P.G.P. P.retty G.ood P.rivacy

www.stordito.it

A cosa serve la crittografia?

La crittografia serve a:

- cifrare un messaggio di testo o un file affinché solo il destinatario sia in grado di leggerlo (questa funzionalita' in Inglese viene chiamata **ENCRYPT**)
- autenticare il testo inviato dal mittente affinché il destinatario sia certo che il messaggio non è stato alterato (questa funzionalita' in Inglese viene chiamata SIGN)
- garantire che l'indirizzo di posta elettronica e la chiave pubblica di una persona appartengono veramente a quella persona (questa funzionalita' in Inglese viene chiamata **TRUST**)

Ogni volta che inviamo una e-mail, essa transita attraverso internet providers che tecnicamente sono in grado di leggerne il contenuto. La crittografia e' quindi nata per rispondere a questi problemi di sicurezza e riservatezza che in alcuni casi sono indispensabili come ad esempio per l'invio di documenti finanziari, strategici, etc

Che cosa e' PGP?

Il tallone d'achille della crittografia classica consiste nel fatto che per cifrare e decifrare un messaggio occorre una password in possesso sia del mittente che del destinatario. Ma queste due persone potrebbero trovarsi a notevole distanza tra di loro o addirittura non conoscersi affatto e pertanto, se non esiste un canale sicuro per scambiarsi la password di cifratura, occorre avvalersi di canali pubblici (telefono, e-mail, chat, posta convenzionale, sms, etc.) attraverso i quali la chiave potrebbe essere intercettata.

Per questo motivo in tempi di guerra fredda un tale di nome Philip Zimmermann invento' un modello di crittografia a doppia chiave che chiamo' PGP (Pretty Good Privacy) e lo rese disponibile su Internet affinche' tutti potessero comunicare protetti dal controllo del governo.

PGP e' un programma che genera automaticamente una coppia di chiavi, una chiamata Pubblica e l'altra chiamata Privata, che sono intimamente legate l'una all'altra attraverso una ulteriore password che scegliamo noi. La chiave segreta non deve mai uscire dal nostro computer, mentre quella pubblica possiamo inviarla a tutti i nostri amici senza paura che ci venga intercettata, anzi e' proprio quello che vogliamo, infatti quando un nostro amico ci inviera' un messaggio cifrandolo usando la nostra chiave pubblica, solo la corrispondente chiave privata sara' in grado di decifrarlo, e quindi soltanto noi poiche' quella chiave privata non e' mai uscita dal nostro computer.

Una chiave pubblica, quindi, potrebbe non essere sicura solo se non si è certi della sua reale appartenenza, cioè solo se temiamo che Carlo ci abbia spedito la sua chiave pubblica spacciandosi per Luca e quindi noi scriviamo a Carlo pensando di stare scrivendo a Luca (si capisce l'estrema rarità del caso descritto.. e comunque e' possibile anche garantire l'appartenenza delle chiavi pubbliche).

Poiche' PGP era un prodotto commerciale, in anni recenti una comunita' di programmatori illuminati ha sviluppato una versione completamente gratuita e open source e l'ha chiamata GPG, per cui e' stata concepito questo manuale.

Riassumendo faccio alcuni esempi di cosa e' possibile fare con GPG:

- io sono in possesso della chiave pubblica di Mario e volendo inviargli una mail riservata, effettuo la cifratura del mio messaggio (Comando ENCRYPT) usando la SUA chiave pubblica. Solo Mario, che ha la corrispondente chiave privata, potra' decodificare la mail
- Viceversa, mi arriva una mail che è stata cifrata sulla base della mia chiave pubblica, io potro' quindi decodificarla (Comando DECRYPT) con la mia chiave segreta corrispondente, dove dico corrispondente perché uno può anche avere più coppie di chiavi a suo nome, in genere una per ogni indirizzo di e-mail.

