



Deniable Encryption

- 1) siete degli orsetti
- 2) venite trovati con le mani nella marmellata
- 3) l'inquisitore vi chiede perché...
- 4) *avete una storia plausibile!*
- 5) ...
- 6) **profit!**



*Gloria, gloria,
gloria all'ipnorospo.*



Deniable Encryption

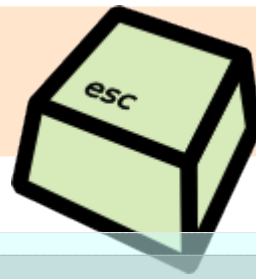
La D.E. vuole risolvere un problema che non è prettamente matematico,

Vuole, usando la crittografia, risolvere un problema che richiede necessariamente un umano attivo tra i nostri avversari.



*Gloria, gloria,
gloria all'ipnorospo.*

PERCHE' INTERESSARSENE ?



2007: Inghilterra rende attiva la terza parte del RIPA

RAW: due anni di detenzione se non riveli una password !?

(approvata per finalità antiterroristiche, è stata usata in processi contro animal right activist ...)

2007: USA reparto immigrazione

può esserti richiesta la password per passare la frontiera USA !?

2007: Phrack: The only laws on Internet are assembly and RFCs

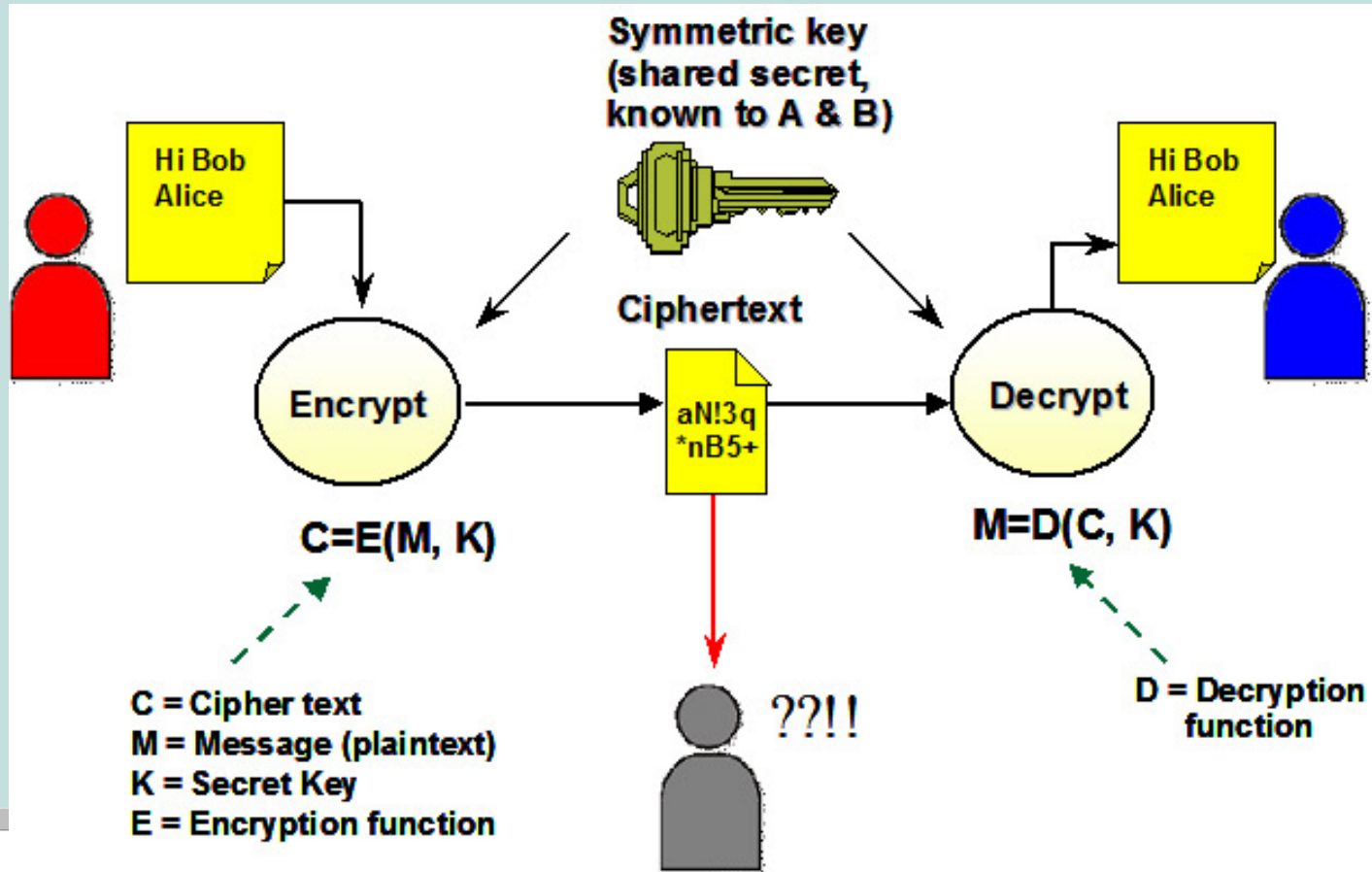
<http://www.phrack.org/issues.html?issue=65&id=6#article>



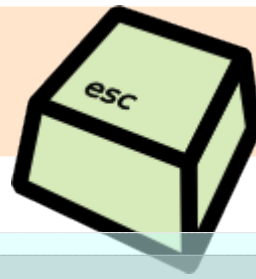
*Gloria, gloria,
gloria all'ipnorospo.*



quando si parla di crittografia, si usa parlare di “chiavi”.
sono i segreti, condivisi o meno tra le parti:



*Gloria, gloria,
gloria all'ipnorospo.*



La comune e intuitiva implementazione vede l'utilizzo di password, e la legge si è focalizzata su quello.

(spesso si tratta di password che proteggono chiavi di lunghezza ed entropia migliori)

ma chi lo dice che i software debbano continuare ad essere così ?
questa era un po' la teoria dell'articolo su phrack, che presentava il software **elettra**.



*Gloria, gloria,
gloria all'ipnorospo.*

Ma prima di parlar di elettra, contestualizziamo:



Qualunque strumento

(software, sociale, informativo)

che deve darvi una sensazione di sicurezza, deve essere valutato in relazione alla minaccia dalla quale volete proteggervi.

