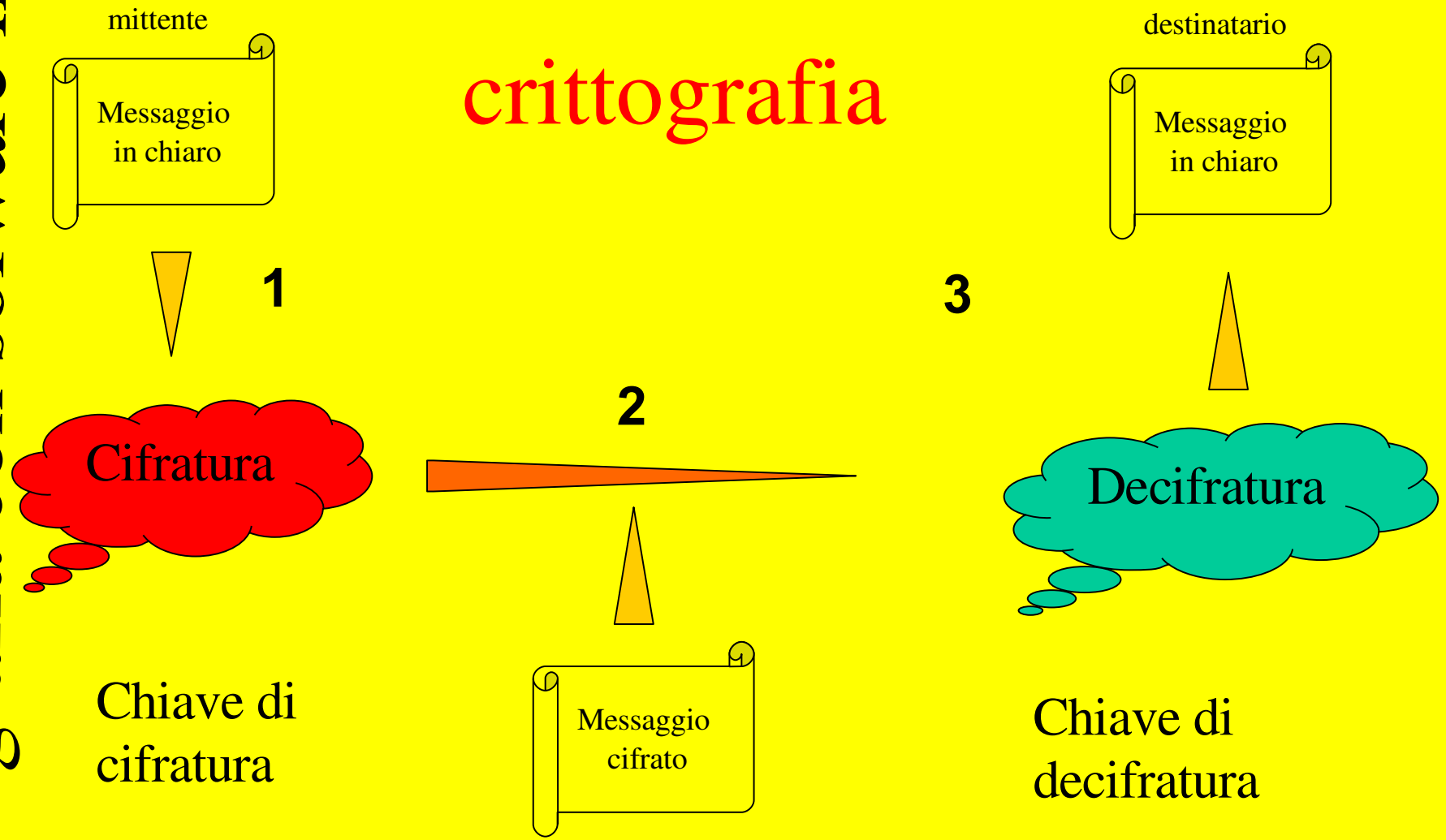
b)scrivere messaggio

c)far crescere capelli

d)inviare lo schiavo

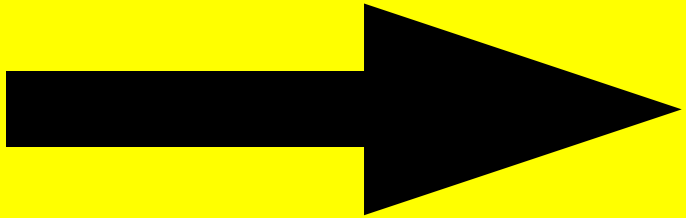
e)rasare di nuovo la testa dello schiavo

crittografia



Steganografia e crittografia

impiegate insieme per alterare e occultare il medesimo testo:



garanzia di un livello di sicurezza molto più alto.

microdot la riduzione di uno scritto alle dimensioni di un punto (agenti tedeschi in America latina durante la seconda guerra mondiale)

Steganografia e crittografia

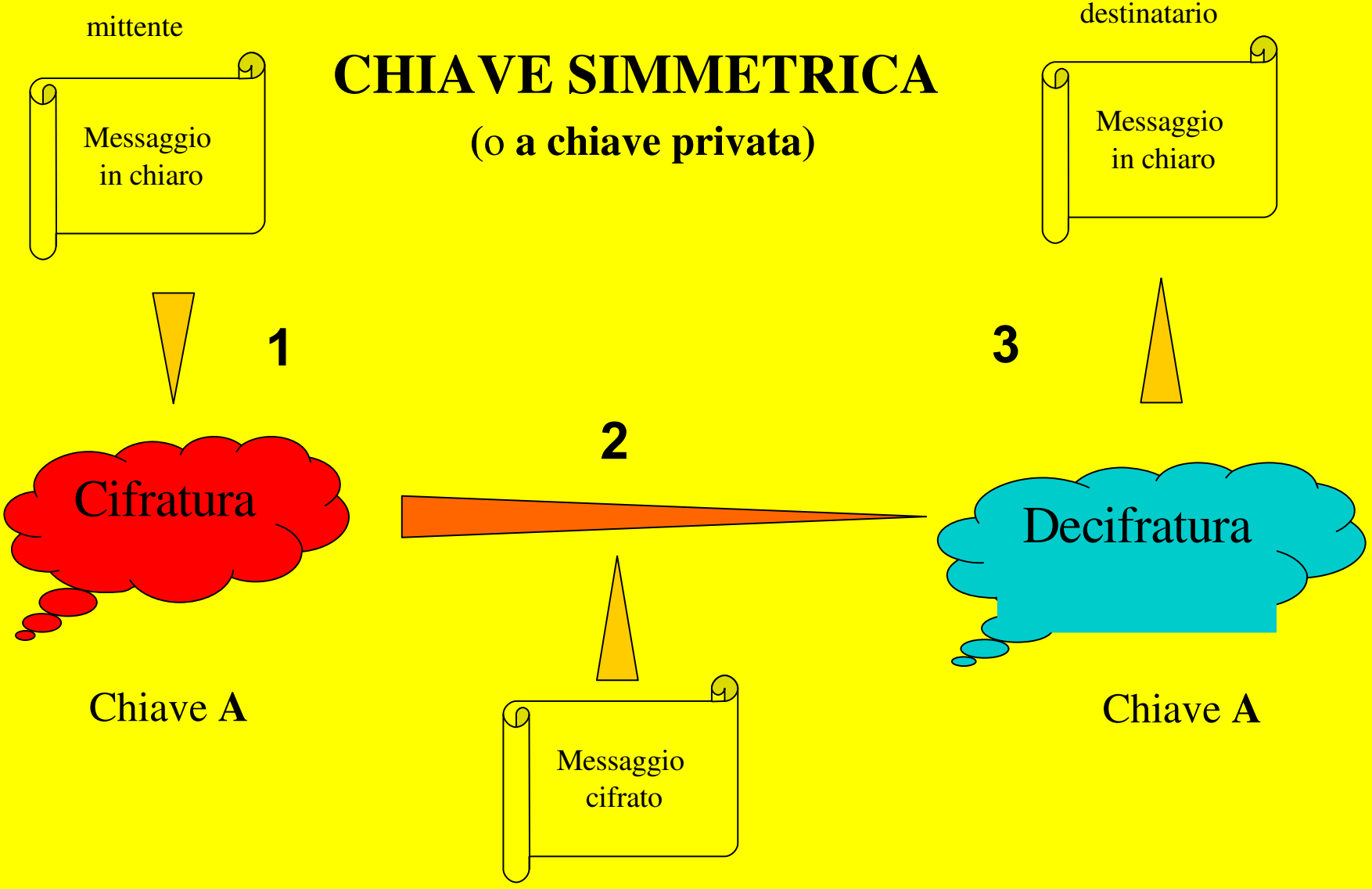
pagina scritta → crittografata → xz%@# → procedimento fotografico → .

macchia diametro inferiore al millimetro, che può essere nascosta in una parola Metro Olografix

Il primo microdot fu scoperto dall' FBI nel 1941 grazie a una soffiata.

CHIAVE SIMMETRICA

(o a chiave privata)



CHIAVE ASIMMETRICA

(o **a chiave pubblica**)

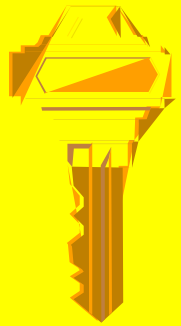
Gpg, Kgp, Kmail

Crittografia con sofware libero

http://www.olografix.org
info@olografix.org
metro olografix
associazione culturale telematica