- Voglio inviare a Mario una mail senza cifrarla ma voglio dargli la certezza che sono proprio io ad averla spedita; in tal caso posso usare la mia chiave privata per firmare (Comando SIGN) il mio messaggio, e quando Mario lo ricevera' potra' usare la mia chiave pubblica e verificare (Comando VERIFY) che il messaggio è stato inviato proprio dal sottoscritto ed inoltre che non è stato in alcun modo alterato da estranei.
- Viceversa, ricevo una mail da Mario che e' stata firmata con la sua chiave privata, e io posso quindi usare la chiave pubblica di Mario per verificare (Comando VERIFY) che quella mail e' stata scritta effettivamente da lui e non modificata da nessun altro

Chiaramente le due operazioni di cifratura e firma possono farsi contemporaneamente (Comando ENCRYPT & SIGN) in modo da cifrare il messaggio per Mario cosi' che solo lui possa leggerlo e al contempo garantirgli che l'ho scritto proprio io e nessuno ha potuto modificarlo.

Quale software e' necessario?

GPG e' di per se un programma a riga di comando, cioe' molto difficile da usare da chi non e' un esperto di computer. Per questo motivo sono nati dei programmi interfaccia (chiamati in inglese "Front End") i quali permettono di usare GPG attraverso una comoda finestra per Windows.

Potete scaricare le versioni installabili di GPG e di svariati Front End dal sito di GPG stesso che e' <u>http://www.gnupg.org</u> tuttavia per installare tali programmi dovete avere diritti da amministratore sul vostro computer. Per questo motivo ho scritto questa guida basandomi sulle versioni portatili (cioe' che non richiedono installazione) di GPG e di Cryptophane (un Front End che io trovo semplice e ben fatto) e che ho reso disponili in un file compresso che potete scaricare da questo link: http://www.stordito.it/software/programmi_per_crittografia.zip

Come lo installiamo?

Una volta scaricato il file compresso dal link sopra, dovete solo decomprimerlo dentro la cartella **C:/Program Files** (in caso vogliate scegliere una cartella diversa e' necessario modificare il file **cryptophane.ini** e indicare il corretto percorso).

Alla fine della operazione vi troverete due nuove sottocartelle al suo interno cosi' nominate:

C:/	Program	Files
~,		

/GnuPG /Cryptophane

🔾 🗢 📕 🕨 Computer 🕨 hards	disk (C:) → Program Files → GnuPG → 🔫 👍		<mark>حد</mark> ا	🚱 🗢 🕌 « harddisk (C:) 🕨 Program Files	► Cryptophane - 49 Se	arch Cryptophane	
Organize • Include in library •	Share with 👻 Burn New folder	8==	• 🔳 🔞	Organize - Include in library - Share w	rith 🕶 Burn New folder	8==	- 🗌 🔞
🔆 Favorites	Name	Date modified	Туре	☆ Favorites	Name	Date modified	Туре
	Doc	Thu 15-9 14:18	File folder		😵 Cryptophane.chm	Wed 07-12 23:40	Compiled HT
🧊 Libraries	gnupg.nls	Thu 15-9 14:18	File folder	Cibraries	G Cryptophane.exe	Sun 18-12 23:13	Application
Desktop	Src .	Thu 15-9 14:19	File folder	Desktop	Cryptophane.ini	Thu 15-9 14:22	Configuration
Documents	gpg.exe	Mon 18-10 12:04	Application	Downloads			
Downloads	gpgkeys_curl.exe	Mon 18-10 12:04	Application				
	gpgkeys_finger.exe	Mon 18-10 12:04	Application				
	gpgkeys_hkp.exe	Mon 18-10 12:04	Application	🛤 Computer			
👰 Computer	gpgkeys_ldap.exe	Mon 18-10 12:04	Application	🏭 harddisk (C:)			
🏜 harddisk (C:)	gpgsplit.exe	Mon 18-10 12:04	Application				
	📰 gpgv.exe	Mon 18-10 12:04	Application				
	🎯 uninst-gnupg.exe	Thu 09-12 12:09	Application				
				🗣 Network			
두 Network							
	۲. III III III III III III III III III I		F		< [
11 items				3 items			

La prima cartella la ignoriamo, e nella seconda clicchiamo il tasto destro del mouse su **Cryptophane.exe** e nel menu contestuale che compare. scegliamo "**Invia a**" e quindi "**Desktop (crea collegamento)**" in modo da trovarci sul desktop di Windows l'icona del programma Cryptophane.