Modelli di minaccia:

1/Basso

Il vostro fidanzato vuol conoscere le vostre preferenze su youporn

2/Medio

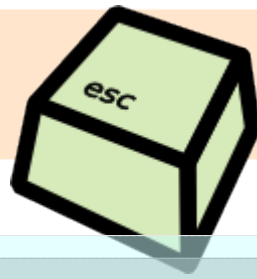
avete una spia alle calcagna che vuol scoprire la vostra ricetta dell'involtino primavera

3/Alto

Il mossad è incazzato con voi perché avete venduto plutonio ad un palestinese al parco



*Gloria, gloria,
gloria all'ipnorospo.*



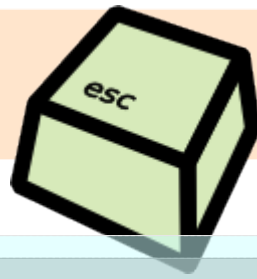
La deniable encryption
crittografia negabile ? (brrr)

E' l'interpretazione crittografica della negazione plausibile (plausible deniability): <http://en.wikipedia.org/wiki/Deniability>

Quest'interpretazione si applica, in crittografia, avendo differenti chiavi che possono decifrare un solo messaggio. A seconda della chiave fornita, un messaggio diverso sarà rivelato. Questo ha senso se, e solo se, la rivelazione (della chiave) ed il rilevamento del messaggio hanno senso (plausible deniability, must to be plausible)



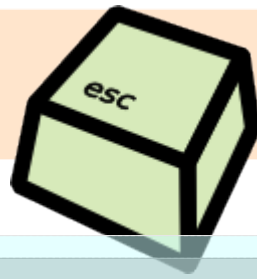
*Gloria, gloria,
gloria all'ipnorospo.*



- 1) **Alice** tradisce il marito **Bob** andando con **Vecna**, e **B** lo sospetta. **A** per comunicare in segreto con **V** genera 2 chiavi. Le da entrambe a **V**.
- 2) **A** scrive a **V** generando un messaggio crittato, composto così: noiose conversazioni algebriche cifrate con la chiave 1, messaggi amorosi cifrati con la chiave 2.
- 3) **V** possiede entrambe le chiavi, decifra entrambi i messaggi, risponde ad entrambi coerentemente e genera una risposta allo stesso modo del punto 2.
- 4) Quando **B** ha dubbi, interroga **A** riguardo lo scambio cifrato, **A** rivela la chiave 1, **B** legge dell'algebra e conclude che **V** è certamente un nerd asessuato. Torna a leggersi la gazzetta mente ignora che c'è una seconda chiave (e un palco di corna).
- 5) **A** e **V** = vissero cifrando felici e contenti.



*Gloria, gloria,
gloria all'ipnorospo.*



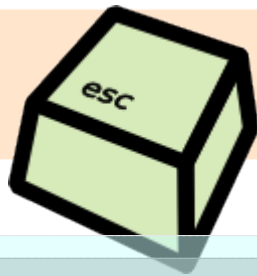
Dicitura noiosa:

Quest'interpretazione si applica, in crittografia, avendo differenti chiavi che possono decifrare un solo messaggio. A seconda della chiave fornita, un messaggio diverso sarà rivelato.

Questo ha senso se, e solo se, la rivelazione (della chiave) ed il rilevamento del messaggio hanno senso (*plausible deniability, must to be plausible*)



*Gloria, gloria,
gloria all'ipnorospo.*



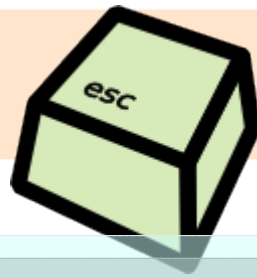
I software che più comunemente fanno deniable encryption (TrueCrypt e i suoi derivati-progenitori: FreeOFTE e BestCrypt)

Funzionano con il concetto di “*hidden volumes*”:

- . L'utente formatta una partizione con dati casuali
- . crea N volumi nascosti, ogni password ne sblocca uno
- . Ad un analisi passiva, ogni password è plausibile apra l'unico *hidden volume*, e che sia l'unico presente nella partizione in analisi.
- . all'analisi passiva, i dati cifrati devono apparire con le stesse proprietà dei dati random che occupano le parti non utilizzate del disco. http://en.wikipedia.org/wiki/Diehard_tests



*Gloria, gloria,
gloria all'ipnorospo.*

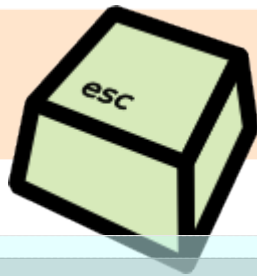


Lo stesso utilizzo della D.E., in questo momento storico, può suonare come un'anomalia!

Per questo motivo, alla richiesta di una password, è necessario ci sia qualcosa di estremamente plausibile!



*Gloria, gloria,
gloria all'ipnorospo.*



Ne consegue che, per essere plausibile, dovrebbe essere utilizzata sempre e comunque.

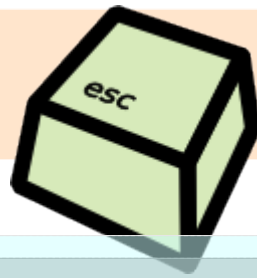
storia di CryptoKitchen: www.inventati.org/cryptokitchen/
ha senso che mi scambi email cifrate (con gnupg) solo quando devo dir qualcosa di sensibile ?

no, o l'avversario dedurrà, dal mio utilizzo di gpg, chi è un contatto da proteggere e chi non lo è.

Per questo motivo deve essere usata indiscriminatamente over possibile. CryptoKitchen era una mailing list cifrata per lo scambio di ricette di cucina.



