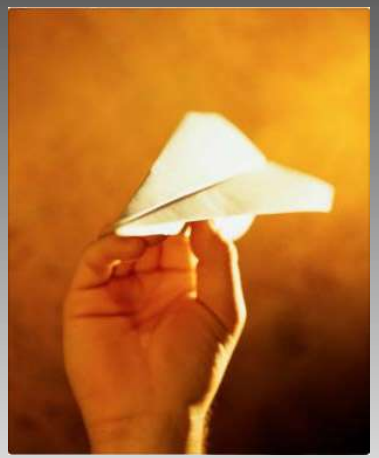
HACKMEETING 2007

GnuPG: concetti di crittografia

LFG

Mission

Introduzione al mondo della crittografia legata all'utilizzo della posta elettronica.



I modelli rimangono validi per qualsiasi altro tipo di fantasioso utilizzo della crittografia stessa.

GnuPG fa uso di diversi concetti di crittografia come **algoritmi simmetrici**, **algoritmi a chiave pubblica**, e **hashing**.

È possibile utilizzare le funzioni di base di GnuPG senza comprendere appieno tali concetti ma, se si vuole usarlo con cognizione di causa, una loro comprensione è necessaria.

Cercheremo di introdurre i **concetti alla base della crittografia utilizzati in GnuPG.**

HACKMEETING 2007

Presentazione

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)