METRO OLOGRAFIX CRYPTO MEETING

chiavi asimmetriche



La chiave **privata**

serve per crittografare

il messaggio

Firma

La chiave **pubblica**

serve per decodificare

il messaggio

Verifica della firma

chiavi asimmetriche

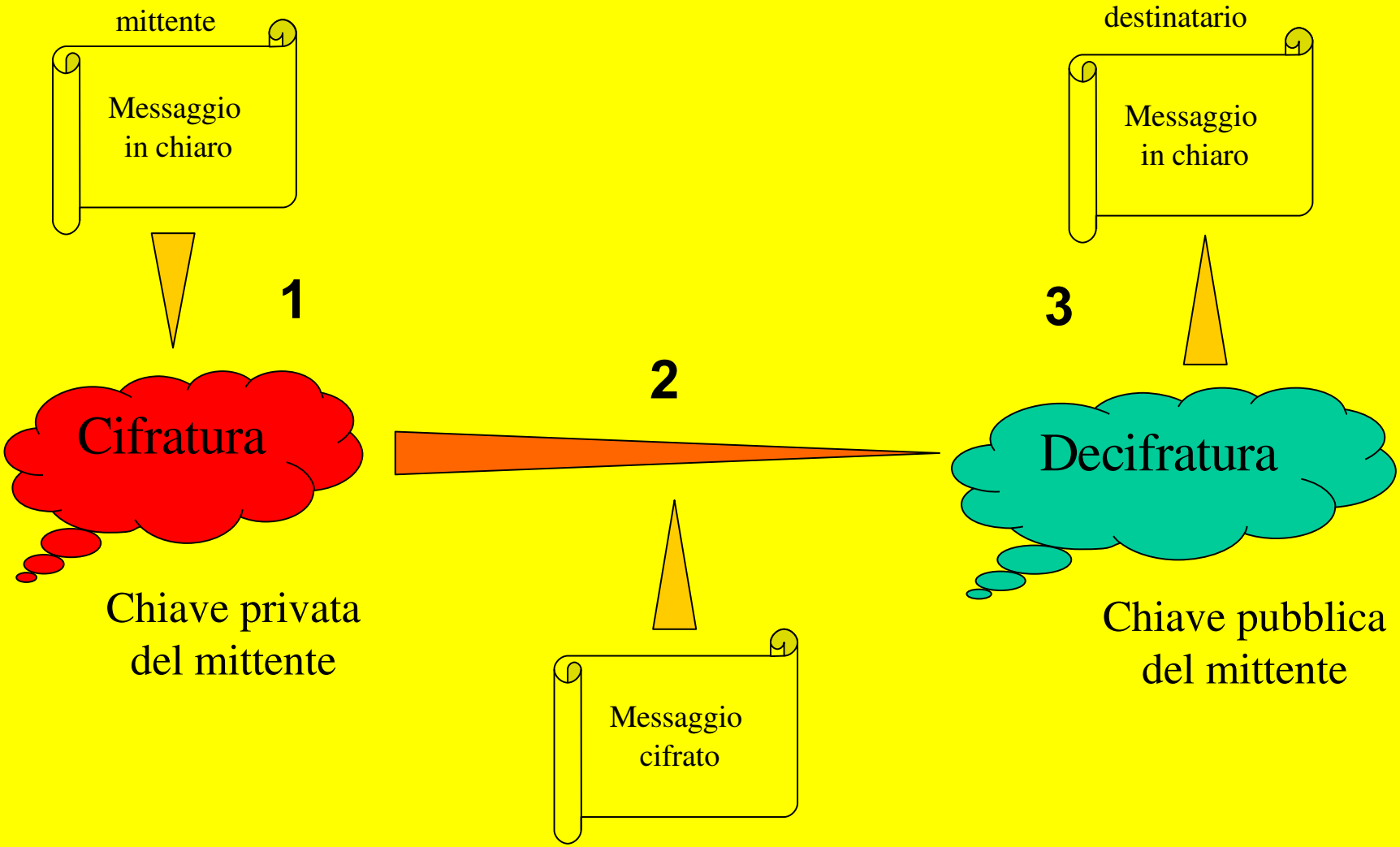
La chiave **privata**

è nota solo al proprietario

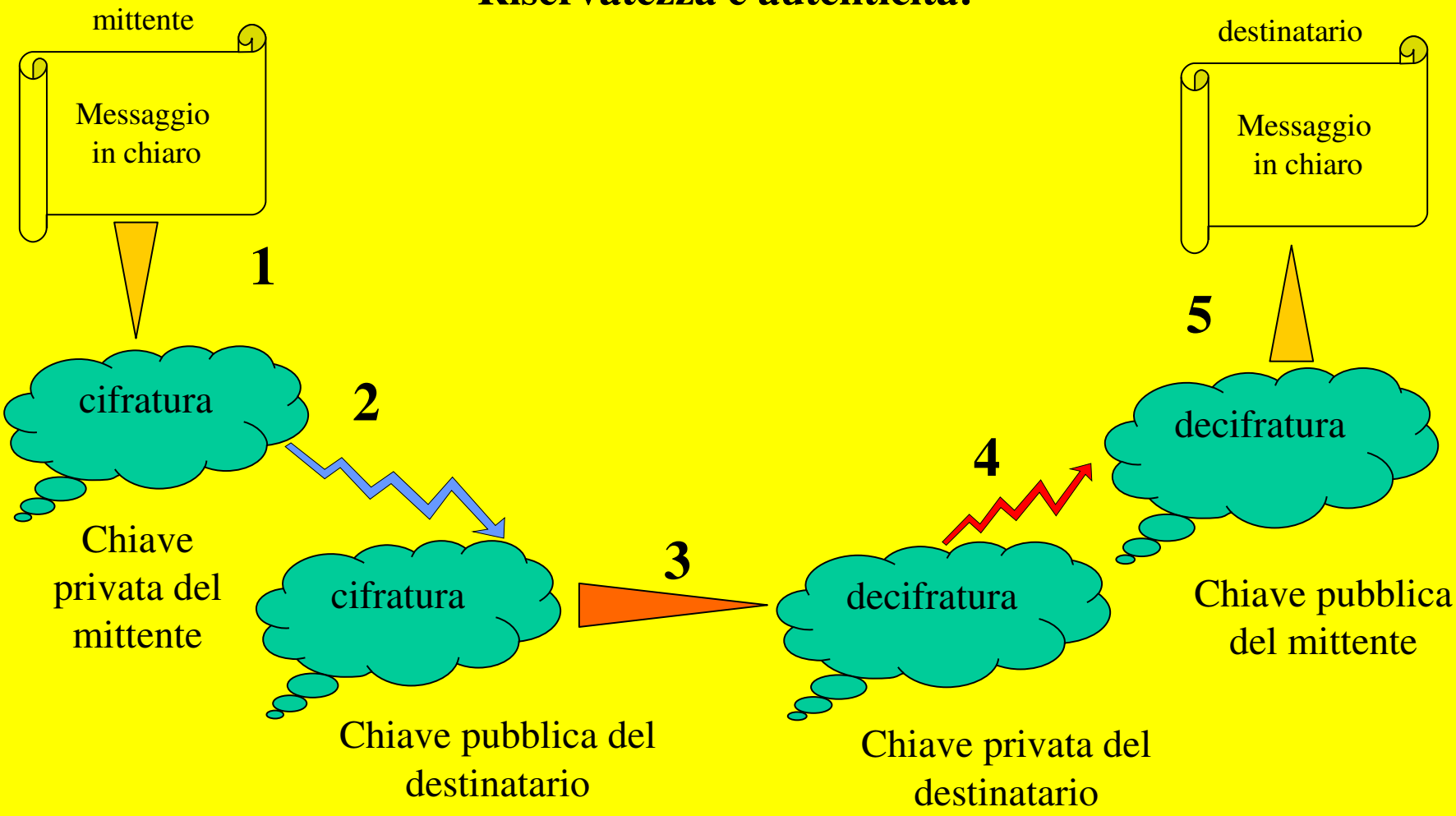
La chiave **pubblica**

è di dominio pubblico

Autenticità:



Riservatezza e autenticità:



Steganografia e crittografia

Crittografia e computer (complessità algoritmo)

- DES (Data Encryption Standard) IBM
  - cifrario a chiave segreta composto
  - prevede 16 cifrature successive (trasposizioni e sostituzioni di bit)
  - basato su chiave a 56 bit (2^{56} chiavi possibili, un numero con sedici cifre decimali!)

Steganografia e crittografia

Crittografia e computer (complessità algoritmo)

- DES (Data Encryption Standard) IBM
  - ipotesi costruire un computer capace di forzare il D.E.S. con una brutale ricerca esaustiva dello spazio chiave (che richiederebbe 3,5 ore).
  - Costo previsto 1 milione di dollari;
  - il computer non è ancora stato realizzato.
  - Si può ritenere ancora sicuro

Steganografia e crittografia

Crittografia e computer (complessità algoritmo)

- DES (Data Encryption Standard) IBM
  - ha il vantaggio della velocità di cifratura che è molto superiore a quella del suo principale rivale il codice RSA.
  - in risposta ai numerosi tentativi di forzatura
    - è stato elaborato il D.E.S. Triplo, uno speciale tipo di D.E.S. a tre livelli di cifratura
    - usare una chiave a 128 bit

Steganografia e crittografia

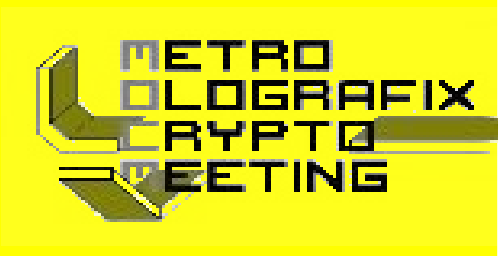
Crittografia e computer (scambio chiavi)

- Anche su canale non sicuro (1)
  - Usare esponenziazione modulare
  - Partire da configurazione di bit nota
  - Alice e Bob (nomi convenzionali dati dai crittografi a due corrispondenti generici) applicano le loro funzioni esponenziali (non è importante in che ordine perché sono commutative)

Steganografia e crittografia

Crittografia e computer (scambio chiavi)

- Anche su canale non sicuro (2)
  - Ognuno spedisce all'altro il risultato ottenuto
  - Ognuno applica la propria funzione a quanto ricevuto
  - Sia Alice che Bob adesso hanno la chiave per cifrare e decifrare



Steganografia e crittografia

Crittografia e computer (scambio chiavi)

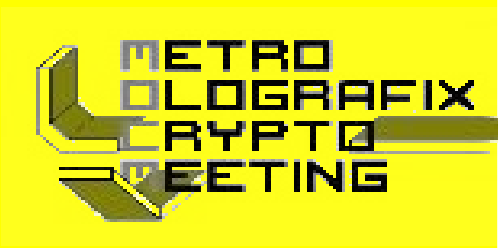
Numero pubblico **2**

Funzione Alice 2^3 → **8**

Funzione di Bob 2^6 → **64**

Funzione di Alice 64^3 → **262144**

Funzione di Bob 8^6 → **262144**



Steganografia e crittografia

Crittografia e computer (scambio chiavi)

- Manca però proprietà delle funzioni unidirezionali (ad es. dopo l'elevamento a potenza prendiamo solo i bit meno significativi in numero definito)
- un intercettatore può ricavare il numero segreto a partire dalla successione pubblica di bit o dalla versione esponenziale che Alice e Bob si scambiano.

Steganografia e crittografia

Crittografia e computer (IDEA)

- 1992 IDEA (International Data Encryption Algorithm).
- ' molto resistente agli attacchi a forza bruta:
  - non solo per la lunghezza della chiave
  - output una combinazione molto complessa dell'input
  - rende difficile la crittoanalisi

Steganografia e crittografia

Crittografia e computer (IDEA)

- Usa tre operazioni
  - addizione senza riporto modulo 2^{16}
  - moltiplicazione modulo 2^{16}
  - or-esclusivo
- Utilizza chiavi a 128 bit e cifra blocchi di 64 bit per volta

Steganografia e crittografia

Crittografia e computer (chiave pubblica)

- Affinamento tecnica scambio chiavi
  - Alice genera con sw apposito coppia chiavi
    - Privata assolutamente segreta
    - Pubblica diffusa liberamente
  - Bob fa lo stesso

Steganografia e crittografia

Crittografia e computer

- cifrario Rivest Shamir Adleman
  - Nel 1976 Diffie ed Hellmann propongono l'idea di una crittografia a chiave pubblica
  - non avevano definito un metodo funzionante
  - Definito da tre matematici Rivest Shamir Adleman chiamato appunto RSA nel 1977 e presentato nel 1978.

Steganografia e crittografia

Crittografia e computer (RSA)

- la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi molto grandi (centinaia di cifre decimali) che restano segreti.
- sfrutta la difficoltà di fattorizzare un numero
- Il sistema si basa su due risultati matematici dovuti a Fermat e a Eulero: la funzione di Eulero e il teorema di Fermat-Eulero.

Steganografia e crittografia

Crittografia e computer (RSA)

- funzione di Eulero N° dei numeri interi primi con n
  - ΦF(n) = n(1 - 1/n1)(1 - 1/n2)...(1 - 1/nm)
    - dove n1, n2 ... nm sono i fattori primi distinti di n.
    - Se n è primo allora ovviamente Φ(n) = n - 1
    - Se n è il prodotto di due numeri primi p e q, è facile verificare che Φ(n) = (p - 1)(q - 1)
- teorema di Fermat-Eulero
  - Dati due numeri qualsiasi m ed N primi tra di loro allora è:
  - $m^{\Phi F(N)} = 1 \pmod N$

http://www.olografix.org
info@olografix.org
metro olografix
associazione culturale telematica

Steganografia e crittografia

Crittografia e computer (RSA)

- Enorme successo con la sempre maggiore diffusione di Internet
- ancor oggi il cifrario a chiave pubblica più usato.
- operazioni sicure sul web (protocollo https) usano oggi certificati basati su RSA

Steganografia e crittografia

Crittografia e computer (RSA)

- Ogni utente del sistema ha una coppia di chiavi, una pubblica e l'altra privata che vengono pubblicate da un ente che ne garantisce l'autenticità.
- RSA è usato anche per generare le firme digitali. Una versione gratuita che ha avuto grande successo è PGP, Pretty Good Privacy.

Steganografia e crittografia

Crittografia e computer (RSA)

- Alice per inviare un messaggio riservato a Bob, deve prima di tutto andare a cercare sull'elenco le chiavi pubbliche di Bob. Usando questi numeri con una serie di calcoli piuttosto complessi Alice ottiene il messaggio cifrato da inviare a Bob.
- Bob riceve il messaggio e usa la sua chiave segreta per decifrarlo con un calcolo; solo lui conosce questo numero e quindi solo lui può decifrare il messaggio (paradossalmente nemmeno Alice può decifrare il suo stesso messaggio).