*Gloria, gloria,
gloria all'ipnorospo.*

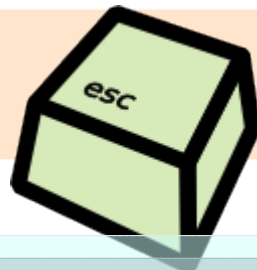


- 1) Se l'obiettivo è la riservatezza, la soluzione è la crittografia
- 2) Se l'obiettivo è l'occultamento plausibile in caso di richiesta forzata, la soluzione è la deniable encryption (a patto ci sia una plausibile risposta: quello dal quale ci si vuole difendere implica necessariamente un elemento umano)
vien anche detta: steganographic encryption
- 3) se l'obiettivo è l'occultamento e basta, la soluzione appropriata è la steganografia

ok, è ora di parlare di software :)



*Gloria, gloria,
gloria all'ipnorospo.*



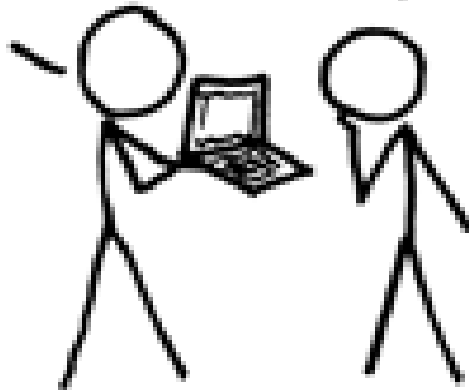
il primo fu *rubberhose filesystem*, voleva risolvere:

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

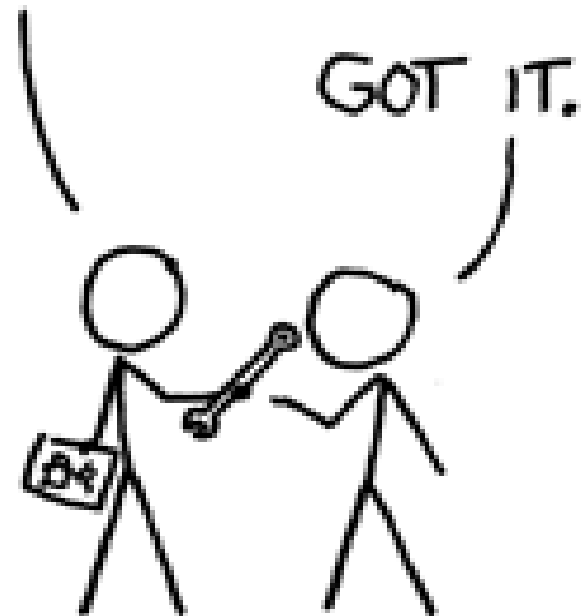
NO GOOD! IT'S
4096-BIT RSA!

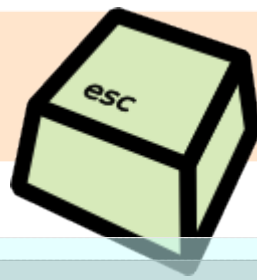
BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.





1996, +

deniable encryption su dischi,

1998, +

steganografia su dischi (pare che al tempo fosse un requisito pseudo-militare: “la segretezza dei dati è più importante della loro fruibilità”)

2002+

2c2, 4c

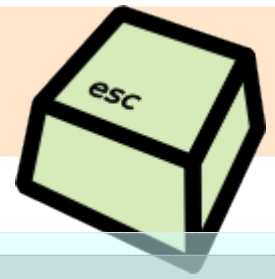
<http://lcamtuf.coredump.cx/2c2.tgz>

<http://dione.ids.pl/~shykta/4c-0001.tgz> (ormai nel void)



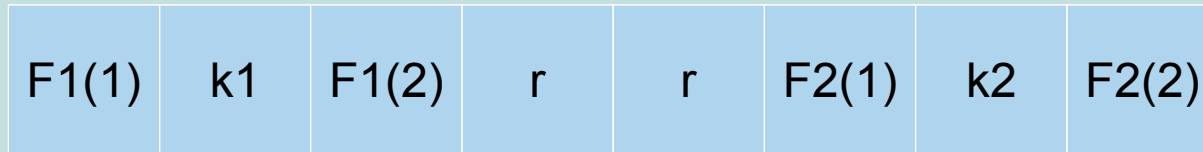
*Gloria, gloria,
gloria all'ipnorospo.*

2c2/4c, un concetto differente:



chiave, hash MD5, ciclata e ricalcolata come fosse un CBC. Ogni byte si considera come contenitore di due blocchi da 4 bit l'uno.

La prima chiave viene hashata, modulo 4, si trova la sua posizione (2 in questo caso) e nel bit antecedente e precedente viene messo il bit numero 1 del File 1



Nel bit successivo viene messo il bit 2 del File 1

Con la seconda chiave, modulo 4, shiftato di 4, stessa applicazione per lo sparpagliamento dei dati il resto è padding random.

Ogni file contiene un checksum interno.

Quando viene passata la password, la decifratura non sa se è il primo o il secondo file. li prova entrambi. Se il checksum combacia: è giusta. se nessun matcha, è un errore.



*Gloria, gloria,
gloria all'ipnorospo.*



X-2:src X\$ lettera

lettera encrypt outputfile [size increment]% plainfile[::password]

lettera decrypt cipherfile [password] [output directory]

lettera checkpass password(s)

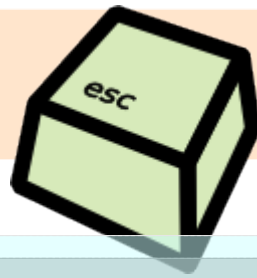
lettera example (show examples of use)

- passwords, if not available, is ask with echo off

<http://www.winstonsmith.info/julia/lettera/>



*Gloria, gloria,
gloria all'ipnorospo.*



concetto di base di elettra:

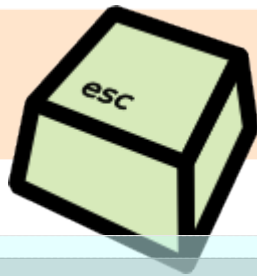
un file cifrato viene compresso, cifrato, aggiunto del random padding (di lunghezza randomica)

in questo modo anche la cifratura di un solo file causa l'aumento di dimensione del file finale

questo è necessario perché, se venisse chiesta una password, e il file decifrato risultasse piccolo rispetto al cifrato, sarebbe la motivazione della plausibilità.