hQQOA33lbTNCI3m2EA//cOMQri3uKxlDYEBw/ByygzIYtrA1SvOdUO1hqw2rs1rX
HYJeJ0RAtxABPDPW8PzNi6+HpG5V/PNb/mo89hrCmxqCB+Ezs9dhT/JUhkhGfzOa
diOHNmmoD3pwlcGphYfGYDUBpuev8gGOBp2qCrNAAev91m+kVAR/NJ4EnT7H8N7d
HFkdT+9lSG/pEDAbmpgq7KP2nocsgCZ62hxkOboi5gZVnOX1G/wz9+dpQniEZkW5
oFZP7z79VsffmPVkfi/E+1P6ffppn1t8sPOeHrBOpnvHGrOUgl1vhPMKaKpFWlxe
S6DS/qfbQoeWEzHUxWBz2lqFQT/kI1WyYVsBjNp0J6QODjFdzAh+uensNCJMnOpb
IHIAqHxiQ9s5/isdnXW1Dg3VnAFakAerCUQX287CAQnIRVPlWbdVqjf+FEioPtaD
S/MkeUWIRPalmyM6nhJ4QJKD85Ryrh5FZZ4PP/iGgFddkzZl4jfuw7hlllEaTatM
f8zZBtWkbXEWf3rpkN9kN8SZMNMlxL/znhncuVeJpt4tx1xFpzYHLhR8ZD1EeaR9
MWUER/Gz8h50ED/9PozgjE28wlS08SihbtToySNvy3opu6+vcy/KicKcc46/sB9P
YosDgNC3avfU83N2IOSl1E6YHXkZPPqKyi1QtCyGhSFZQRid4Ex9d5qdAenlid4P
/j3dSnf8eJWSst/RqvkEHKxI6xqrD+AmZnmR6yB1xkg/a5JYf16iZwTsF+mCPa6A
cQPWlBNIVAp1H0bZDkmlxJ9bVCka7yhxcO6DI9lXEQVlgcA5B6To0PUDOo7B5wuK
KoGRgA1NoTjNcL5YCdZm1b0nN5dLBv/jNva0zAKBQQPLdTp312HQQLU2yZk0Mv+P
3AnDmaXv2Oc3kxkJipD3ksxj2uNbSijzynBTHbgVK60njgEjKa0TWQ5MO77NR/Ri
9axqPWqg/8TJjMVq1lUoDmRDy7NMqpMLWeGon7TkIjWuj8TbLmdmkM1/7j08tE+L
CiE+ek1U9U53qmp1AuFK6QqL5lAiZWgK2XyW27w3eInEr7AyPKeRv22LKKCRj88X
K3z3pjADRKVzQvpTOObWChr/M0TlcF8hB+s4XL44MlFargwCR9Lc5CmQoTEd+v5a
JuqTwX7zz4tzT8V4xrVGH8N5GRIrAgp7wyr1GGP/3uZ1OfifFtiqMwQIdkTH7o7f
5+pEa2sOYAYNETpFhFL0jjgksdglfwrpd6avadj3DzMdv+URWvjOaSIr8hEeK8Va
rfviehdpGwXVOn/y7NXoxkamwJ+qB2izKeTv3WTzZjBLRKtDCNeuVhUdpRmqkEl9