Steganografia e crittografia

Cifrari a chiave pubblica

calcoli piuttosto complessi

Metodo	Problema arduo
• DH (Diffie-Hellman)	calcolo del logaritmo discreto
• El Gamal	calcolo del logaritmo discreto
• RSA	fattorizzazione di un intero
• DSA	calcolo del logaritmo discreto

Steganografia e crittografia

Cifrari a chiave pubblica

calcoli piuttosto complessi

- calcolo del logaritmo discreto
- $a^b = x \bmod n$
- $b = \log_a x \bmod n$
  - calcolo della potenza è relativamente semplice
  - calcolo del logaritmo è computazionalmente molto complesso, può avere più soluzioni o anche nessuna.

Steganografia e crittografia

Cifrari a chiave pubblica

calcoli piuttosto complessi

- Per es. in un'aritmetica di ordine 7 si ha:
  - $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4, 2^6 = 1$
  - e quindi p.es. il $\log_2 4$ è 2 ma anche 5. Viceversa non esistono $\log_2 3$, $\log_2 5$, $\log_2 6$.
- Si ritiene che la complessità computazionale del calcolo del logaritmo discreto sia dello stesso ordine di una fattorizzazione anche se manca una dimostrazione.

Steganografia e crittografia

Crittografia e computer (RSA)

- Alice genera le sue chiavi pubbliche e private
- Alice genera due numeri primi distinti p e q e li moltiplica tra di loro ottenendo il numero N che viene reso pubblico, mentre p e q devono restare segreti.
  - Esempio:
    - **p** = 5; **q** = 11
    - p*q = 5*11 = 55 quindi **N** = 55

Steganografia e crittografia

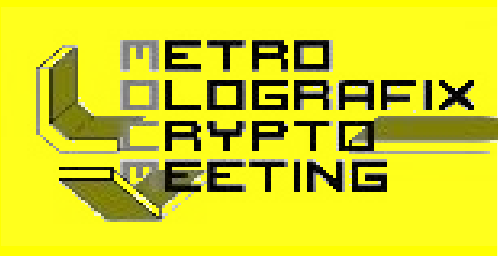
Crittografia e computer (RSA)

- Alice calcola b che è la funzione di Eulero di n:
- **b** = Φ(n) = (p-1)*(q-1)
- Il numero b deve restare segreto.
  - Esempio:
    - Φ(55) = (5 - 1).(11 - 1) = 4*10 = 40
    - **b** = 40

Steganografia e crittografia

Crittografia e computer (RSA)

- Alice calcola il primo intero e che sia primo con b (non abbia divisori in comune)
  - ovvero MCD(e, b) = 1
- Il numero **e** è la seconda chiave pubblica
  - Esempio:
    - e = 2 -> MCD(2, 40) = 2 NO
    - e = 3 -> MCD(3, 40) = 1 SI
    - Quindi e = 3



Steganografia e crittografia

Crittografia e computer (RSA)

- Alice calcola il numero d inverso di e nell'aritmetica finita di ordine b, che è il più piccolo x per cui sia
- e*d mod b = 1;
- il numero **d é la chiave per decifrare** e deve restare segreto
- si potrebbe usare il metodo basato sulla funzione di Eulero ma per numeri grandi la complessità sarebbe proibitiva; molto più efficiente un'estensione del classico algoritmo di Euclide per l'MCD

Steganografia e crittografia

Crittografia e computer (RSA)

- Esempio:
  - d = 2 -> 2*3 mod 40 = 6 NO
  - d = 3 -> 3*3 mod 40 = 9 NO
  - d = 4 -> 4*3 mod 40 = 12 NO
  - ...
  - d = 26 -> 26*3 mod 40 = 78 mod 40 = 38 NO
  - d = 27 -> 27*3 mod 40 = 81 mod 40 = 1 SI
  -
  - quindi d = 27

Steganografia e crittografia

Crittografia e computer (RSA)

- Bob invia un messaggio ad Alice
  - Bob lo scompone in una sequenza di numeri (in precedenza ci si è accordati riguardo alla modalità di "traduzione"; potrebbero essere p.es. i codici ASCII dei singoli caratteri ma così il cifrario degenererebbe in un banale cifrario monoalfabetico)
  - Bob legge le chiavi pubbliche di Alice N e E e trasmette i numeri m uno alla volta cifrandoli con la formula

$$c=m^e \bmod n$$

Steganografia e crittografia

Crittografia e computer (RSA)

- Esempio: per trasmettere il numero 7
  - Bob calcola $c = m^e \bmod N = 7^3 \bmod 55 = 343 \bmod 55 = 13$
  - il numero da trasmettere è quindi 13.
- Alice decifra il messaggio cifrato di Bob
  - Alice usa la chiave di decifrazione d segreta
  - $m = c^d \bmod N$
  - infatti si dimostra che $c^d \bmod N = m$.
  - Esempio: $m = c^d \bmod n = 13^{27} \bmod 55 = 7$

Steganografia e crittografia

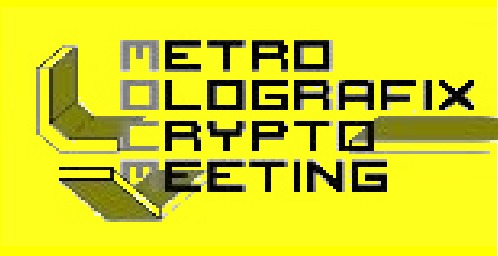
riassumendo

Utente	Parte Pubblica		Parte Segreta		
Alice	N	E	p, q [N = p*q]	B = F(N)	D
	55	3	5, 11 [55 = 5*11]	40 = Φ(55)	29

Steganografia e crittografia

Crittografia e computer (RSA)

- considerato sicuro perchè si ritiene che solo individuando i fattori primi della chiave pubblica sarebbe possibile decifrare il messaggio
- la fattorizzazione di un numero enorme (si usano oggi chiavi di 1024 o 2048 bit) richiede tempi proibitivi



Steganografia e crittografia

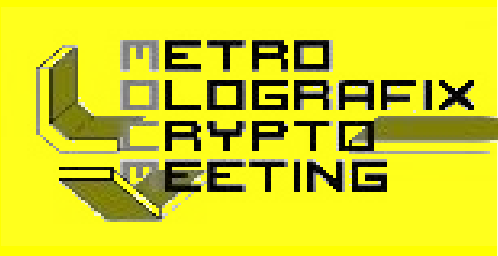
Crittografia e computer (RSA)

- Non è dimostrato che sia necessaria la fattorizzazione per forzare RSA
- potrebbe esistere un metodo per calcolare la funzione di Eulero $\Phi(N)$, senza conoscere i fattori primi di N
- è stato dimostrato però che il calcolo della funzione di Eulero comporta una complessità paragonabile alla fattorizzazione
- finora nessun metodo del genere è stato trovato

Steganografia e crittografia

Crittografia e computer (RSA)

- difetto di RSA
  - mole dei calcoli aritmetici
    - codifica consiste essenzialmente in un elevamento a potenza in un'aritmetica finita
    - essenziale avere algoritmi veloci per il calcolo della potenza.
  - molto più lento (circa mille volte) del DES
  - si usano spesso soluzioni miste:
    - RSA è utilizzato solo per trasmettere la chiave segreta di un DES
    - il messaggio vero e proprio viene trasmesso appunto con il DES



Steganografia e crittografia

Confronto metodi

Chiave	Vantaggi	Svantaggi
Simmetrica	Velocità	Difficoltà scambiare chiave
		Utenti N
		Chiavi --> N * (N-1) / 2
Asimmetrica	N utenti: N+N chiav	Lentezza

Steganografia e crittografia

Crittografia e computer (GPG)

- Lo GNU Privacy Guard
  - sostituto completo e libero di PGP
  - non usa l'algoritmo brevettato IDEA
  - può essere usato senza restrizioni
  - conforme alla RFC2440 (OpenPGP).
  - la versione 1.0.0 è stata rilasciata il 7/09/1999
  - ultima versione stabile 1.4.2

Steganografia e crittografia

Crittografia e computer (GPG)

- Caratteristiche
  - strumento a linea di comando senza nessun aspetto grafico
  - può essere considerato come un backend per altre applicazioni.
  - fornisce tutte le funzionalità necessarie, compreso un sistema di menù interattivo. I comandi forniti da questo strumento saranno sempre di piú di quelli forniti da un qualsiasi suo frontend

Steganografia e crittografia

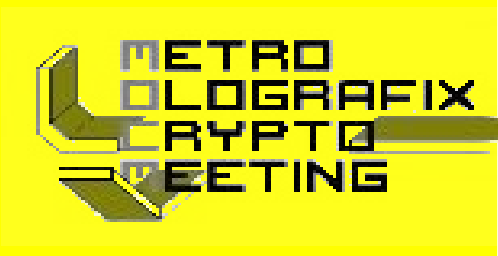
Crittografia e computer (GPG)

- Caratteristiche (2)
  - Sostituto completo di PGP, scritto da zero
  - Non utilizza algoritmi brevettati.
  - Coperto da licenza GPL
  - Implementazione OpenPGP completa (si veda la RFC2440 su RFC Editor)
  - Più funzionale di PGP e con alcune migliorie in fatto di sicurezza rispetto a PGP 2
  - Decifra e verifica i messaggi di PGP 5, 6 e 7

Steganografia e crittografia

Crittografia e computer (GPG)

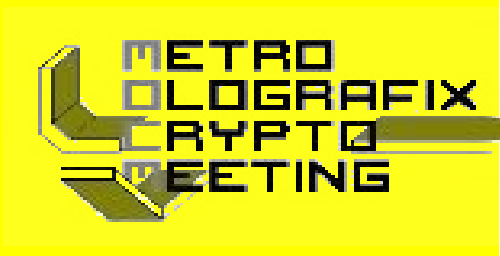
- Caratteristiche (3)
  - Supporta ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 e TIGER.
  - Facile implementazione di nuovi algoritmi usando i moduli d'estensione
  - Lo User ID è forzato ad un formato standard.
  - Supporta le date di scadenza di chiavi e firme



Steganografia e crittografia

Crittografia e computer (GPG)

- Caratteristiche (3)
  - Supporto multilingue tra cui l'**italiano**
  - Sistema di aiuto in linea.
  - Destinatari anonimi opzionali.
  - Supporto integrato per server di chiavi HKP (wwwkeys.pgp.net).
  - File di patch firmati processabili con il comando patch.



Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key //`**crea una nuova coppia di chiavi primaria.
  - `Per favore scegli che tipo di chiave vuoi:`
  - `(1) DSA e ElGamal (default)`
  - `(2) DSA (firma solo)`
  - `(4) ElGamal (firma e cifra)`
  - `Cosa scegli?`

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria
  - Diversi tipi di coppie di chiavi
  - Una chiave primaria deve essere capace di:
    - Fare firme (solo tre opzioni)
      - L'opzione 1 crea in realtà due coppie di chiavi: una coppia di chiavi di tipo DSA che rappresenta la coppia di chiavi primaria ed è utilizzabile solo per firmare
      - Una coppia di chiavi subordinata di tipo ElGamal, usata per criptare

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **gpg --gen-key** //crea una nuova coppia di chiavi primaria.
  - L'opzione 2 simile alla precedente
    - crea solo una coppia di chiavi DSA.
  - L'opzione 4
    - crea una singola coppia di chiavi ElGamal utilizzabile sia per firmare che per criptare
    - è possibile in un secondo momento creare sotto-chiavi addizionali per cifrature e firme.

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria.
  - dimensione chiave DSA compresa fra **512 e 1024** bit
  - chiave ElGamal può essere di qualsiasi dimensione
  - GnuPG accetta chiavi non più piccole di 768 bit
  - Se si chiede una chiave DSA > 1024 sarà solo di 1024 bit
  - Default 1024 bit
  - Max consigliato 2048 (diventa lento!)

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria.
  - > lunghezza chiave > sicurezza contro attacchi a forza bruta
  - utilizzo comune la dimensione di default è adeguata
  - chiave lunga
    - più economico aggirare la cifratura piuttosto che provare a romperla
    - cifratura e decifratura sono più lente
    - influenza negativamente la lunghezza della firma
    - una volta scelta non può più essere modificata

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria.
  - scegliere una data di scadenza (con opzione 1 utilizzata sia per la coppia di chiavi ElGamal che per quella DS).
    - Per favore specifica per quanto la chiave sarà valida.
      - 0 = la chiave non scadrà
      - <n> = la chiave scadrà dopo n giorni
      - <n>w = la chiave scadrà dopo n settimane
      - <n>m = la chiave scadrà dopo n mesi
      - <n>y = la chiave scadrà dopo n anni

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria.
  - chiave che non scade adeguata per la maggior parte degli utenti
  - Negli altri casi la scadenza va scelta con cura tenendo presente che:
    - è possibile cambiarla
    - potrebbe risultare difficile comunicare un cambiamento alle persone che possiedono quella chiave pubblica.