*Gloria, gloria,
gloria all'ipnorospo.*



concetto di base di elettra, parte 2:

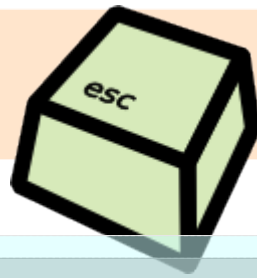
se vengono messi più file, il concetto è lo stesso: padding randomico prima e dopo.

le password scelte dall'utente non devono collidere (non collidono quasi mai, ma è vagamente possibile), perché dalla password si deriva un *entry point*.

l'entry point contiene dei dati che appaiono del random del tutto simile a quello che lo precede, ma è in realtà un hash



*Gloria, gloria,
gloria all'ipnorospo.*



concetto di base di elettra, parte 3:

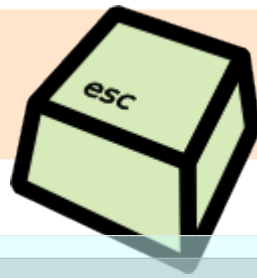
l'hash è generato dalla password, come l'entry point. se combacia, la password è valida (è un check utilizzato per comunicare l'errore all'utente che inserisce una password non valida)

in linea teorica, la crittografia ne fa anche a meno...

tra i dati cifrati c'è anche l'originale nome del file, la lunghezza, un checksum.



*Gloria, gloria,
gloria all'ipnorospo.*



funzionamento decifratura di elettra
inserimento di 2 o più password
ogni password viene hashata (N volte)
ogni hash equivale ad un checksum e ad un offset
se l'hash non compara, prova N+1...



*Gloria, gloria,
gloria all'ipnorospo.*

hack per riciclare enigmail a supportar elettra = mELETTRA



Compose: prova con mELETTRA

Send Contacts Spell Attach OpenPGP S/MIME Save

From: vecna <vecna@s0ftpj.org>

To: vecna@s0ftpj.org

To:

Subject: prova con mELETTRA

ELETTRA PASSWORD: "focaccia"

Saluti a tutti,
ho appena fatto la mia prima AG che sta fermentando da 3 gg. una IPA
senza pretese. Ho usato solo malto pale già crushed acquistato in
Inghilterra.

Poichè vorrei complicarmi la vita alla prossima cotta, vorrei sapere
se qualcuno mi può dire:

- specialty grains come chocolate vanno inseriti nel mash iniziale
insieme agli altri 2-row barley?
- nello step mashing si fa comunque sempre una prima fase di hot
strike a 78 gradi o si comincia più in basso (a seconda delle varie
ricette ho visto 62, 68 etc.)

VI ringrazio moltissimo per le risposte.

Mao

ELETTRA PASSWORD: "panzerotto"

UDT: Breaking the Data Transfer Bottleneck

UDT is a reliable UDP based application level data transport protocol
for distributed data intensive applications over wide area high-speed
networks. UDT uses UDP to transfer bulk data with its own reliability
control and congestion control mechanisms. The new protocol can transfer
data at a much higher speed than TCP does. UDT is also a highly
configurable framework that can accommodate various congestion control
algorithms. (Presentation: PPT 450KB / Poster: PDF 435KB)|



hack per riciclare enigmail a supportar elettra = mELETTRA



The screenshot shows an email client window with a menu bar (Edit, View, Go, Message, OpenPGP, Tools, Window, Help) and a toolbar with various icons. The main pane displays a list of emails under the 'Inbox' folder. The selected email is 'prova con mELETTRA'.

Subject: prova con mELETTRA
From: [vecna](#)
Date: 17:18
To: vecna@s0ftpj.org

***** BEGIN ELETTRA DECRYPTED PART *****
***** END OF ELETTRA DECRYPTED PART *****



Gloria

hack per riciclare enigmail a supportar elettra = mELETTRA



prova con mELETTRA

Get Mail Write Address Book Decrypt Reply Reply All Forward Tag Delete Junk Pri

Subject: prova con mELETTRA
From: [vecna](#)
Date: 17:18
To: vecna@s0ftpj.org

***** BEGIN ELETTRA DECRYPTED PART *****

Saluti a tutti,
ho appena fatto la mia prima AG che sta fermentando da 3 gg. una IPA
senza pretese. Ho usato solo malto pale gi=E0 crushed acquistato in
Inghilterra.

Poich=E8 vorrei complicarmi la vita alla prossima cotta, vorrei sapere
se qualcuno mi pu=F2 dire:

- specialty grains come chocolate vanno inseriti nel mash iniziale
insieme agli altri 2-row barley?
- nello step mashing si fa comunque sempre una prima fase di hot
strike a 78 gradi o si comincia pi=F9 in basso (a seconda delle varie
ricette ho visto 62, 68 etc.)

VI ringrazio moltissimo per le risposte.

Mao

***** END OF ELETTRA DECRYPTED PART *****



glo

hack per riciclare enigma a supportar elettra = mELETTRA



```
This is an OpenPGP/MIME encrypted message (RFC 2440 and 3156)
-----enigD4C663B080664F425E3DF309
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification
```