/3uc/Sp/BATdwbRwOMF2gHjUUrUyRq27xSe7mLT9Oxff0l8BAn6b2/8xOpZ3TNUK
qRl91vaHU5OlZPhR0U6ehHqN67b/+ac/IG4cYWSqlnGgqzaUBNnC5XlTu3ywSfYR
OLPWObMoVyec8Sz2h9QYwYuHAo+NRap6+0GBgQ5czL29wQ==
=mRVO
-----END PGP MESSAGE-----
```

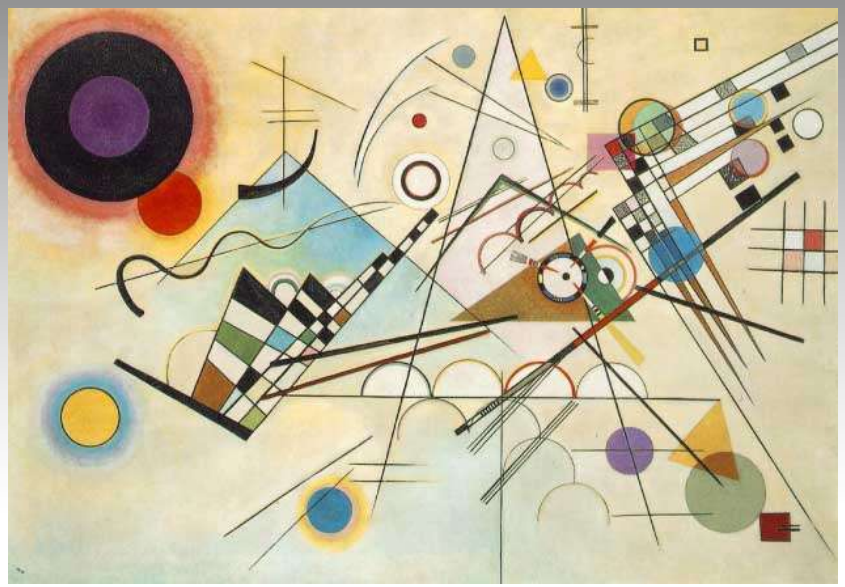
“La loro filosofia si chiama Open World e il loro obiettivo è distruggere i muri di protezione delle principali reti informatiche di tutto il mondo”
(Luca Panerai)

#C10771
member of AGOW and orgoglione to be.
-
Gian

LFG

prima domanda lecita:

cosa intendiamo per “crittografia”?



Wassily Kandinsky, Composizione VIII, 1923

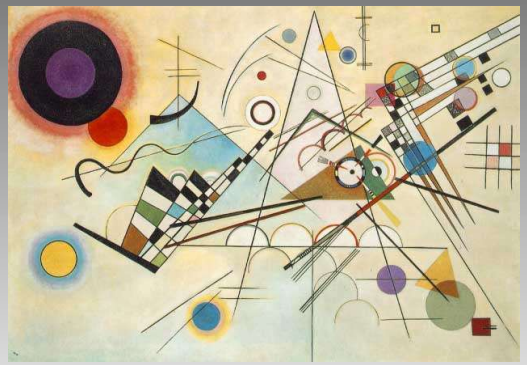
prima risposta lecita:

definizione etimologica corretta:

yn cnebyn “pevggbtensvn” qrevin qnyyn cnebyn terpn Xelcgóf pur fvtavsvpn anfpbfgb r qnyyn cnebyn terpn teácurva pur fvtavsvpn fpevirer.

Shannon -jj Behrens. gcipher 0.5, June 2003

confronto:



yn cnebyn “pevggbtensvn” qrevin qnyyn cnebyn terpn Xelcgóf pur fvtavsvpn anfpbfgb r qnyyn cnebyn terpn teácurva pur fvtavsvpn fpevirer.

ci servono delle basi più forti per non perderci...

HACKMEETING 2007

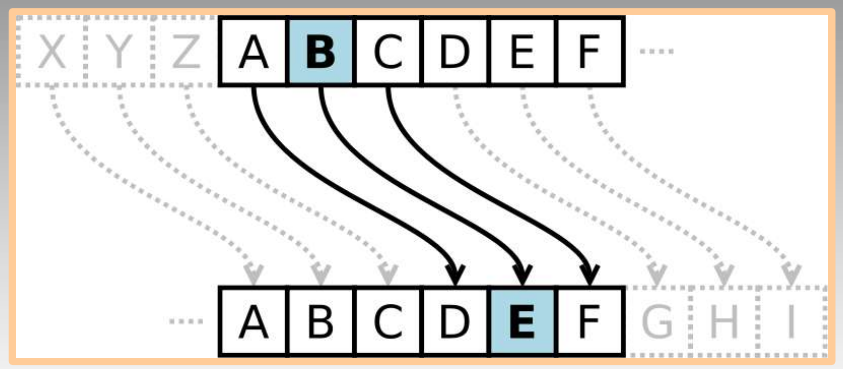
L'incomincio

Gaio Giulio Cesare, 100 a.C - 44 a.C
Precursore del diritto alla privacy
nella corrispondenza

LFG

cifrario di Cesare

Testo in chiaro	**a b c d e f g h i l m n o p q r s t u v z**
Testo cifrato	**D E F G H I L M N O P Q R S T U V Z A B C**



Esempio:

FHVDUH QH VDSHYD QD FLIUD