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria.
  - Viene poi chiesto uno USERID `Nome e Cognome:`
    - Utilizzato per associare la chiave che si sta creando ad una persona reale.
    - Solamente uno User ID viene creato nel momento in cui si genera una nuova chiave
    - È possibile aggiungere ulteriori User ID in seguito nel caso in cui si desiderasse utilizzare la chiave in contesti diversi, come ad esempio sul lavoro e a casa
    - Va creato con cura in quanto non può più essere modificato.

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-key`** `//`crea una nuova coppia di chiavi primaria.
  - GnuPG necessita di una “frase d’ordine”[3] `passphrase` per proteggere le chiavi primarie e subordinate
    - lunghezza senza limiti
    - scelta con attenzione dal punto di vista della sicurezza
      - usata per sbloccare la chiave privata
      - è uno dei punti più deboli di GnuPG (così come di altri sistema di crittografia a chiave pubblica)
      - unica protezione che si possiede nel caso in cui un’altra persona entri in possesso della propria chiave privata

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-revoke /* genera un certificato di revoca per la chiave pubblica primaria */`**
- Certificato di revoca indispensabile se:
  - si dimentica la passphrase
  - la propria chiave privata viene compromessa o persa
  - pubblicato per segnalare ad altri che la chiave pubblica non deve più essere usata
- Farlo subito dopo aver generato le chiavi

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-revoke /* genera un certificato di revoca per la chiave pubblica primaria */`**
  - chiave pubblica revocata
    - utilizzata per verificare firme fatte in passato
    - non può più essere usata per cifrare futuri messaggi
    - la revoca non influisce sulla propria capacità di decifrare messaggi spediti in passato, se si possiede ancora l'accesso alla chiave privata

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --gen-revoke /* genera un certificato di revoca per la chiave pubblica primaria */`**
- **`gpg --output revoca.asc --gen-revoke mia_chiave`**
  - `mia_chiave` ID o una qualsiasi altra parte dello User ID che identifica la propria coppia di chiavi
  - Il certificato generato è memorizzato nel file `revoca.asc`
    - omettendo `--output` risultato su standard output
    - metterlo nella propria cassetta di sicurezza

chi pubblica il certificato di revoca rende la chiave pubblica corrispondente inutile

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --list-keys /* elenca le chiavi pubbliche presenti nel proprio portafoglio */`**
- **necessario per potersi scambiare le chiavi**
- **Per spedire una chiave pubblica ad un corrispondente è necessario prima esportarla**

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **gpg --export /* esporta la chiave individuata da ID o una qualsiasi altra parte dello User ID */**

```
gpg --output alice.gpg --export tentuc@alice.it
```

- **La chiave è esportata in un formato binario**
  - **Problemi se**
    - **spedita per posta elettronica**
    - **pubblicata in una pagina web**
    - **Soluzione: l'opzione --armor forza output con protezione armatura ASCII**

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --import /* importa la chiave pubblica primaria */`**
  - **`gpg --import bob.gpg`**
    - la chiave importata deve venir convalidata
    - GnuPG utilizza un potente e flessibile modello basato sulla fiducia
      - non richiede all'utente di convalidare personalmente ogni chiave
      - può comunque risultare necessaria la convalida personale di alcune chiavi

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --import /* importa la chiave pubblica primaria */`**
  - **`gpg --import bob.gpg`**
    - chiave convalidata
      - verificando l'impronta digitale della chiave stessa
        - visualizzata con l'opzione `--fingerprint`
      - firmandola poi per certificarla come valida

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --import /* importa la chiave pubblica primaria */`**
  - firmandola poi per certificarla come valida
    - prima però è necessario editarla
  - `gpg --edit-key bob@tin.it`
  - E poi dare il comando
    - `fpr` che fornirà l'impronta digitale del tipo 268F 448F CCD7 AF34 183E 52D8 9BDE 1A08 9E98 BC16

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --import /* importa la chiave pubblica primaria */`**
  - L'impronta digitale di una chiave va verificata con il possessore di quella chiave. Ciò può essere fatto
    - di persona
    - per telefono
    - con qualsiasi mezzo
      - per garantirsi che si sta comunicando con il vero possessore della chiave. Se combaciano allora si può essere sicuri di possedere una copia corretta della chiave

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --import /* importa la chiave pubblica primaria */`**
  - controllata l'impronta digitale, si può procedere alla firma in modo da convalidarla.
  - La verifica di una chiave rappresenta un punto debole nella crittografia a chiave pubblica
    - è necessario essere estremamente attenti e controllare sempre un'impronta digitale di una chiave con il possessore
    - prima di firmare la chiave stessa con il comando `sign`

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --import /* importa la chiave pubblica primaria */`**
  - Dopo la firma è possibile controllare la chiave listando le firme ad essa applicate e rilevare la firma che si è appena aggiunta
  - Ogni User ID avrà sulla chiave una o più autofirme e una firma per ogni utente che ha convalidato la chiave
  - Il comando relativo è `check`

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --encrypt /* cifra il documento indicato */`**
  - È necessario possedere le chiavi pubbliche dei destinatari a cui si intende spedire il messaggio
  - Se non si indica il documento da cifrare legge lo standard input
  - Il risultato cifrato è stampato sullo standard output oppure dove specificato con l'opzione –`output`
  - Il documento, oltre ad essere criptato, viene compresso per ragioni di maggior sicurezza

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --encrypt /* cifra il documento indicato */`**
  - **`gpg --output doc.gpg --encrypt --recipient bob@tin.it doc`**
  - L'opzione `--recipient` viene utilizzata una sola volta per ogni destinatario e richiede un argomento extra che specifichi con quale chiave pubblica debba essere criptato il documento
  - In particolare non è possibile decifrare un documento criptato da voi stessi, a meno che non abbiate incluso la vostra chiave pubblica nella lista dei destinatari.

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --decrypt /* decifra il documento indicato */`**
  - **`Bob$ gpg --output doc --decrypt doc.gpg`**
  - Verrà richiesta la passphrase per sbloccare la chiave segreta di Bob
  - `Inserisci la passphrase:`

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --symmetric /* cifra il documento indicato con un algoritmo simmetrico*/`**
  - **`gpg --output doc.gpg --symmetric doc`**
  - la passphrase viene derivata da una frase d'ordine fornita al momento in cui il documento viene criptato
  - per una buona sicurezza, non dovrebbe essere la stessa passphrase utilizzata per proteggere la propria chiave privata
  - La cifratura simmetrica è utile per rendere sicuri i propri documenti quando non è necessario comunicare ad altri la parola d'ordine utilizzata.

Steganografia e crittografia

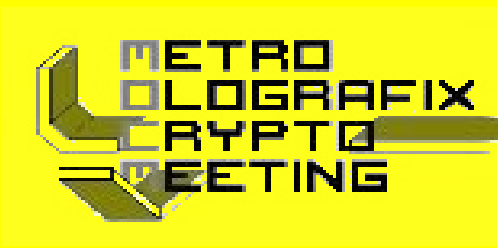
Crittografia e computer (GPG: uso)

- **`gpg --sign // firma il documento indicato`**
  - Una firma digitale
    - certifica e appone la data ad un documento. Se il documento viene successivamente modificato in qualsiasi modo, una verifica della firma fallirà
    - è come una firma fatta a mano con l'ulteriore beneficio di essere a prova di manomissione
    - La distribuzione dei sorgenti di GnuPG è firmata in modo tale da permettere agli utenti di verificare che il codice sorgente non sia stato modificato dal momento in cui è stato creato il pacchetto

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --sign // firma il documento indicato`**
  - Una firma è fatta utilizzando la chiave privata di colui che firma. La firma viene verificata utilizzando la corrispondete chiave pubblica. Per esempio Alice userebbe la propria chiave privata per firmare digitalmente il suo ultimo lavoro per il Linux Day
  - Chiunque potrebbe usare la chiave pubblica di Alice per controllare la firma e verificare che la presentazione sia effettivamente quella mandata da Alice e che non sia stato modificata dal momento in cui Alice l'ha spedita



Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **gpg --verify // per controllare la firma**
- **gpg --decrypt /* per controllare la firma e recuperare il documento originale */**
  - bob% **gpg --output doc --decrypt doc.sig**
  -

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --clearsign /* avvolge il documento in una firma ASCII-armored ma non lo modifica in nessun altro modo */`**
  - Utile per firmare messaggi per Usenet o messaggi di posta elettronica che non dovrebbero essere compressi
  - `alice$ gpg --clearsign doc`
  - serve la passphrase per sbloccare la chiave segreta

Steganografia e crittografia

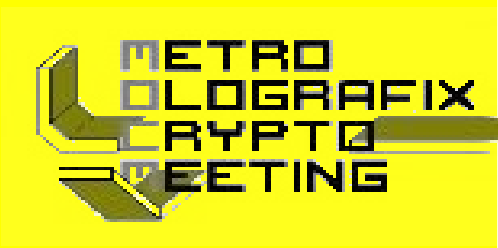
Crittografia e computer (GPG: uso)

- **`gpg --clearsign /* avvolge il documento in una firma ASCII-armored ma non lo modifica in nessun altro modo */`**
  - L'output è del tipo -----BEGIN PGP SIGNED MESSAGE-----
  - Hash: SHA1 [...]
  - -----BEGIN PGP SIGNATURE-----
  - Version: GnuPG v1.4.1 (GNU/Linux) [...]
  - -----END PGP SIGNATURE-----

Steganografia e crittografia

Crittografia e computer (GPG: uso)

- **`gpg --detach-sign /* firma il documento in un file separato */`**
  - Gli utenti possono evitare così di editare il documento (anche quello firmato in chiaro) per poter recuperare l'originale
  - `alice$ gpg --output doc.sig --detach-sig doc`
    - serve sempre la passphrase
  - Sia il documento che la firma distaccata sono necessarie per verificare la firma stessa. L'opzione `--verify` può essere utilizzata per controllare la firma.
  - `bob% gpg --verify doc.sig doc`



Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- L'algoritmo di cfratura usato in GPG fa dipendere la sicurezza solo dalla chiave
- Quindi un malintenzionato che conoscesse il tipo di algoritmo utilizzato sarebbe solo a meno di metà dell'opera perché solo la conoscenza della chiave gli permetterebbe di sfruttare la conoscenza dell'algoritmo

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **algoritmo ibrido**
  - utilizza sia sistema simmetrico sia a chiave pubblica
  - utilizza un algoritmo a chiave pubblica per condividere una chiave per il sistema simmetrico
  - Il messaggio effettivo è quindi criptato usando tale chiave
  - la chiave simmetrica utilizzata è differente per ogni messaggio spedito (**chiave di sessione**)

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **algoritmo ibrido**
  - GnuPG usa algoritmi ibridi (anche PGP)
  - La chiave di sessione, criptata utilizzando l'algoritmo a chiave pubblica, e il messaggio da spedire, cifrato con l'algoritmo simmetrico, sono automaticamente combinati in un solo pacchetto
  - Il destinatario usa la propria chiave privata per decifrare la chiave di sessione che viene poi usata per decifrare il messaggio.