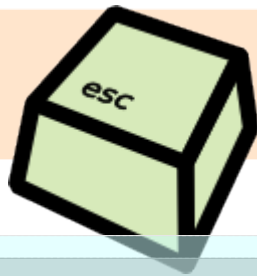
```
Version: 1
```

```
-----enigD4C663B080664F425E3DF309
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"
```

```
----- mELETTRA HEADER BEGIN -----
info ? check http://www.delirandom.net/melettra
```

```
658EH7Tucj13+Qn4CsL+8qrv2urwbf84Gsk7h+dVZhjUP1rTMDMVV29ypsWJqt1Ixa1ZUKx0
i4G29GegDQcrrVdmT6nL/FVZ13GcBwZjETI5ODbKXKOVjQ+4vJrHEL5BWL8sJill5A0GOaCF
3wclyedh9sLPiSGh7HrQFksdCWxU+F1+iDhRDoGhobbIpOscyeza4ehsMssK3U1jBfnE6Hdc
uLbpe6I1RAFdIJE8qd0BOGHRgsi4FRr5YNjXa6za54EOVhle3XhsMJQwLRGK1Njc+ZlQAnNA
8qSGsUVWCtoEReRt8KYCdoKIhY8UVpATa8v/him6qNSLs7515KsxSgg1F1kLZk7CPFxDu0fy
lFppcMjA0g7Fylposzsec6mc8DGJDBgNh4FHJnsdkEXbIB3N6cOXNS5OqJO+s1GEAUS9BZKp
6jqcrTARpRIROUkgEc5LE1AyQhqk5wQsmzRoHgJtFetEyARxLPw01bDuQycYQKsafLv8N/bV
e8r7ad1/AL02yNCwHGvY/DGYCixH18+f4V4UR8iY+YHOMdIXbYaZOHqjGU2sWdJYRUB89BSA
E+343HQolxd9NW0SjWhcRsn9Q23DJre6H2GR/NwIn6YXizHPvxHZe+/CSIEJc2SRaw7liRix
zoFlt2+PSX4mGvKXsX3J6pWFxVRiLJeOqrikvuHyZ976fkCOhuFmuc6kyEGzAVx46lvMangP
AnoC47Pylh20a86tM7Ec9ml0yo7ZcQsqujEr0V8loKGd3GzROITRe+ynrsoregDct9na8/Ue
kKlpCN5jxK1KPH4r2QF5K+7YWotQy8MjRr6nCyubqCyED//hRTvgLf3/QiWhD5mgLUA7CfPN
bmE6b6zcG+mcmRilvxVilt8zglWPjDWG2UM9yipwHWsrWjHTRiNgPpvmMDM0ENI2qEW9UXQ0
AORa/dWwoPAllgctPlmC0LvrS2cKS01RihmsUJYnm3DITYTChd5RvGfvBDrtRpum9zIMbjbx4
qBwfGIB+cfi8dlmkenC+A8myb98Iso2chva0ryg3/IbCDeCtwFsJIsBZculF0TTntGkdbU2K
KccbMtfj2ccYObzrQ8aVAhtyfrDD4G7CKeKtVWziJ+wppi0Vlhw3cQQJVM6WF50qTz8Y2/EG
RwX0dSWPKgicWC9ohQatVvicA65/iyB8uDsJW3+pewAVLB2A3m05rPYI292BGXBHrTER48fe
ExtMvosCa0rNzkDImfZ3r2EnERZuB3G5Ak7Fz21WgjQyinppcApCqVMOicz0UpEvR/VyZyz
FRUPLALiYf1M3H0Byfz2JZ1X3Cuq9/fNpisiH3I5yJL9rTENWe/9r8y9ZpOdQM5GxH50kPpt
X3K8JHc61p3OCpH2OXJWpg0uJIEV/GEy3kmyFCD95n6y6JL1IBAEclMms7fwzXJEXK/IkDrq
```





Funzionamento spicciolo di mELETTRA
(se vi viene in mente un nome migliore, you welcome)

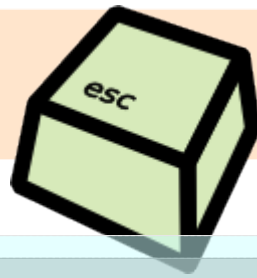
E' un file (melettra-wrapper.c) che viene configurato in enigmmail per essere usato al posto di gpg.

quando gpg viene invocato, se il messaggio passato contiene ELETTRA PASSWORD:"*" o ELETTRA HEADER, viene gestito dal wrapper.

altrimenti, flussi stdin/stdout e parametri vengono passati a gpg.



*Gloria, gloria,
gloria all'ipnorospo.*



melettra non ha un bel codice,

ma tu puoi essere la sua rinascita!

è un'alpha release orfana

perché è stata fatta apposta per ESC, e
domani ESC sarà finito.

è all'url <http://www.delirandom.net/melettra>

10x, domande ?



*Gloria, gloria,
gloria all'ipnorospo.*



Deniable Encryption

- 1) siete degli orsetti
- 2) venite trovati con le mani nella marmellata
- 3) l'inquisitore vi chiede perché...
- 4) *avete una storia plausibile!*
- 5) ...
- 6) **profit!**



*Gloria, gloria,
gloria all'ipnorospo.*



Deniable Encryption

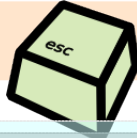
La D.E. vuole risolvere un problema che non è prettamente matematico,

Vuole, usando la crittografia, risolvere un problema che richiede necessariamente un umano attivo tra i nostri avversari.



*Gloria, gloria,
gloria all'ipnorospo.*

PERCHE' INTERESSARSENE ?



2007: Inghilterra rende attiva la terza parte del RIPA
RAW: due anni di detenzione se non riveli una password !?
(*approvata per finalità antiterroristiche, è stata usata in processi
contro animal right activist ...*)

2007: USA reparto immigrazione
può esserti richiesta la password per passare la frontiera USA !?

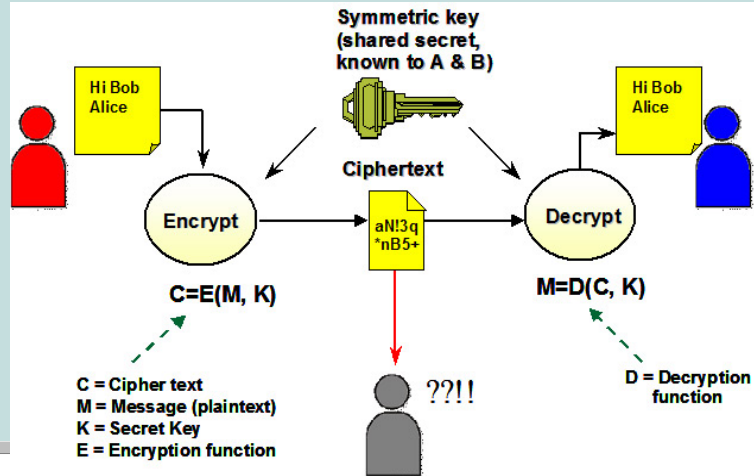
2007: Phrack: The only laws on Internet are assembly and RFCs
<http://www.phrack.org/issues.html?issue=65&id=6#article>



*Gloria, gloria,
gloria all'ipnorospo.*



quando si parla di crittografia, si usa parlare di “chiavi”.
sono i segreti, condivisi o meno tra le parti:



*Gloria, gloria,
gloria all'ipnorospo.*



La comune e intuitiva implementazione vede l'utilizzo di password, e la legge si è focalizzata su quello.

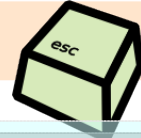
(spesso si tratta di password che proteggono chiavi di lunghezza ed entropia migliori)

ma chi lo dice che i software debbano continuare ad essere così ?
questa era un po' la teoria dell'articolo su phrack, che presentava il software **elettra**.



*Gloria, gloria,
gloria all'ipnorospo.*

Ma prima di parlar di elettra, contestualizziamo:



Qualunque strumento
(*software, sociale, informativo*)
che deve darvi una sensazione di sicurezza, deve essere valutato in
relazione alla minaccia dalla quale volete proteggervi.