CESARE NE SAPEVA NA CIFRA

alcune definizioni...

alcune definizioni...

Testo in chiaro (cleartext) :

un dato che possiamo leggere e capire senza l'ausilio di nessun mezzo particolarmente speciale

Cifratura (encryption) :

un qualsiasi metodo che ci permette di nascondere un testo in chiaro modificandone la sostanza.

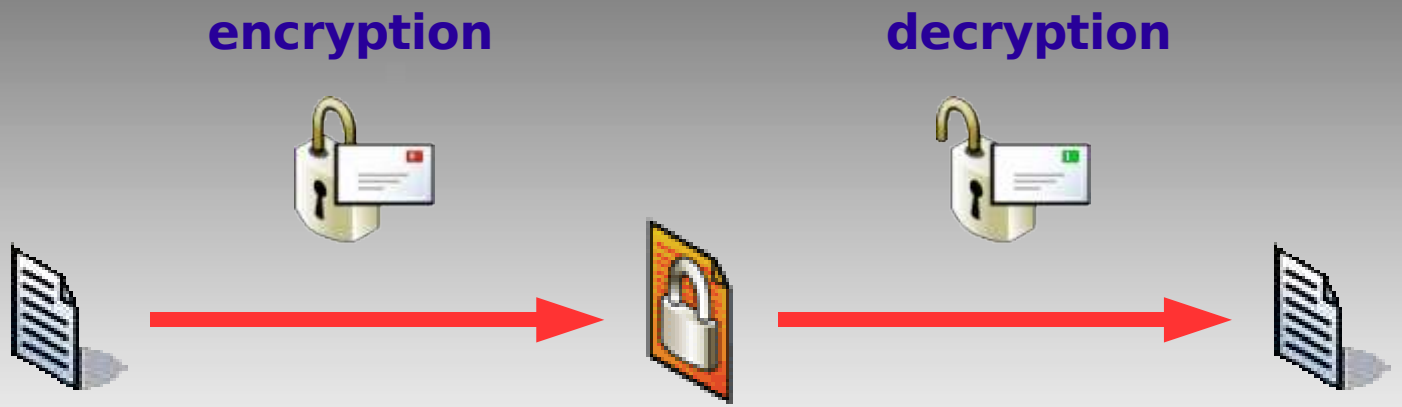
Testo cifrato (cypertext)

il naturale risultato, illeggibile, di una cifratura.

Decifratura (decryption) :

un qualsiasi metodo che ci permette di riottenere il testo in chiaro da un testo cifrato

descrizione del processo



seconda risposta lecita:

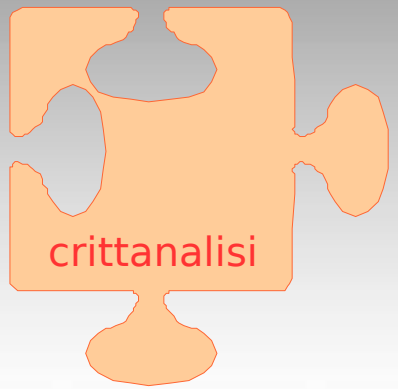
definizione intuitiva:

- la crittografia ci permette di salvare informazioni sensibili e di trasmetterle attraverso canali considerati insicuri (internet?) in modo che nessuno possa leggerle, eccezione fatta per i destinatari del messaggio.

- la crittografia è la scienza che utilizza la matematica per criptare e decriptare le informazioni.

buoni vs cattivi

VS

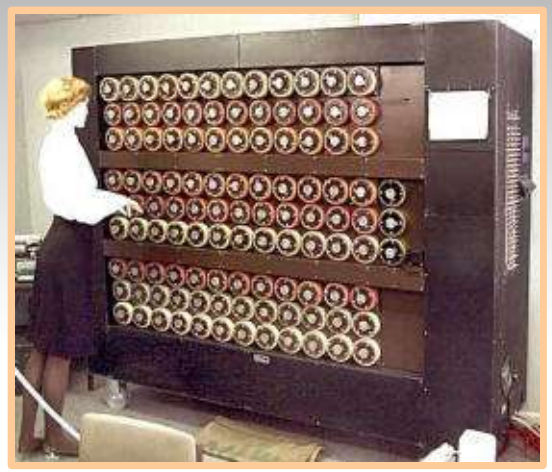


HACKMEETING 2007

crittografia

crittanalisi

VS



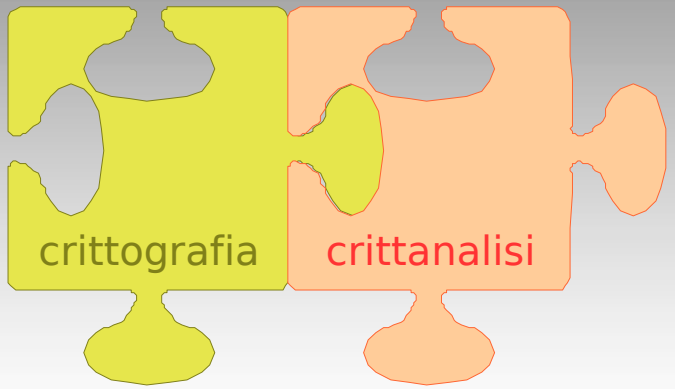
Enigma

Bomba

LFG

ancora definizioni...

crittologia (cryptology)



come funziona ?

un **algoritmo crittografico** (cipher) è una funzione matematica usata per i processi di codifica e decodifica.