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **algoritmo ibrido**
  - In PGP e GnuPG l'algoritmo a chiave pubblica è probabilmente il più debole dei due
  - se un malintenzionato dovesse decifrare una chiave di sessione, egli sarebbe in grado di leggere solo un messaggio, quello criptato con quella chiave di sessione
  - per poter leggere un altro messaggio dovrebbe decifrare un'altra chiave di sessione

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **Una funzione hash è una funzione da molti a uno che mappa i suoi valori di ingresso in un valore appartenente ad un insieme finito**
  - **Es. f(x) = x mod 37, che mappa tutti gli x al resto della divisione tra x e 37.**
  - **La firma digitale di un documento è il risultato dell'applicazione di una funzione hash al documento stesso**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **funzione hash deve soddisfare a due importanti proprietà**
  - **dev'essere difficile trovare due documenti che possiedono lo stesso valore di hash**
  - **dato un valore di hash deve essere difficile recuperare il documento che ha prodotto quel valore.**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **SHA e MD5 sono due algoritmi usati specificamente per firmare i documenti**
  - **la firma è il valore che si ottiene applicando la loro funzione di hash**
  - **un'altra persona può controllare la firma applicando la stessa funzione di hash alla propria copia del documento**
  - **se i due valori sono uguali si può essere praticamente certi che i documenti sono identici**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **Alcuni algoritmi a chiave pubblica (RSA)possono venire usati per firmare documenti**
  - **chi firma cripta il documento con la propria chiave privata**
  - **chi controlla la firma e vuol vedere il documento usa semplicemente la chiave pubblica del firmatario per decifrarlo**
  - **vengono soddisfatte le due proprietà richieste dalla funzione hash, ma è troppo lento per risultare utilizzabile**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **documento e firma spediti in chiaro**
    - **un malintenzionato potrebbe infatti modificare il documento e generare la corrispondente firma senza che il destinatario ne venga a conoscenza**
  - **solo il documento è cifrato**
    - **un malintenzionato potrebbe manomettere la firma e provocare un fallimento del controllo sulla firma**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **usare una cifratura a chiave pubblica ibrida per criptare sia la firma che il documento**
    - **sembra corretto, ma in effetti non ha senso**
    - **se tale algoritmo mettesse veramente al sicuro il documento, esso sarebbe anche al sicuro da eventuali manomissioni e non ci sarebbe bisogno di alcuna firma**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
  - **usare una cifratura a chiave pubblica ibrida per criptare firma e documento**
    - **solo la chiave di sessione per l'algoritmo simmetrico viene criptata usando la chiave privata del firmatario**
    - **chiunque è in grado di usare la chiave pubblica per recuperare la chiave di sessione**
    - **sarebbe banale recuperare tale chiave di sessione e criptare documenti modificati e firme da spedire in nome del mittente.**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
- **Soluzione: algoritmo a chiave pubblica per cifrare solo la firma**
  - il valore di hash viene criptato usando la chiave privata del firmatario
  - chiunque può controllare la firma usando la corrispondente chiave pubblica
  - il documento firmato può essere spedito usando qualsiasi altro algoritmo di cifratura, anche in chiaro se si tratta di un documento pubblico

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Firme digitali**
- **Soluzione: algoritmo a chiave pubblica per cifrare solo la firma**
  - se il documento venisse modificato, il controllo della firma fallirebbe
  - il controllo della firma serve a questo
  - il **Digital Signature Standard (DSA)** è un algoritmo per la firma a chiave pubblica che funziona come appena descritto
    - **è l'algoritmo principale usato da GnuPG per firmare** documenti.

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi**
- **manomissione delle chiavi**
- è una delle principali debolezze per quanto concerne la sicurezza della crittografia a chiave pubblica
  - uno spione potrebbe manomettere il mazzo di chiavi di un utente
  - creare la chiave pubblica di qualcuno e postarla affinché altri la scarichino e la utilizzino

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi**
- **manomissione delle chiavi**
  - **attacco man in the middle**
    - Chris crea una nuova coppia di chiavi pubblica/privata
    - rimpiazza la copia della chiave pubblica di Bob in possesso di Alice con la nuova chiave pubblica
    - intercetta i messaggi che Alice spedisce a Bob

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi**
- **manomissione delle chiavi**
  - **attacco man in the middle**
    - il messaggio intercettato
      - viene decriptato utilizzando la nuova chiave privata
      - recriptato usando la vera chiave pubblica di Bob
      - tale messaggio viene inviato a Bob

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi**
- chiave pubblica consiste
  - una parte della chiave di firma generale
  - una parte delle sottochiavi subordinate di firma e cifratura
  - un insieme di User ID utilizzati per associare una chiave pubblica ad una persona reale
  - Ogni componente contiene delle informazioni circa se stesso

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi**
- Per una chiave tali informazioni includono
  - l'ID della chiave
    - quando è stata creata
    - quando scadrà, etc
  - per uno User ID includono
    - il nome della persona reale che la identifica
    - un commento opzionale
    - un indirizzo di posta elettronica

Steganografia e crittografia

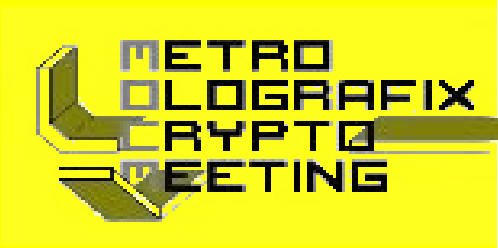
Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi**
- La struttura della chiave privata è simile, tranne per il fatto che essa contiene solo la parte privata delle chiavi e non ci sono informazioni sullo User ID
- L'opzione --edit-key può venir usata per visualizzare una coppia di chiavi

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi `--edit-key`**
- **La chiave pubblica viene visualizzata assieme alla disponibilità di una privata**
  - **informazioni per ogni componente della chiave pubblica**
    - **pub per chiave pubblica principale di firma**
    - **sub per chiave pubblica subordinata**
    - **la lunghezza della chiave in bit**
    - **il tipo D DSA, G ELGamal cifra e firma, g solo cifratura; l'ID**
    - **Le date di creazione e di scadenza**



Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Gestione delle chiavi `--edit-key`**
- **La chiave pubblica viene visualizzata assieme alla disponibilità di una privata**
  - Informazioni più dettagliate sulla chiave possono essere ottenute con comandi interattivi
  - **toggle** commuta fra le componenti pubbliche e quelle private della coppia di chiavi se queste sono effettivamente entrambi disponibili

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Integrità della chiave**
  - **Rischio sicurezza**
    - Distribuendo solo la propria chiave pubblica, si rendono note le componenti pubbliche della propria chiave principale e di quelle subordinate assieme allo User ID
    - è possibile per un malintenzionato manomettere la chiave
    - la chiave pubblica, infatti, può essere modificata aggiungendo o sostituendo altre chiavi, oppure aggiungendo o cambiando lo User ID

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Integrità della chiave**
  - **Rischio sicurezza**
    - Modificando l'UserID, un malintenzionato potrebbe cambiare l'indirizzo di posta elettronica dello User ID reale per fare in modo che arrivino al proprio indirizzo i messaggi dell'utente ignaro
    - Cambiando anche una delle chiavi di cifratura, il malintenzionato sarebbe perfino capace di decifrare i messaggi a lui reindirizzati.

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Integrità della chiave**
  - **Rischio sicurezza**
    - l'utilizzo della **firma digitale** rappresenta una **soluzione** a questo **problema**. Quando delle informazioni sono firmate con una chiave privata, la corrispondente chiave pubblica è legata alle informazioni firmate
    - solo la corrispondente chiave pubblica può essere usata per verificare la firma e assicurare che quelle informazioni non siano state modificate.

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Integrità della chiave**
  - **Rischio sicurezza**
    - Una chiave pubblica può essere protetta contro la manomissione
      - utilizzando la corrispondente chiave privata principale per **firmare le componenti della chiave pubblica e lo User ID**
      - Si legano così tali componenti alla chiave pubblica principale
      - tale operazione prende il nome di **autofirma**
      - la **chiave pubblica legata agli User ID autofirmati** prende il nome di **certificato**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Convalidare le altre chiavi del proprio mazzo**
- la chiave di un corrispondente è convalidata controllando personalmente l'impronta digitale della chiave e quindi firmando la sua chiave pubblica con la propria chiave privata
- Controllando personalmente l'impronta digitale si può essere certi che la chiave appartiene realmente a quella persona e, poiché la chiave viene poi firmata, si può essere sicuri di riuscire a rilevare ogni tentativo di manomissione futuro
- Sfortunatamente questa procedura risulta antipatica quando, per qualche motivo, si debba convalidare un gran numero di chiavi o comunicare con persone che non si conoscono direttamente.

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Convalidare le altre chiavi del proprio mazzo**
- GnuPG risolve questo problema con un meccanismo comunemente conosciuto come rete della fiducia
- In tale modello la responsabilità di convalidare le chiavi pubbliche è delegata a persone di cui ci si fida quindi in pratica la fiducia è soggettiva
- Ad es se la chiave di Bob è valida per Alice in quanto è stata lei a firmarla
  - Alice potrebbe non fidarsi di Bob e della sua capacità di convalidare propriamente le chiavi che egli firma
  - Alice potrebbe non considerare valide le chiavi di Chris e Dan basandosi solo sulle firme di Bob

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Convalidare le altre chiavi del proprio mazzo**
- **GnuPG rete della fiducia**
  - associa ad ogni chiave pubblica presente nel proprio mazzo un'indicazione di quanto ci si fidi del possessore di quella chiave
  - Ci sono quattro livelli di fiducia
    - sconosciuto (nessuna informazione sul giudizio del possessore nella chiave di firma)
      - le chiavi del proprio mazzo che non siano le proprie partono così
    - Nessuna (si sa che il possessore non firma opportunamente le chiavi degli altri)

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Convalidare le altre chiavi del proprio mazzo**
- **GnuPG rete della fiducia**
  - marginale (il possessore capisce le implicazioni che comporta firmare una chiave ed è capace di convalidare le chiavi propriamente prima di firmarle)
  - Piena (il possessore ha un'eccellente comprensione di ciò che comporta firmare una chiave e la sua firma su una chiave è tanto valida quanto la propria)

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Convalidare le altre chiavi del proprio mazzo**
- **GnuPG rete della fiducia**
  - Un livello di fiducia per la chiave è qualcosa che si assegna da soli alla chiave ed è considerata un'informazione privata
    - non viene inclusa con la chiave quando questa è esportata
    - viene perfino salvata separatamente dal proprio mazzo di chiavi in un elenco a sé stante
  - **comando trust** nell'editor delle chiavi di GnuPG (--edit-key) usato per impostare la fiducia che si possiede verso il possessore di una chiave

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Convalidare le altre chiavi del proprio mazzo**
- **GnuPG rete della fiducia**
  - permette di usare un algoritmo più elaborato per convalidare una chiave
    - in precedenza solo se era stata firmata di persona
    - ora se soddisfa due condizioni:
      - è firmata da un numero sufficiente di chiavi valide cioè (valori di default in GPG):
        - è stata firmata di persona
        - è stata firmata da una chiave di cui ci si fida pienamente
        - è stata firmata da 3 chiavi con fiducia marginale
      - il percorso delle chiavi firmate che risale fino alla propria chiave è al massimo di 5 passi.

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Distribuire le chiavi**
- in teoria la propria chiave viene distribuita dandola di persona al proprio corrispondente
- in pratica per posta elettronica o qualche altro mezzo di comunicazione elettronico
  - Ok se si hanno solo pochi corrispondenti
  - numerosi corrispondenti si può pubblicare nella homepage del proprio sito
    - inaccettabile se le persone che hanno bisogno di quella chiave non sanno dove trovarla

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Distribuire le chiavi (server di chiavi)**
- raccolgono e distribuiscono chiavi pubbliche
- quando richiesta, il server consulta il suo database e restituisce la chiave pubblica cercata se trovata
- prezioso anche quando molte persone firmano in continuazione chiavi di altri
- Senza dopo che Bob ha firmato la chiave di Alice dovrebbe spedire una copia della chiave pubblica di Alice ad Alice stessa, cosicché Alice possa aggiornare il proprio mazzo di chiavi e distribuire la sua nuova copia a tutti i suoi corrispondenti
- è responsabilità di Alice e di Bob verso la comunità intera mantenere una stretta rete di fiducia e migliorare così la sicurezza di GnuPG

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Distribuire le chiavi (server di chiavi)**
- Diventa pesante se la firma di chiavi avviene con frequenza
- il processo diventa più semplice
  - Bob firma la chiave di Alice
  - la invia al server di chiavi
  - il server aggiunge la firma di Bob alla copia della chiave di Alice in suo possesso
  - le persone interessate recuperano la copia aggiornata della chiave di Alice dal server

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Distribuire le chiavi (server di chiavi)**
- Si usa l'opzione a linea di comando --send-keys
- richiede uno o più specificatori di chiave
- le chiavi indicate vengono spedite al server di chiavi
- il server al quale inviare le chiavi è specificato con l'opzione --keyserver
- l'opzione --recv-keys viene usata per ottenere delle chiavi da un server
  - richiede che venga specificato un ID di chiave
- **gpg --keyserver certserver.pgp.com --send-key bob@tin.it**
- Ci sono diversi server di chiavi. I principali si sincronizzano a vicenda