Modelli di minaccia:

1/Basso

Il vostro fidanzato vuol conoscere le vostre preferenze su youporn

2/Medio

*avete una spia alle calcagna che vuol scoprire la vostra ricetta
dell'involtino primavera*

3/Alto

*Il mossad è incazzato con voi perché avete venduto plutonio ad un
palestinese al parco*



*Gloria, gloria,
gloria all'ipnorospo.*



La deniable encryption
crittografia negabile ? (brrr)

E' l'interpretazione crittografica della negazione plausibile (plausible deniability): <http://en.wikipedia.org/wiki/Deniability>

Quest'interpretazione si applica, in crittografia, avendo differenti chiavi che possono decifrare un solo messaggio. A seconda della chiave fornita, un messaggio diverso sarà rivelato. Questo ha senso se, e solo se, la rivelazione (della chiave) ed il rilevamento del messaggio hanno senso (plausible deniability, must to be plausible)



*Gloria, gloria,
gloria all'ipnorospo.*



- 1) Alice tradisce il marito Bob andando con Vecna, e B lo sospetta. A per comunicare in segreto con V genera 2 chiavi. Le da entrambe a V.
- 2) A scrive a V generando un messaggio crittato, composto così: noiose conversazioni algebriche cifrate con la chiave 1, messaggi amorosi cifrati con la chiave 2.
- 3) V possiede entrambe le chiavi, decifra entrambi i messaggi, risponde ad entrambi coerentemente e genera una risposta allo stesso modo del punto 2.
- 4) Quando B ha dubbi, interroga A riguardo lo scambio cifrato, A rivela la chiave 1, B legge dell'algebra e conclude che V è certamente un nerd asessuato. Torna a leggersi la gazzetta mente ignora che c'è una seconda chiave (e un palco di corna).
- 5) A e V = vissero cifrando felici e contenti.



*Gloria, gloria,
gloria all'ipnorospo.*



Dicitura noiosa:

Quest'interpretazione si applica, in crittografia, avendo differenti chiavi che possono decifrare un solo messaggio. A seconda della chiave fornita, un messaggio diverso sarà rivelato.

Questo ha senso se, e solo se, la rivelazione (della chiave) ed il rilevamento del messaggio hanno senso (*plausible deniability, must to be plausible*)



*Gloria, gloria,
gloria all'ipnorospo.*



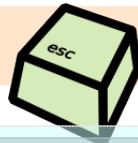
I software che più comunemente fanno deniable encryption (TrueCrypt e i suoi derivati-progenitori: FreeOFTE e BestCrypt)

Funzionano con il concetto di “*hidden volumes*”:

- . L'utente formatta una partizione con dati casuali
- . crea N volumi nascosti, ogni password ne sblocca uno
- . Ad un analisi passiva, ogni password è plausibile apra l'unico *hidden volume*, e che sia l'unico presente nella partizione in analisi.
- . all'analisi passiva, i dati cifrati devono apparire con le stesse proprietà dei dati random che occupano le parti non utilizzate del disco. http://en.wikipedia.org/wiki/Diehard_tests



*Gloria, gloria,
gloria all'ipnorospo.*



Lo stesso utilizzo della D.E., in questo momento storico, può suonare come un'anomalia!

Per questo motivo, alla richiesta di una password, è necessario ci sia qualcosa di estremamente plausibile!



*Gloria, gloria,
gloria all'ipnorospo.*



Ne consegue che, per essere plausibile, dovrebbe essere utilizzata sempre e comunque.

storia di CryptoKitchen: www.inventati.org/cryptokitchen/
ha senso che mi scambi email cifrate (con gnupg) solo quando devo dir qualcosa di sensibile ?

no, o l'avversario dedurrà, dal mio utilizzo di gpg, chi è un contatto da proteggere e chi non lo è.

Per questo motivo deve essere usata indiscriminatamente over possibile. CryptoKitchen era una mailing list cifrata per lo scambio di ricette di cucina.



*Gloria, gloria,
gloria all'ipnorospo.*



- 1) Se l'obiettivo è la riservatezza, la soluzione è la crittografia
- 2) Se l'obiettivo è l'occultamento plausibile in caso di richiesta forzata, la soluzione è la deniable encryption (a patto ci sia una plausibile risposta: quello dal quale ci si vuole difendere implica necessariamente un elemento umano)
vien anche detta: steganographic encryption
- 3) se l'obiettivo è l'occultamento e basta, la soluzione appropriata è la steganografia

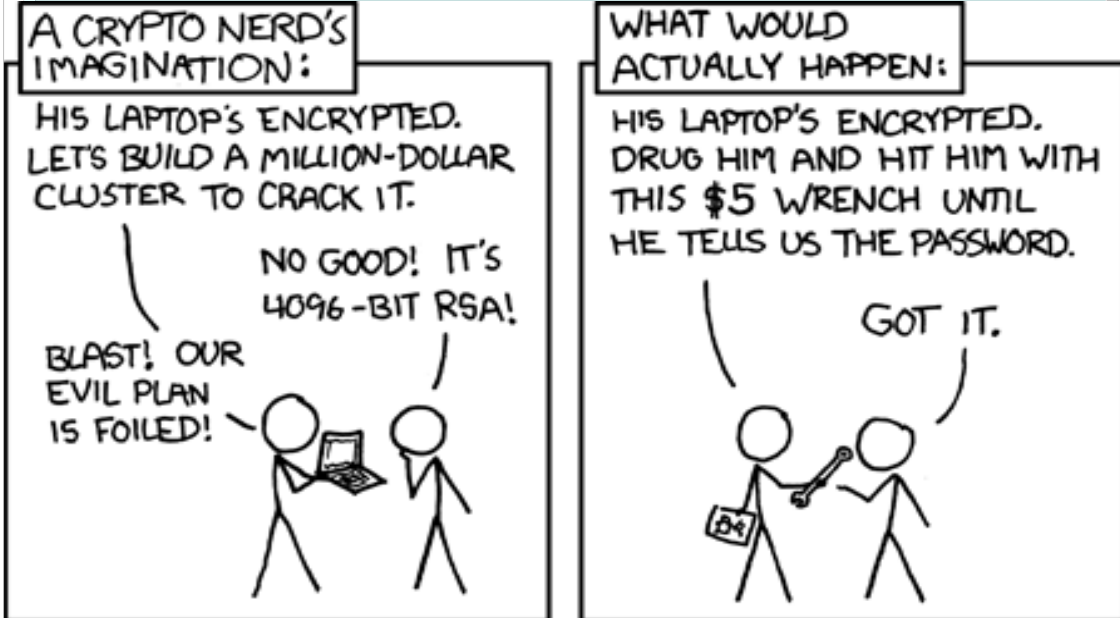
ok, è ora di parlare di software :)