un algoritmo crittografico lavora in combinaizone con una **chiave** (key) per cifrare e decifrare l'informazione.

la **sicurezza di un dato** cifrato dipende interamente da due fattori: la resistenza dell'algoritmo crittografico e la segretezza della chiave.

sicurezza

Un buon algoritmo di cifratura **racchiude completamente la sicurezza nella chiave senza lasciare nulla nell'algoritmo**. In altre parole, non dovrebbe essere di alcun aiuto per un malintenzionato conoscere il tipo di algoritmo utilizzato. Solo se ottenesse la chiave la conoscenza dell'algoritmo sarebbe necessaria.

L'algoritmo usato in GnuPG possiede tale proprietà.

Poiché tutta la sicurezza è riposta nella chiave, è importante che sia veramente difficile indovinare la chiave stessa. Detto altrimenti, **l'insieme di chiavi possibili, cioè lo spazio delle chiavi, deve essere grande**.

Crittanalisi: ridurre la dimensione dello spazio di chiavi

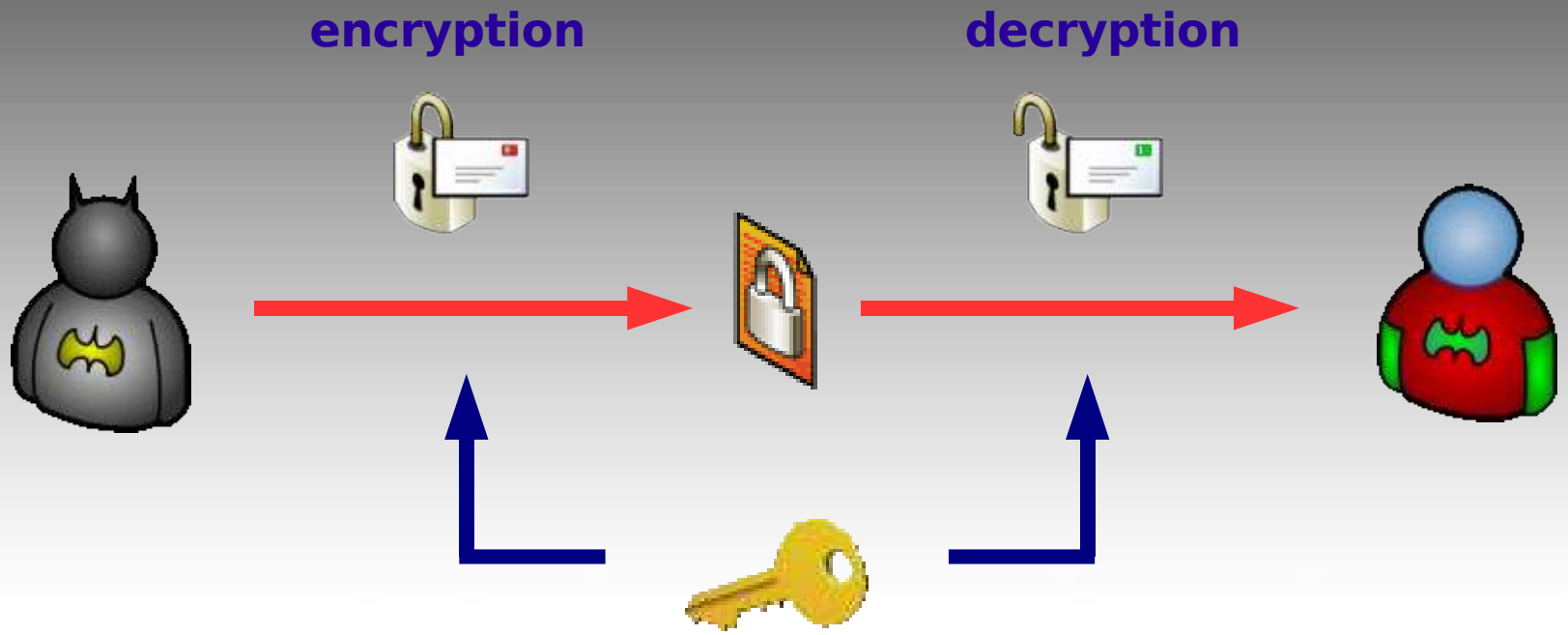
definizione...

L'algoritmo crittografico in combinazione con **tutte le possibili chiavi** e **protocolli** che ne permettono il funzionamento formano un

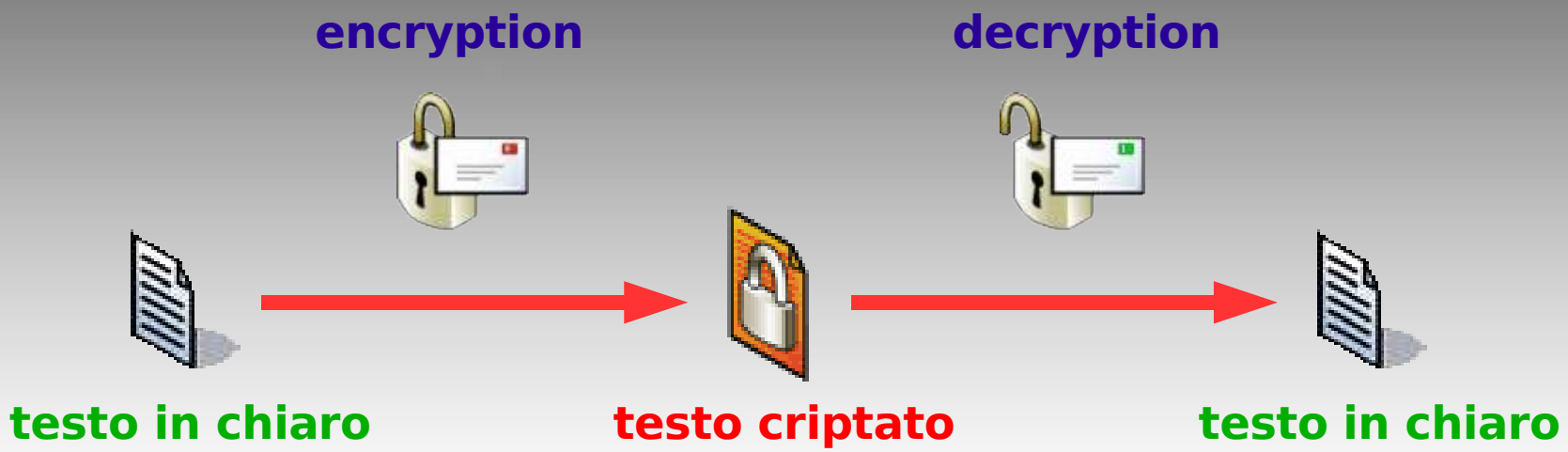
criptosistema
(cryptosystem)

PGP ne è un validissimo esempio!

Crittografia Convenzionale



conforme al modello descritto



Algoritmi Simmetrici

Cifrario di Cesare
algoritmo = shift
key = 3

ENIGMA

DES

3DES

Blowfish

IDEA

...

Prima risposta lecita - Shannon