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Definire i propri requisiti di sicurezza**
- GnuPG è uno strumento per proteggere la propria privacy
- la propria privacy è protetta se è possibile corrispondere con altri senza che nessuno possa intromettersi e leggere i nostri messaggi
- Il modo in cui usare GnuPG dipende dalla determinazione e dalla ricchezza di risorse di chi vuole leggere i nostri messaggi criptati

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Definire i propri requisiti di sicurezza**
- Un ficcanaso può essere
  - un amministratore di sistema senza scrupoli che legge a caso la posta altrui
  - una spia che sta provando a rubare i segreti del successo della nostra scuola
  - un'agenzia per il rispetto della legge che cerca di accusarvi
  - **l'obiettivo, in ultima analisi, consiste nel rendere più costoso il recupero dei dati non criptati di quanto valgano i dati stessi.**

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Definire i propri requisiti di sicurezza**
- La personalizzazione del proprio uso di GnuPG orbita attorno a quattro punti:
  - la scelta della dimensione della chiave della propria coppia di chiavi pubblica/privata
  - la protezione della propria chiave privata
  - la scelta delle date di scadenza e dell'uso di sottochiavi
  - la gestione della propria rete della fiducia

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Definire i propri requisiti di sicurezza**
- una dimensione della chiave scelta bene protegge dagli attacchi a forza bruta
- proteggere la propria chiave privata evita che un malintenzionato possa usarla per decifrare messaggi criptati e firmare messaggi a nostro nome
- la corretta gestione della rete della fiducia evita che dei malintenzionati fingano di essere le persone con le quali usualmente si comunica
- così bilanciamo il lavoro extra dovuto all'uso di GnuPG con la privacy che esso offre

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Scegliere la dimensione della chiave**
- in OpenPGP una coppia di chiavi pubblica/privata possiede, normalmente, più di una chiave
  - al minimo possiede una chiave di firma principale e probabilmente una o più sotto-chiavi addizionali di cifratura
- utilizzando i parametri preimpostati per la generazione di chiavi con GnuPG, la chiave principale sarà di tipo DSA e le sotto-chiavi di tipo ElGamal

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Scegliere la dimensione della chiave**
- Lo standard DSA prevede chiavi fino a 1024 bit
  - non è particolarmente alto per cui si dovrebbero usare chiavi DSA da 1024 bit.
- Le chiavi ElGamal possono essere di qualsiasi dimensione
- GnuPG è un sistema a chiave pubblica ibrido
  - la chiave pubblica viene usata per criptare una chiave di sessione da 128 bit
  - la chiave privata è usata per decriptarla

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Scegliere la dimensione della chiave**
- GnuPG è un sistema a chiave pubblica ibrido
  - la dimensione della chiave influenza la velocità di cifratura e decifratura in quanto il costo di questi algoritmi cresce esponenzialmente con il crescere della dimensione della chiave
  - chiavi grandi richiedono
    - più tempo ad essere generate
    - più spazio per essere salvate
    - raccomandata 1024 bit(oltre occorre un esperto in sicurezza dati e attenti alle rapine!!!)

Steganografia e crittografia

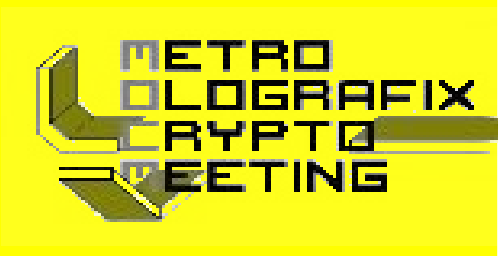
Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Proteggere la propria chiave privata**
- lavoro più importante che si deve considerare quando si vuole utilizzare GnuPG correttamente
- Se si perde è un evento catastrofico
  - tutti i dati criptati con quella chiave privata possono essere decifrati
  - chi la trova può firmare a nostro nome
  - non sarà più possibile decriptare documenti cifrati personalmente in futuro o nel passato
  - non sarà più possibile fare alcuna firma

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Proteggere la propria chiave privata**
- riporre in un posto sicuro il certificato di revoca della propria chiave pubblica
- salvare una copia della propria chiave privata su un supporto protetto da scrittura
  - masterizzare un CD-ROM, riporlo nella cassetta di sicurezza della propria banca in busta sigillata
  - salvare il tutto su un dischetto e nasconderlo da qualche parte in casa propria
  - Dovrebbe durare tanto tempo quanto si prevede di utilizzare la chiave



Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Proteggere la propria chiave privata**
- GnuPG non salva su disco la chiave privata così com'è
- viene invece criptata utilizzando un algoritmo di cifratura simmetrico
- questo è il motivo per cui si necessita di una passphrase per poter accedere alla chiave
- ci sono due barriere che un malintenzionato deve superare per poter accedere alla vostra chiave privata: deve aver effettivamente accessso alla chiave e deve riuscire a superare la cifratura

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Proteggere la propria chiave privata**
- Una buona passphrase è assolutamente cruciale nell'uso di GnuPG
- qualsiasi malintenzionato che riesca a guadagnare l'accesso alla propria chiave privata deve oltrepassare la cifratura della chiave privata stessa

Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Proteggere la propria chiave privata**
- il motivo per cui si prova prima con la passphrase consiste nel fatto che la maggior parte delle persone sceglie una passphrase più facile da indovinare di una chiave casuale a 128 bit
- se la passphrase è una parola, è molto più economico provare tutte le parole presenti nei dizionari delle lingue del mondo
- anche se i caratteri della parola sono permutati è comunque più semplice provare con delle parole da dizionario a cui sono applicate delle regole di permutazione

Steganografia e crittografia

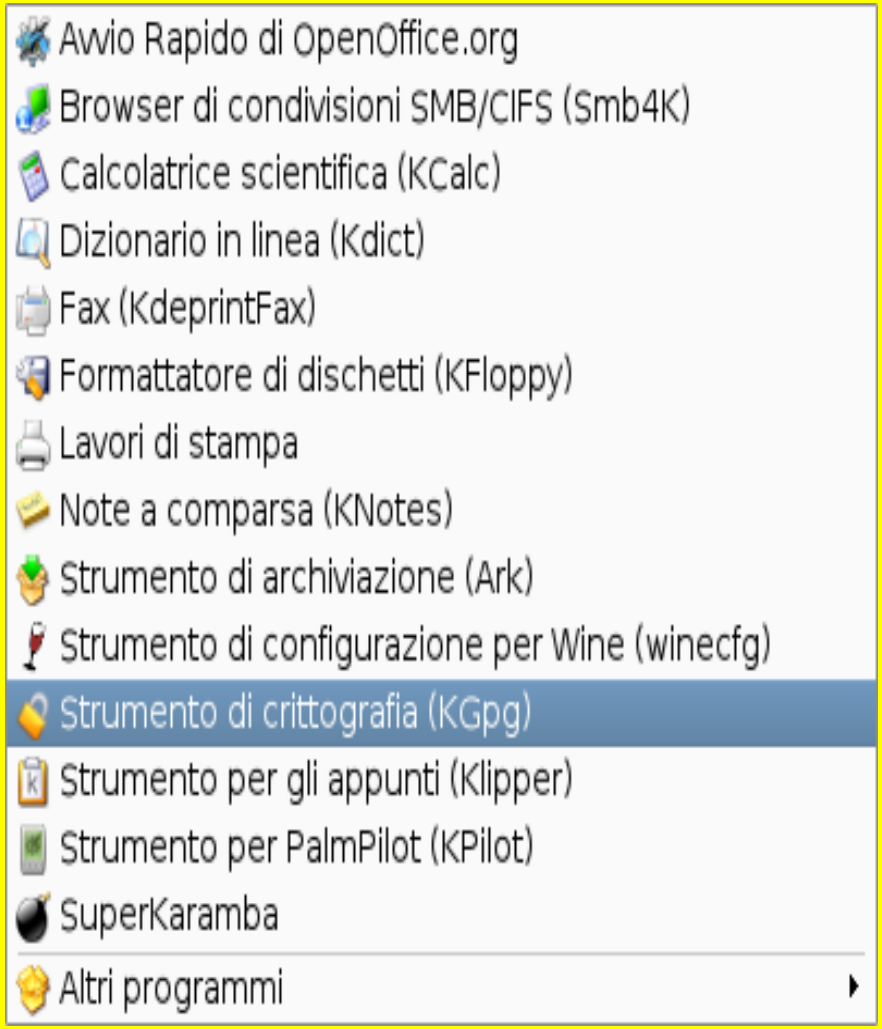
Crittografia e computer (GPG: riflessioni)

- **Uso quotidiano di GnuPG**
- **Proteggere la propria chiave privata**
- Lo stesso problema si applica a citazioni
- passphrase basate su frasi del linguaggio naturale sono esempi poveri, in quanto esiste poca casualità e molta ridondanza nel linguaggio naturale
- Una buona passphrase: le lettere iniziali di una canzone, poesia che si ricorda a memoria cambiando qualche lettera in numero, usando maiuscole e minuscole e caratteri speciali
- una buona scelta è importante per assicurare la propria privacy

Steganografia e crittografia

Crittografia e computer (KGPG)

- **Kgpg è una semplice interfaccia grafica per GnuPG**
- **non è necessario ricordarsi i comandi e le opzioni**
- Per lanciare Kgpg cliccare sul pulsante di avvio, menù accessori, Strumento di crittografia



Steganografia e crittografia

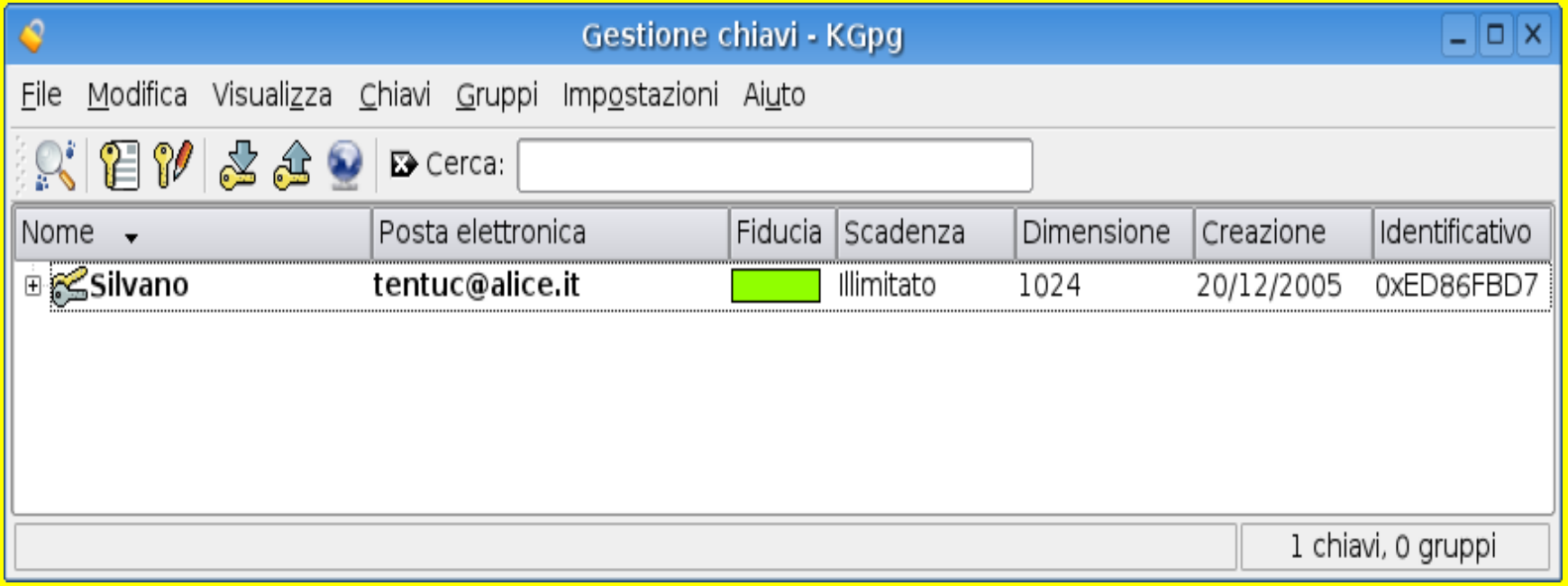
Crittografia e computer (KGPG)