*Gloria, gloria,
gloria all'ipnorospo.*



il primo fu *rubberhose filesystem*, voleva risolvere:





1996, +

deniable encryption su dischi,

1998, +

steganografia su dischi (pare che al tempo fosse un requisito pseudo-militare: “la segretezza dei dati è più importante della loro fruibilità”)

2002+

2c2, 4c

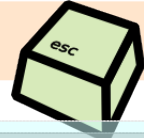
<http://lcamtuf.coredump.cx/2c2.tgz>

<http://dione.ids.pl/~shykta/4c-0001.tgz> (ormai nel void)



*Gloria, gloria,
gloria all'ipnorospo.*

2c2/4c, un concetto differente:



chiave, hash MD5, ciclata e ricalcolata come fosse un CBC. Ogni byte si considera come contenitore di due blocchi da 4 bit l'uno.

La prima chiave viene hashata, modulo 4, si trova la sua posizione (2 in questo caso) e nel bit antecedente e precedente viene messo il bit numero 1 del File 1

F1(1)	k1	F1(2)	r	r	F2(1)	k2	F2(2)
-------	----	-------	---	---	-------	----	-------

Nel bit successivo viene messo il bit 2 del File 1

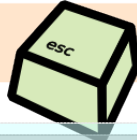
Con la seconda chiave, modulo 4, shiftato di 4, stessa applicazione per lo sparpagliamento dei dati il resto è padding random.

Ogni file contiene un checksum interno.

Quando viene passata la password, la decifratura non sa se è il primo o il secondo file. li prova entrambi. Se il checksum combacia: è giusta. se nessun matcha, è un errore.



*Gloria, gloria,
gloria all'ipnorospo.*

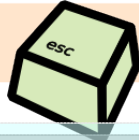


X-2:src X\$ elettra
elettra encrypt outfile [size increment]% plainfile[::password]
elettra decrypt cipherfile [password] [output directory]
elettra checkpass password(s)
elettra example (show examples of use)
- passwords, if not available, is ask with echo off

<http://www.winstonsmith.info/julia/elettra/>



*Gloria, gloria,
gloria all'ipnorospo.*



concetto di base di elettra:

un file cifrato viene compresso, cifrato, aggiunto del random padding (di lunghezza randomica)

in questo modo anche la cifratura di un solo file causa l'aumento di dimensione del file finale

questo è necessario perché, se venisse chiesta una password, e il file decifrato risultasse piccolo rispetto al cifrato, sarebbe la motivazione della plausibilità.



*Gloria, gloria,
gloria all'ipnorospo.*



concetto di base di elettra, parte 2:

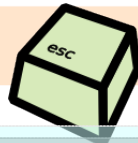
se vengono messi più file, il concetto è lo stesso: padding randomico prima e dopo.

le password scelte dall'utente non devono collidere (non collidono quasi mai, ma è vagamente possibile), perché dalla password si deriva un *entry point*.

l'entry point contiene dei dati che appaiono del random del tutto simile a quello che lo precede, ma è in realtà un hash



*Gloria, gloria,
gloria all'ipnorospo.*



concetto di base di elettra, parte 3:

l'hash è generato dalla password, come l'entry point. se combacia, la password è valida (è un check utilizzato per comunicare l'errore all'utente che inserisce una password non valida)

in linea teorica, la crittografia ne fa anche a meno...

tra i dati cifrati c'è anche l'originale nome del file, la lunghezza, un checksum.



*Gloria, gloria,
gloria all'ipnorospo.*



funzionamento decifrazione di elettra
inserimento di 2 o più password
ogni password viene hashata (N volte)
ogni hash equivale ad un checksum e ad un offset
se l'hash non compara, prova N+1...



*Gloria, gloria,
gloria all'ipnorospo.*

hack per riciclare enigmail a supportat elettra = mELETTRA



Compose: prova con mELETTRA

Send Contacts Spell Attach OpenPGP S/MIME Save

From: vecna <vecna@s0ftpj.org>

To: vecna@s0ftpj.org

Subject: prova con mELETTRA

Sign Message ⌘⇧S
 Encrypt Message ⌘⇧E
 Use PGP/MIME for This Message
Ignore Per-Recipient Rules

ELETTRA PASSWORD:"focaccia"

Saluti a tutti,
ho appena fatto la mia prima AG che sta fermentando da 3 gg. una IPA
senza pretese. Ho usato solo malto pale già crushed acquistato in
Inghilterra.

Poichè vorrei complicarmi la vita alla prossima cotta, vorrei sapere
se qualcuno mi può dire:
- specialty grains come chocolate vanno inseriti nel mash iniziale
insieme agli altri 2-row barley?
- nello step mashing si fa comunque sempre una prima fase di hot
strike a 78 gradi o si comincia più in basso (a seconda delle varie
ricette ho visto 62, 68 etc.)

VI ringrazio moltissimo per le risposte.

Mao

ELETTRA PASSWORD:"panzerotto"

UDT: Breaking the Data Transfer Bottleneck

UDT is a reliable UDP based application level data transport protocol
for distributed data intensive applications over wide area high-speed
networks. UDT uses UDP to transfer bulk data with its own reliability
control and congestion control mechanisms. The new protocol can transfer
data at a much higher speed than TCP does. UDT is also a highly
configurable framework that can accommodate various congestion control
algorithms. (Presentation: PPT 450KB / Poster: PDF 435KB)

hack per riciclare enigmail a supportar elettra = mELETTRA



Edit View Go Message OpenPGP Tools Window Help

Inbox

Subject

- o prova con mELETTRA
 - o Re: domande hackare.
 - o talk esc
 - o Re: talk esc
 - o elettra prova
 - o Ottobre
 - o [unz] CFM (Call For Minchiate)
 - o Re: [unz] CFM (Call For Minchiate)
 - o Re: [unz] CFM (Call For Minchiate)
 - o Re: [unz] CFM (Call For Minchiate)
 - o Re: [unz] CFM (Call For Minchiate)
 - o Re: [unz] CFM (Call For Minchiate)
 - o Re: [unz] CFM (Call For Minchiate)