```
# aptitude install gcipher


$ gcipher -C Rot -k 13
yn cnebyn “pevggbtensvn” qrevin qnyyn cnebyn terpn Xelcgóf pur
fvtavsvpn anfpbfgb r qnyyn cnebyn terpn teácurva pur fvtavsvpn
fpevirer.



la parola “crittografia” deriva dalla parola greca Kryptós che
significa nascosto e dalla parola greca gráphein che significa
scrivere.
```

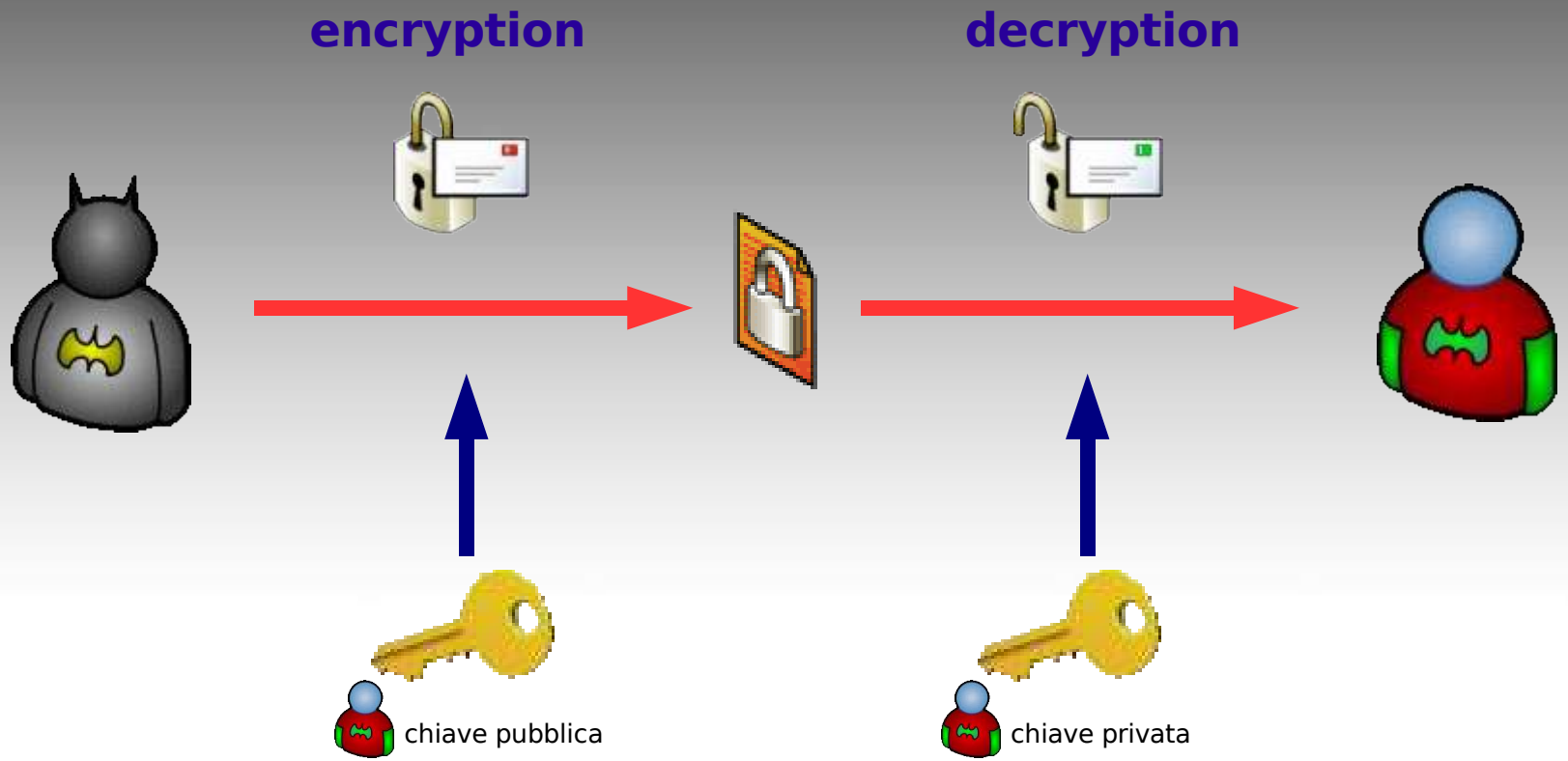
Algoritmi Simmetrici

sicurezza: spazio delle chiavi molto grande, algoritmi forti*.

scambio della chiave: intercettazione, sicurezza del canale.

chiavi necessarie: n persone che volgiono comunicare privatamente tra loro necessitano di **n(n-1)/2** chiavi per ogni coppia!

Crittografia a chiave pubblica



Algoritmi a chiave pubblica

scambio della chiave: risolto il problema!

chiavi necessarie: n persone che volgiono comunicare privatamente tra loro necessitano di n chiavi.

velocità: molto costosi!!

gli algoritmi a chiave pubblica non sono una panacea

Algoritmi Ibridi - GnuPG