- **all'avvio di Kgpg compare un'icona a forma di lucchetto sul pannello**

Steganografia e crittografia

Crittografia e computer (KGPG)

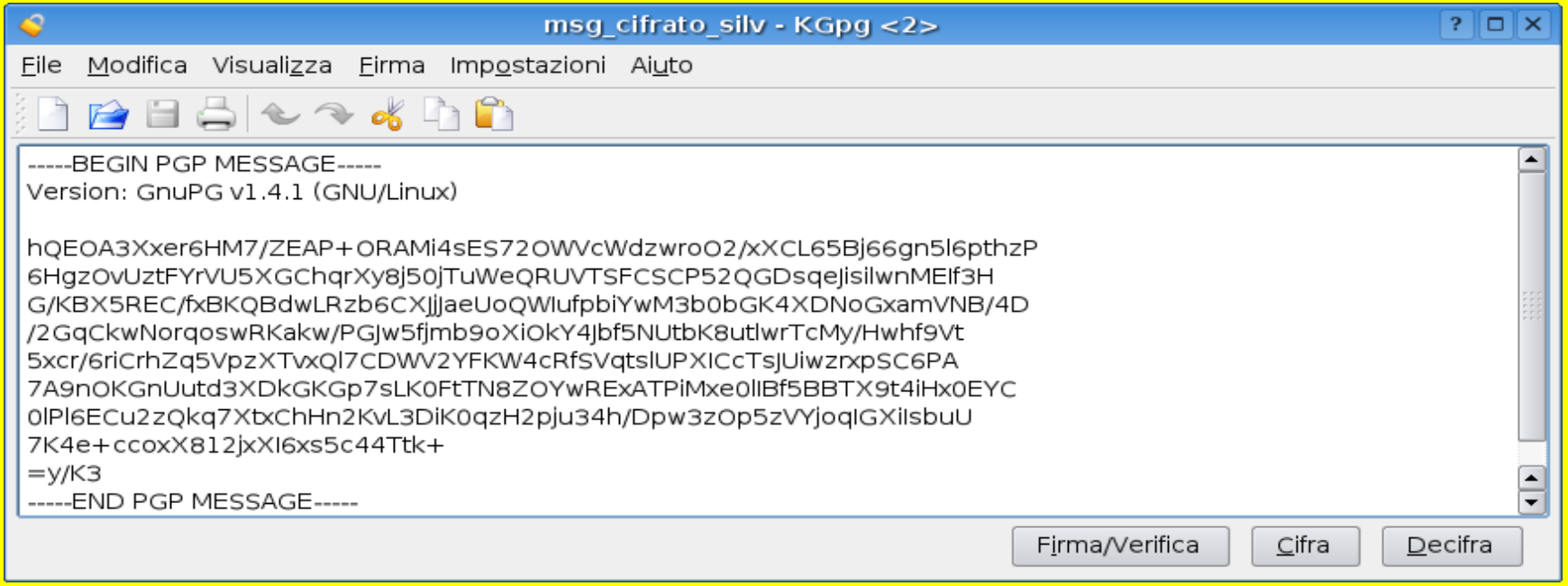
- **cliccando sul lucchetto appare la finestra di gestione delle chiavi (importare, esportare, firmare e modificare)**



Steganografia e crittografia

Crittografia e computer (KGPG)

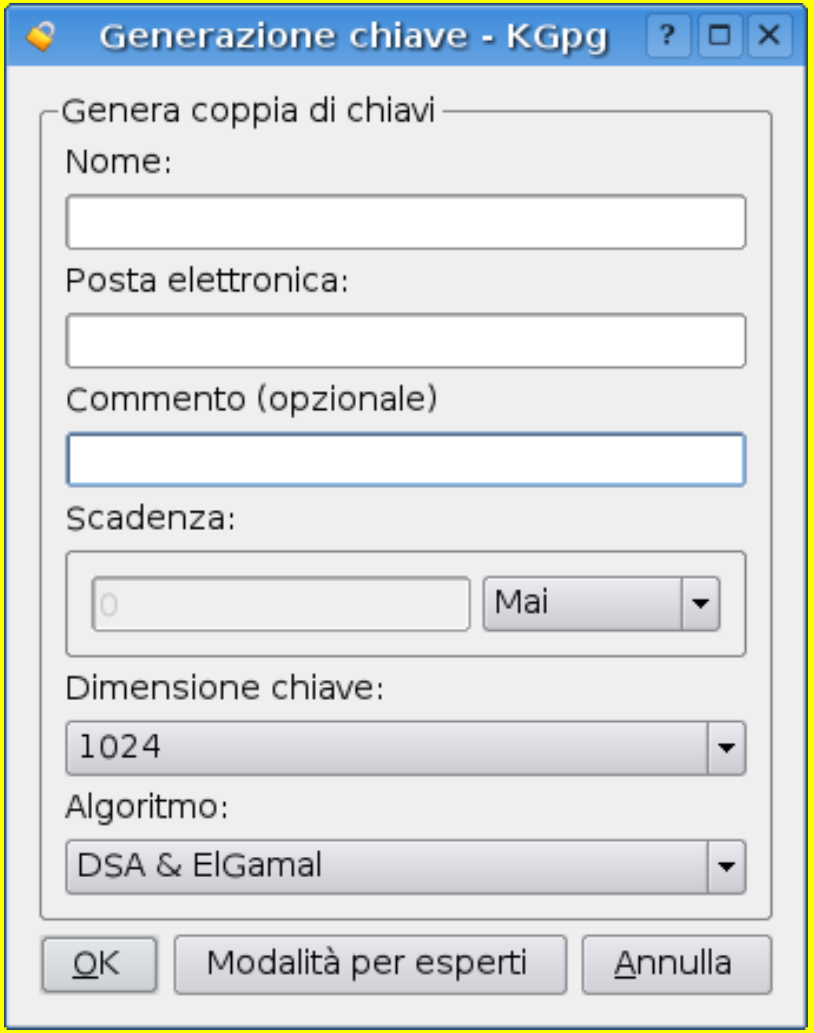
- **con un click destro invece si apre l'editor dove digitare o incollare il testo da cifrare o decifrare**

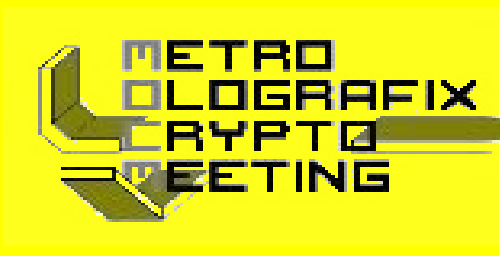


Steganografia e crittografia

Crittografia e computer (KGPG)

- **Generazione chiavi**
  - al primo avvio compare la finestra di dialogo per la generazione della prima chiave (anche dal Gestore delle Chiavi da Chiavi-> Genera coppia chiavi)





Steganografia e crittografia

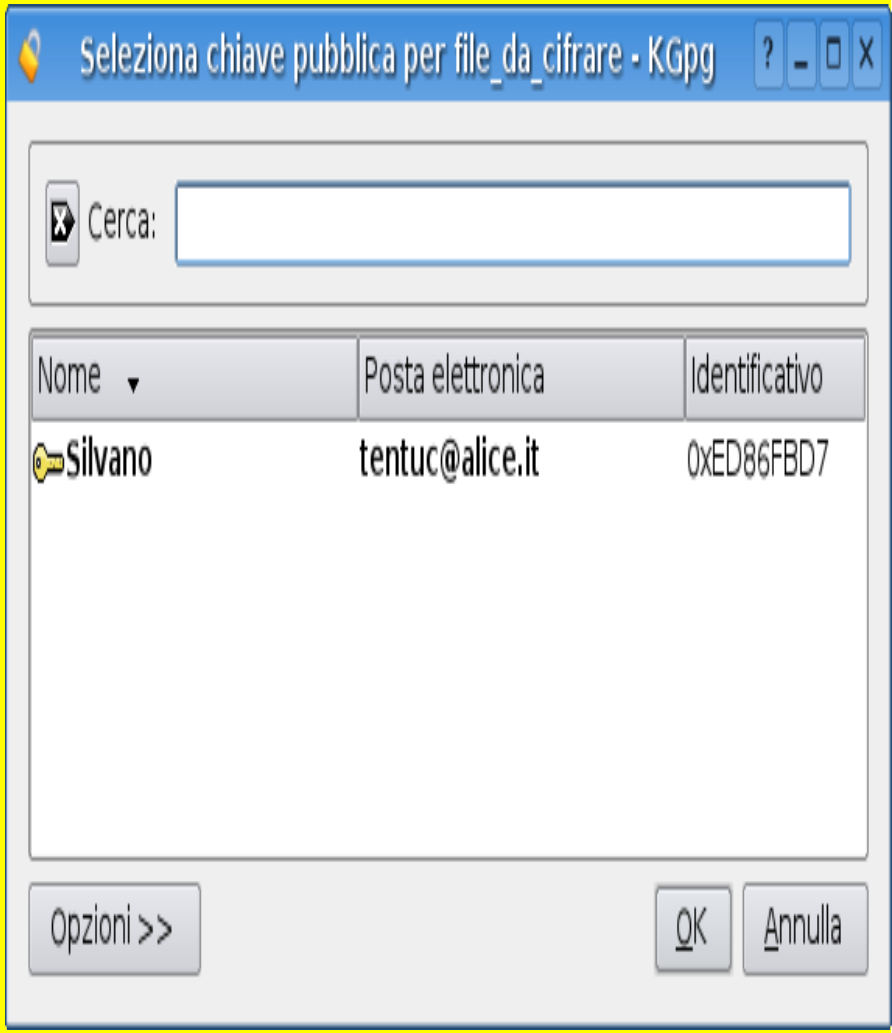
Crittografia e computer (KGPG)

- **Cifratura con Konqueror**
  - clic destro sul file da cifrare
  - Azioni->Cifra file > nel menù
  - Scegliere la chiave pubblica del destinatario nella finestra di dialogo delle Chiavi Pubbliche
  - clic su Cifra (file cifrato salvato con una estensione .asc o .gpg)

Steganografia e crittografia

Crittografia e computer (KGPG)

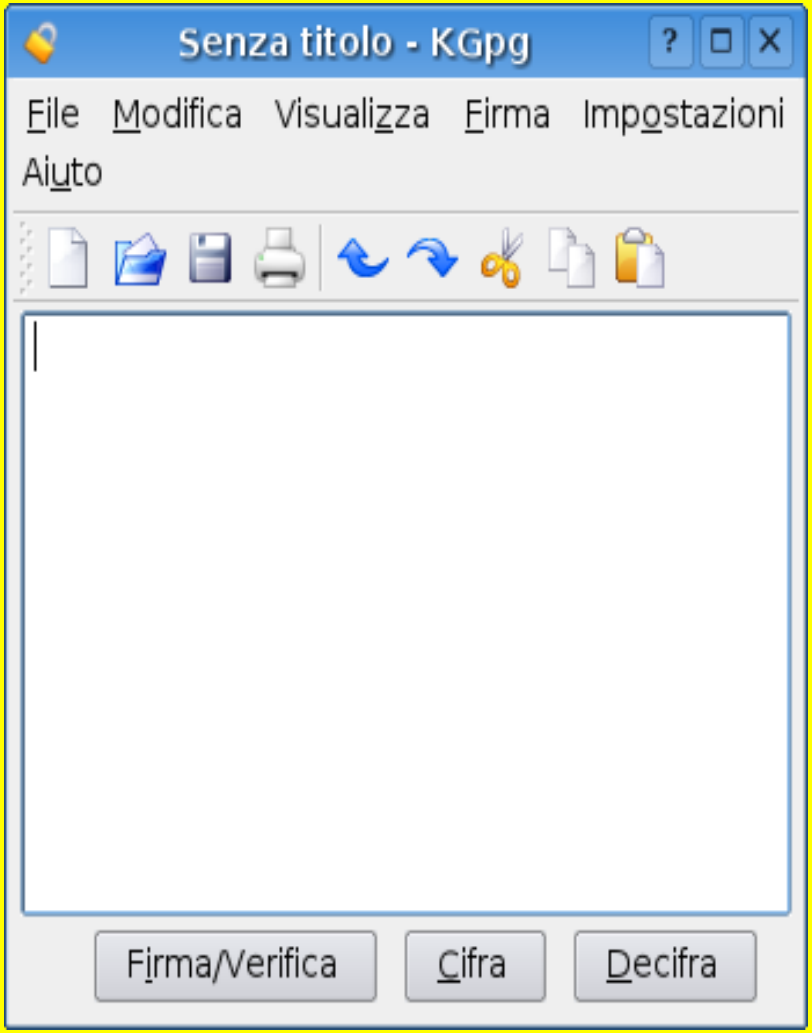
- **Cifrare un File o un Testo con l'applet di Kgpg**
  - Trascinare il file sull'applet nel pannello
  - se non cifrato si può scegliere la chiave pubblica.