Subject: prova con mELETTRA

From: [vecna](#)

Date: 17:18

To: vecna@s0ftpj.org

```
***** BEGIN ELETTRA DECRYPTED PART *****
***** END OF ELETTRA DECRYPTED PART *****
```



Gi
glori

hack per riciclare enigmail a supportar elettra = mELETTRA



prova con mELETTRA

Get Mail Write Address Book Decrypt Reply Reply All Forward Tag Delete Junk Pri

Subject: prova con mELETTRA
From: vecna
Date: 17:18
To: vecna@s0ftpj.org

***** BEGIN ELETTRA DECRYPTED PART *****

Saluti a tutti,
ho appena fatto la mia prima AG che sta fermentando da 3 gg. una IPA
senza pretese. Ho usato solo malto pale gi=E0 crushed acquistato in
Inghilterra.

Poich=E8 vorrei complicarmi la vita alla prossima cotta, vorrei sapere
se qualcuno mi pu=F2 dire:
- specialty grains come chocolate vanno inseriti nel mash iniziale
insieme agli altri 2-row barley?
- nello step mashing si fa comunque sempre una prima fase di hot
strike a 78 gradi o si comincia pi=F9 in basso (a seconda delle varie
ricette ho visto 62, 68 etc.)

VI ringrazio moltissimo per le risposte.

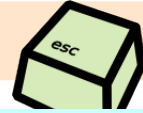
Mao

***** END OF ELETTRA DECRYPTED PART *****



glo

hack per riciclare enigmail a supportar lettera = mELETTRA



```
This is an OpenPGP/MIME encrypted message (RFC 2440 and 3156)
-----enigD4C663B080664F425E3DF309
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

-----enigD4C663B080664F425E3DF309
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"
```

```
----- mELETTRA HEADER BEGIN -----
info ? check http://www.delirandom.net/melettra
```

```
658EH7Tucj13+Qn4CsL+8qrv2urwbf84Gsk7h+dVzhjUP1rTMDMVV29ypsWJqt1IxaLzUKx0
i4G29GegDQcrrVdmT6nL/FVZ13GcBwZjETI50DbKXK0vJq+4vJrHEL5BWL8sJi115A0GOaCF
3wclyedh9sLPiSGh7HrQFksdCWxU+F1+iDhRDoGhobbIpOscyeza4ehsMssK3U1jBfnE6Hdc
uLbpe6I1RAFdIJE8qd0BOGHRqsi4FRr5YNjXa6za54EOVh1E3XhsMJQwLRGK1Njc+Z1QANNA
8qSGsUVWCtoEReRt8KYCdoKIhY8UVpATa8v/him6qNSLs7515KsXsgq1FlkLzK7CPFXDu0fy
lFppcMjA0g7Fylposzsec6mc8DGJDBgNh4FHJnsdkEXbIB3N6cOXNS5OqJ0+slGEAUS9BZKp
6jgcrTARpRIROUkgEc5LElAyQhQk5wQsmzRoHgJtFetEyARxLPw01bDuQycYQKsafLw8N/bV
e8r7ad1/AL02yNCwHGvY/DGYCixH18+f4V4UR8iY+YHOMdIXbYazOHqjGU2sWdJYRUB89BSA
E+343HQo1xd9NW0SjWhcRsn9Q23DJre6H2GR/NwIn6YXizHPvxHZe+/CSIEJc2SRAw7liRix
zoFlt2+PSX4mGvKXsX3J6pWFxVRiLJeOqrikvuHyz976fkCOhuFmuc6kyEGzAVx46lvMangP
AnoC47Pylh20a86tM7Ec9m1Oyo7ZcQsqjEr0V8loKGd3GzROITRe+ynrsORgDCT9nA8/UE
kKlpCN5jxK1KPH4r2QF5K+7YWOtQy8MjRr6nCyubqCyED//hRTvgLf3/QiWhD5mgLUA7cFPN
bmE6b6zcG+mcmRIlvxVilt8zq1WPjDWG2UM9yipwHwSrWjHTRiNgPpVbMDM0ENI2qEW9UXQ0
AORA/dWwoPallgctPlmC0LvrS2cKS01RihmsUJYnm3DITYTChd5RvGfvBDrtrpump9zIMbjbx4
qBwfGIB+cfi8dlMkenC+A8myb98Iso2chva0ryg3/IbCDeCtwFsJIsBZculF0TTntGkdbU2K
KccbMtfj2ccY0bzrQ8aVAHtyfRDD4G7CKeKtVWziJ+wppi0Vlh3cQQJVM6WF50qTz8Y2/EG
RwX0dSWPKgicWC9ohQAtVvicA65/iyB8uDsJW3+pewAVLB2A3m05rPYI292BGXBHrTER48fE
EXtMvosCa0rNzkDImfZ3r2EnERZuB3G5Ak7Fz21WgjQyinppecApCqVMOicz0UpEvR/VyZyz
FRUPLALiYfLM3H0ByfZ2JZ1X3Cuq9/fNPiSih3I5yJL9rTENWe/9r8y9ZpOdQM5GxH50kPpT
X3K8Jhc61p3OCpH2OXJWpg0uJIEV/GEy3kmyFCD95n6y6JL1IBAcLmms7fWzXJEXX/IkDrq
.....
```





Funzionamento spicciolo di mELETTRA
(se vi viene in mente un nome migliore, you welcome)

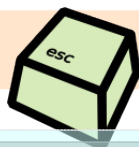
E' un file (melettra-wrapper.c) che viene configurato in
enigmail per essere usato al posto di gpg.

quando gpg viene invocato, se il messaggio passato contiene
ELETTRA PASSWORD:"*" o ELETTRA HEADER, viene
gestito dal wrapper.

altrimenti, flussi stdin/stdout e parametri vengono passati
a gpg.



*Gloria, gloria,
gloria all'ipnorospo.*



melettra non ha un bel codice,
ma tu puoi essere la sua rinascita!

è un'alpha release orfana
perché è stata fatta apposta per ESC, e
domani ESC sarà finito.

è all'url <http://www.delirandom.net/melettra>

10x, domande ?



*Gloria, gloria,
gloria all'ipnorospo.*