Un algoritmo ibrido utilizza sia un sistema simmetrico che uno a chiave pubblica. In particolare esso funziona utilizzando un algoritmo a chiave pubblica per condividere una chiave per il sistema simmetrico. Il messaggio effettivo è quindi criptato usando tale chiave e successivamente spedito al destinatario.

Poiché il metodo di condivisione della chiave è sicuro, la chiave simmetrica utilizzata è differente per ogni messaggio spedito. Per questo viene detta a volte **chiave di sessione**.

Sia PGP che GnuPG usano algoritmi ibridi. 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.

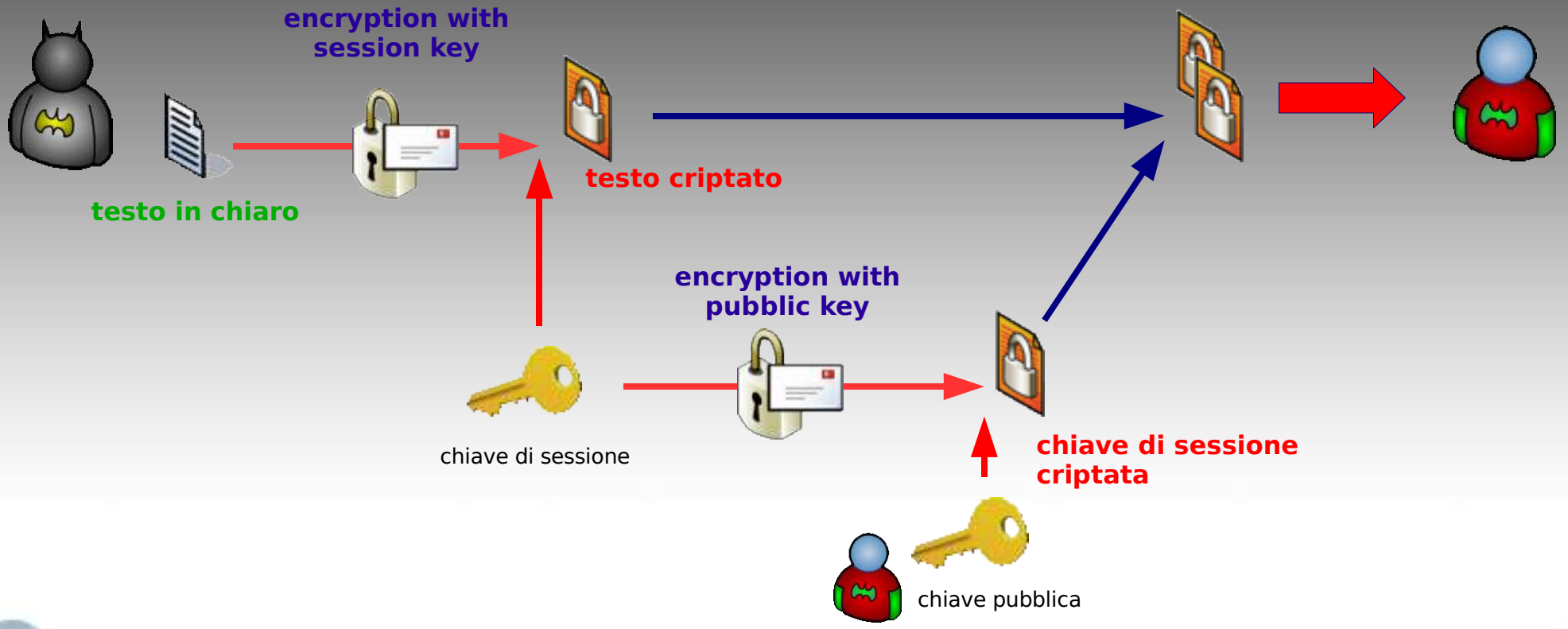
Algoritmi Ibridi - GnuPG

Un algoritmo ibrido non è mai più forte del più debole algoritmo utilizzato, sia esso quello a chiave pubblica o quello simmetrico.

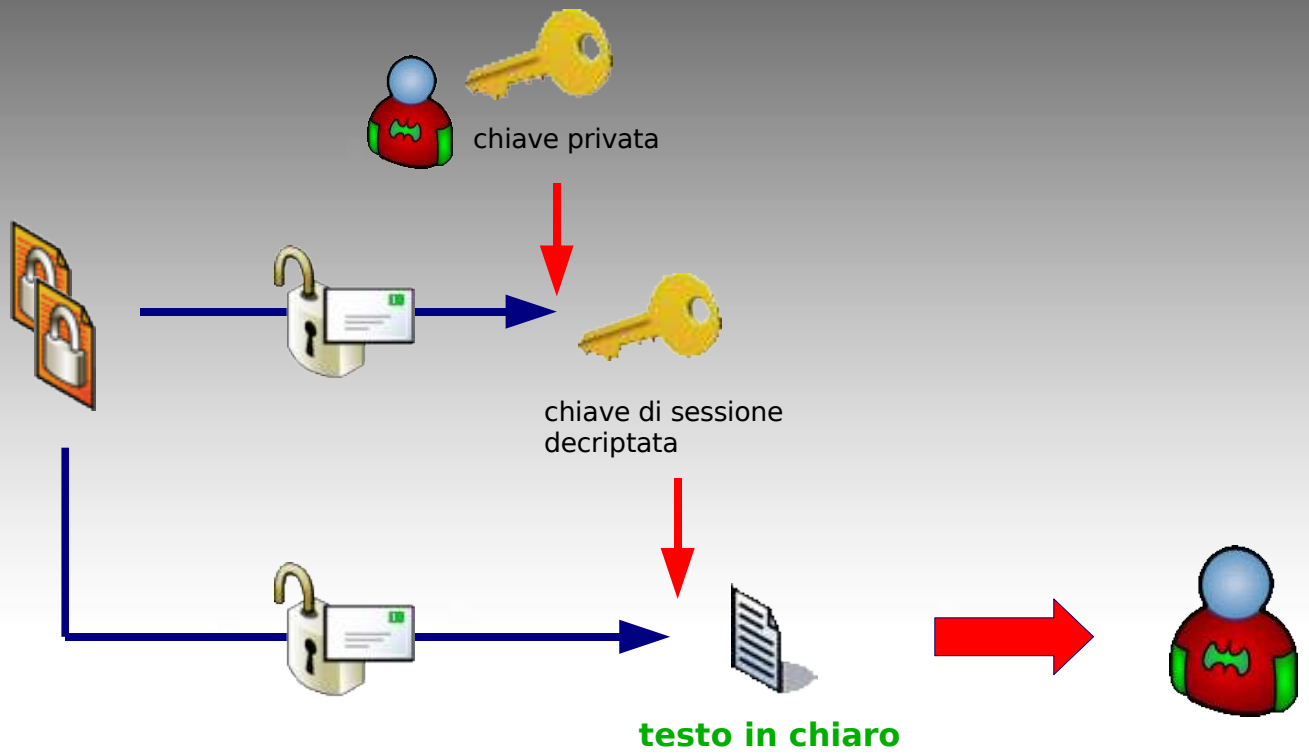
Se un malintenzionato dovesse decifrare una chiave di sessione, egli sarebbe in grado di leggere solo un messaggio, quello criptato con quella chiave di sessione. Il malintenzionato dovrebbe ricominciare di nuovo e decifrare un’altra chiave di sessione per poter leggere un altro messaggio.