Steganografia e crittografia

Crittografia e computer (KGPG)

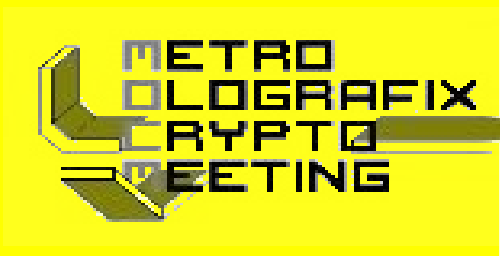
- **Cifrare testo dall'editor**
  - cliccare sul pulsante Cifra
  - scegliere la chiave pubblica
  - cliccare su Cifra
  - compare il messaggio cifrato



Steganografia e crittografia

Crittografia e computer (KGPG)

- **Decifrare un file da Konqueror**
  - cliccare sul file da decifrare
  - inserire la frase segreta
  - o trascinare un file di testo cifrato e lasciarlo nella finestra dell'editor di Kgpg (vi verrà decifrato)
    - anche con file remoti!
  - o File->Decifra File e scegliere un file da decifrare



Steganografia e crittografia

Crittografia e computer (KGPG)

- **Decifrare un testo nell'editor**
  - Copiare o trascinare e lasciare il testo che vuoi decifrare
  - cliccare sul pulsante Decifra
  - inserire la frase segreta

Steganografia e crittografia

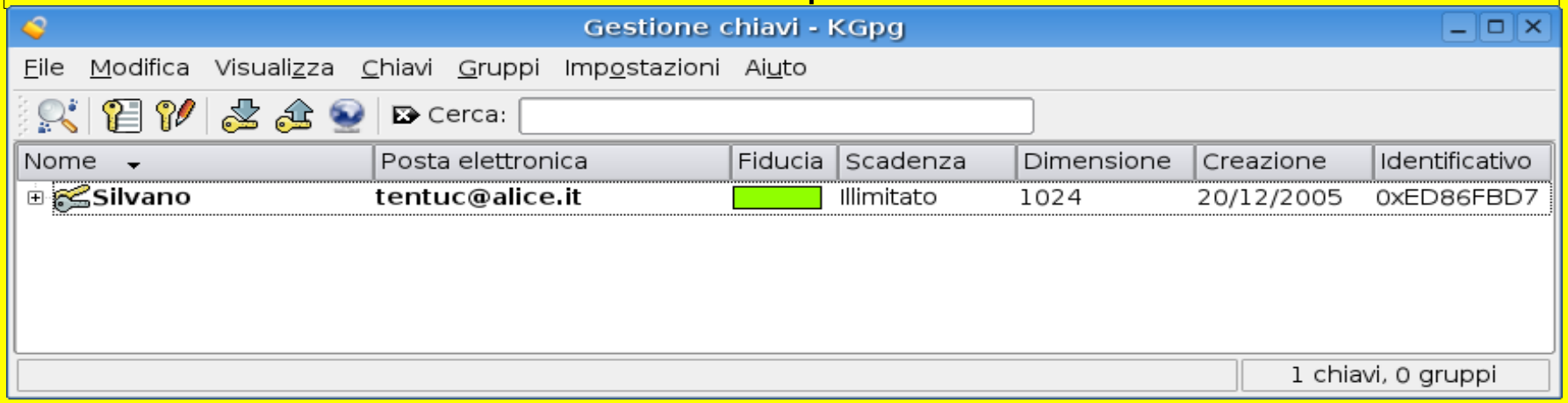
Crittografia e computer (KGPG)

- **Decifrare testo o un file con l'applet di Kgpg**
  - trascinare un file cifrato oppure il testo selezionato sull'applet di Kgpg nel vassoio di sistema
  - inserire la frase segreta, e il file/testo decifrato verranno salvati oppure aperti nell'editor di Kgpg
  - anche con decifra appunti del menù dell'applet di Kgpg

Steganografia e crittografia

Crittografia e computer (KGPG)

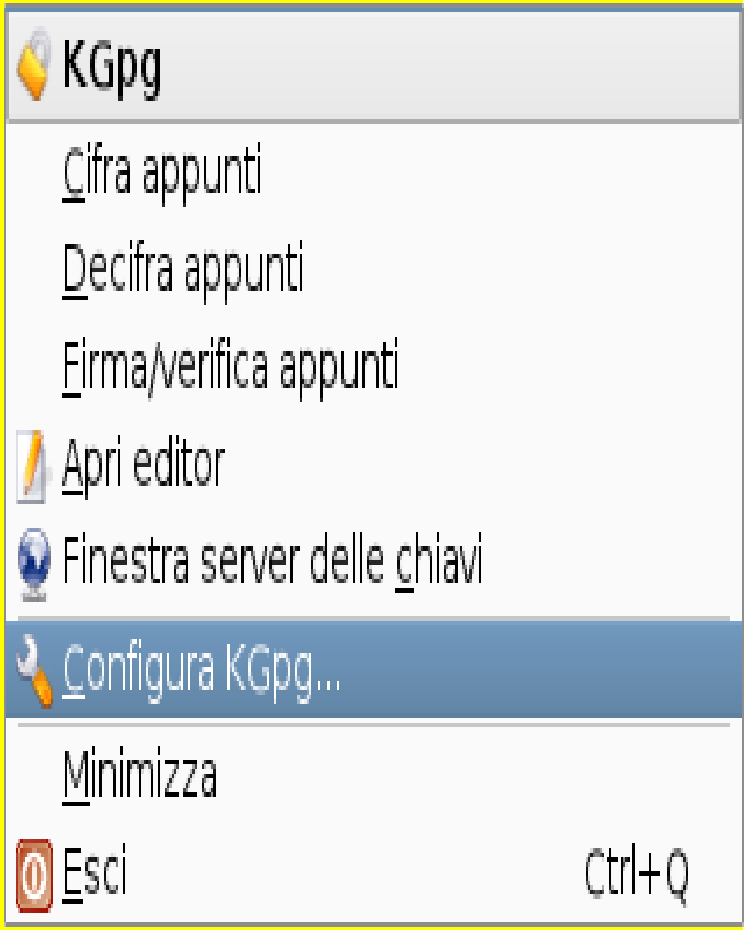
- **Gestione chiavi**
  - funzioni disponibili con clic destro sulla chiave
  - per importare/esportare le chiavi pubbliche
    - usare il trascinamento o
    - le scorciatoie di Copia/Incolla



Steganografia e crittografia

Crittografia e computer (KGPG)

- **Configurare Kgpg**
  - clic destro sull'applet
  - si possono impostare i parametri predefiniti per la cifratura, per la decifratura, per l'interfaccia utente e per l'applet.

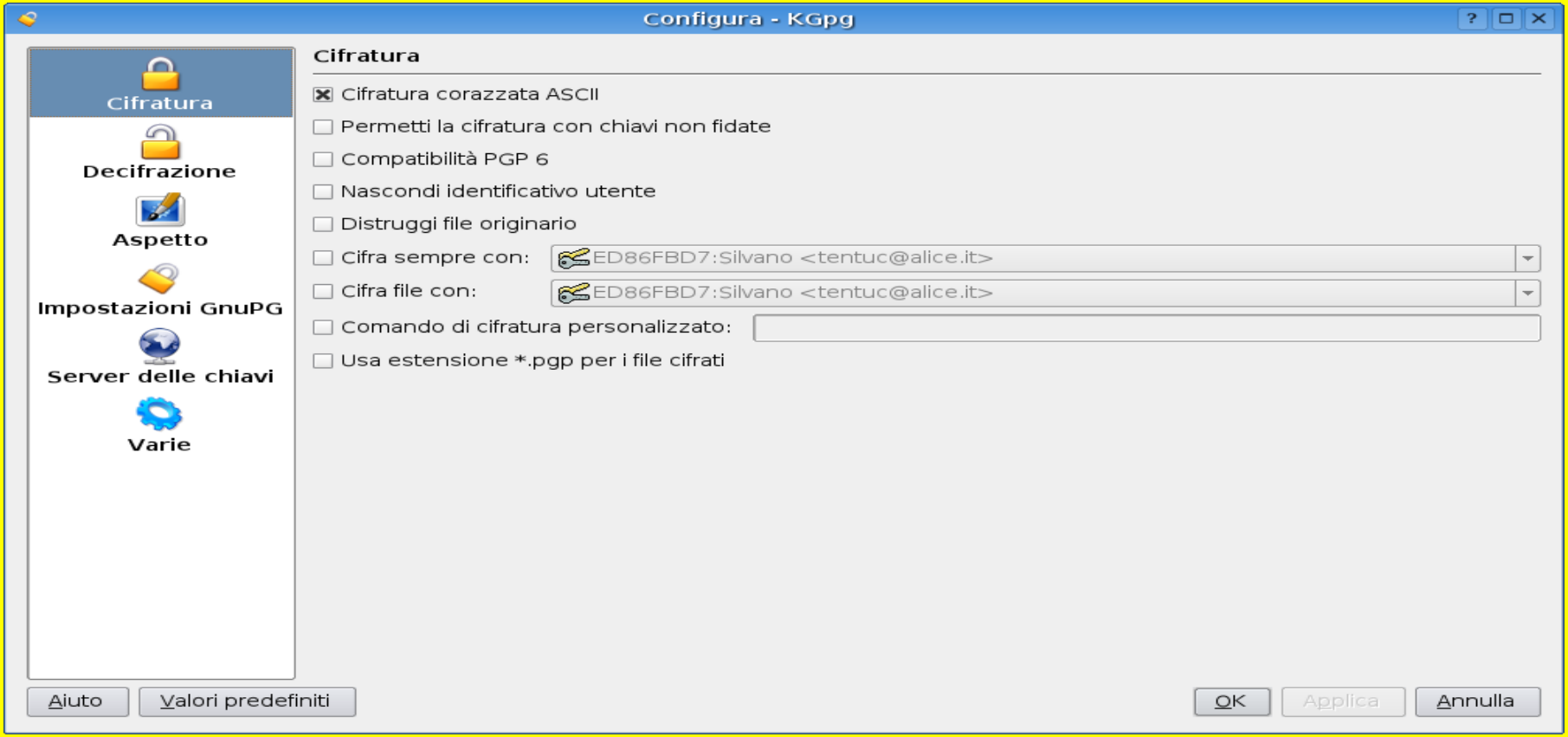


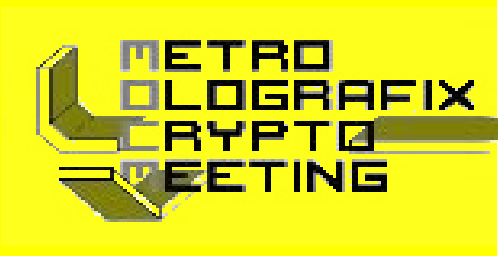
http://www.olografix.org
info@olografix.org
metro olografix
associazione culturale telematica

Steganografia e crittografia

Crittografia e computer (KGPG)

- **Configurare Kgpg**





Steganografia e crittografia

Crittografia e computer (GPG: riflessioni)

- **Uso legale di GnuPG**
- Bert-Japp Koops ha un'eccellente manuale di sopravvivenza alle leggi sulla crittografia

Fine!

Riferimenti bibliografici

- storia crittografia
- approfondimenti su RSA
- Approfondimenti su DES
- pagina principale GPG
- manuale Gnu sulla privacy

Gpg, Kgp, Kmail

Crittografia con sofware libero

http://www.olografix.org
info@olografix.org
metro olografix
associazione culturale telematica

Domande?