La combinazione dei due modelli di encryption mette insieme la convenienza (e sicurezza) della public key con la velocità della crittografia convenzionale: quest'ultima è 1000 volte più veloce della public key encryption. Performance e distribuzioni delle chiavi sono implementate senza sacrificare sicurezza!

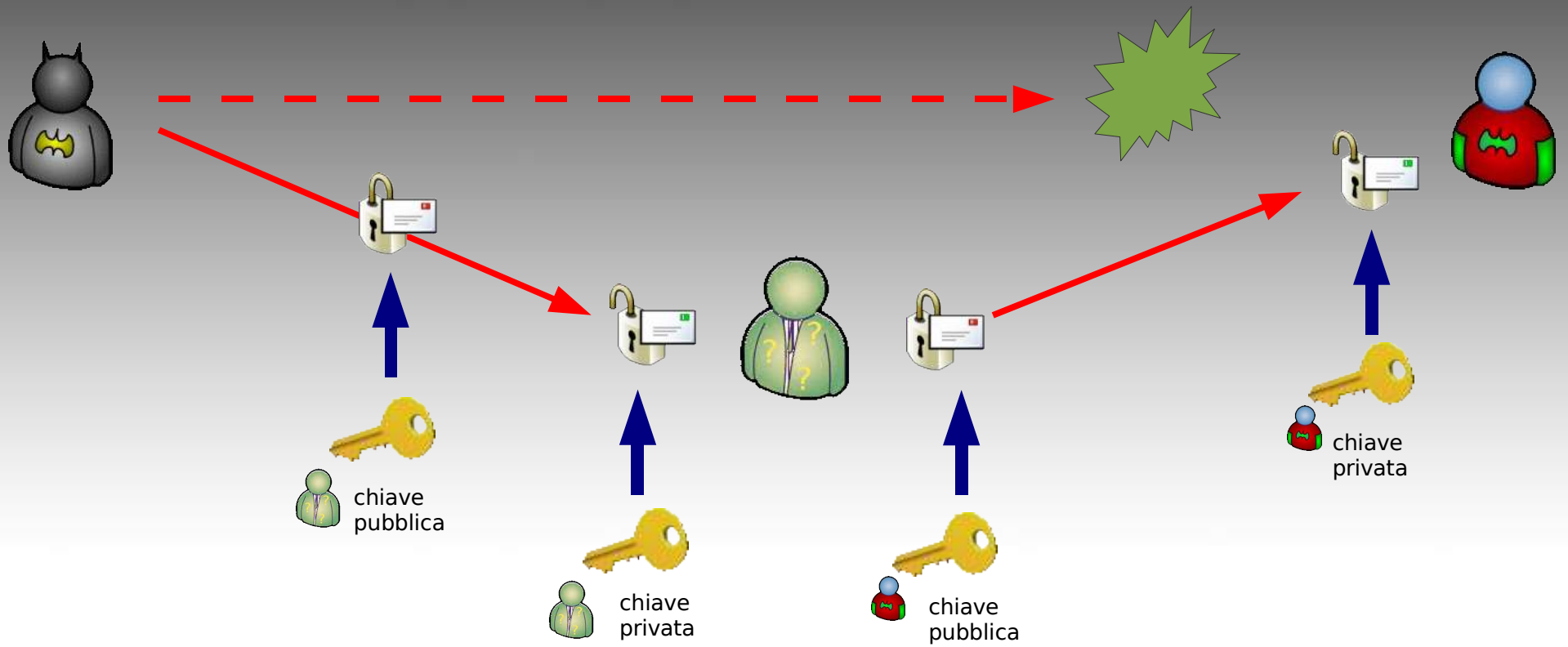
Algoritmi Ibridi - codifica:



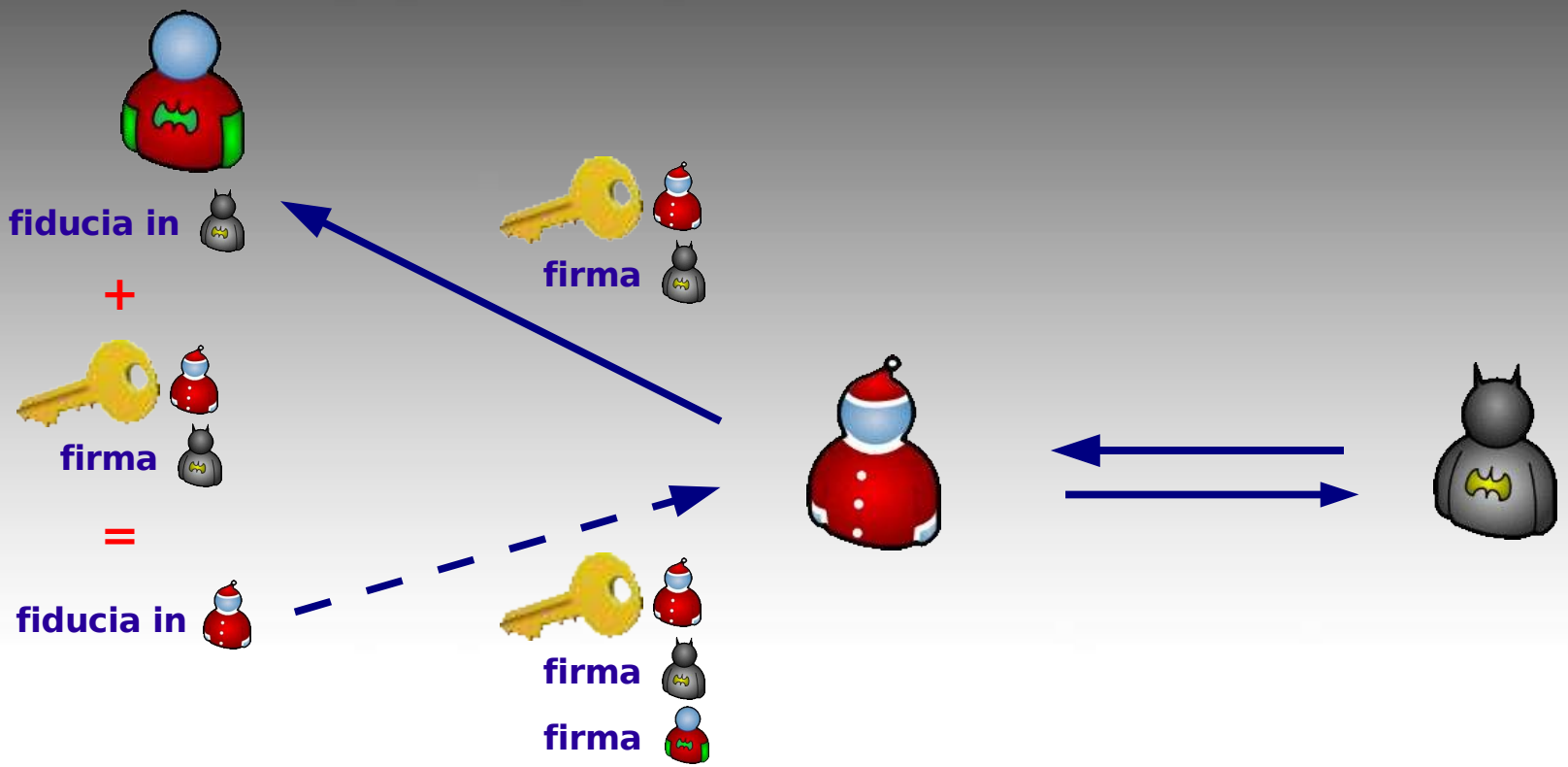
Algoritmi Ibridi - decodifica:



Fiducia e MITM



Rete della Fiducia



Livelli di Fiducia

sconosciuto : non c'è nessuna informazione sul giudizio del possessore nella chiave di firma. Le chiavi del proprio mazzo che non siano le proprie hanno inizialmente questo livello di fiducia.

nessuna : si sa che il possessore non firma opportunamente le chiavi degli altri.

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.

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.

domande ?

“Ma se un HUB e uno Switch si incontrano, possono essere amici?”
Lapo