A questo punto e' fatta, ci basta doppio cliccare sull'icona sopra e saremo pronti al prossimo paragrafo!

Come generiamo la nostra coppia di chiavi?

È decisamente la cosa fondamentale, o no? ... quindi lanciate **Cryptophane** e vi troverete davanti la finestra sottostante:

G ^o Cryptopha File View	ane 0.7.0 Kevs Tools Help						• ×
Filter	795 Teen						0
Name	E-mail	Trust	Sigs	Created	Expires	Key ID	
•							•
	ruptophane hint: Starting out using Cru	Intonhane					
	you've never used cryptography products bef	ore, start by <u>Creatir</u>	ng a Sec	ret Key for you	irself.		
U II	you've previously made a private key that you	'd like to import inti	o Cryptop	hane, learn a	bout Importing	3 Secret Keys.	
							//.

La finestra centrale elenca le chiavi pubbliche e private e quindi e' vuota perche' lo abbiamo appena installato. Andiamo allora nel menu **Keys** e scegliamo **Generate secret keys** come mostrato qui sotto:

Ke	ys
	Properties of Selected Key
	Sign Selected Key
	Edit Trust of Selected Key
	Delete Selected Key
	Generate Revocation Certificate for Selected Key
	Search Keyserver
	Get Key from Keyserver
	Refresh from Keyserver
	Send to Keyserver
<	Generate Secret Key

Si aprira' la finesta sottostante in cui ci viene richiesto **Nome Cognome** e l'indirizzo **E-Mail** a cui tale chiave corrispondera'. Nota bene che tali informazioni saranno "incorporate" nelle chiavi generate, pertanto dovete fare una coppia di chiavi per ogni indirizzo e-mail dove desiderate ricevere o scrivere messaggi crittografati.

Generate Secret	Key	Image: State Sta
Enter your detail	s below to create a new key for your Cryp	otophane keyring.
Name:	Paolo Lombardi	
E-mail address:	paololombardi.it@gmail.com	
Comment:		🗖 Key expires
New passphrase		DSA key length: 1024 💌
Confirm passphr	BSE: ************************************	ElGamal key length: 1024 💌
		<u>G</u> enerate <u>C</u> ancel

Nella stessa finestra dovete scegliere la "passphrase" che rappresenta una ulteriore sicurezza al sistema della doppia chiave. Nota bene che se la dimenticate, sara' per sempre irrecuperabile tutta la posta crittografata che avete inviato e ricevuto.

Siamo pronti, e finalmente potete premere il pulsante Generate



Ed ecco che nella finestra principale di Cryptophane comparira' elencata la nostra prima chiave

ile View Keve	Tools Help						-
The view Reys	Tools Help						
ilter							 1
Name	E-mail	Trust	Sigs	Created	Expires	Key ID	
🛏 Paolo Lombardi	paololombardi.it@gmail.com	Ultimate	1	2011-09-30		019E1B40	
		111					
-	ane hint: Adding other neonle's l	ceys to your k	eyring				
Cryptopl	iane nine. Adding other people's r						
Cryptopl Learn how	v to search for other people's keys using	the <u>Search Key</u>	server F	unction.			

Ora la prima cosa da fare e' una copia di sicurezza delle nostra coppia di chiavi, su un memory stick esterno.

In questo modo, se mai un giorno cambiassimo il computer, o dovesse rompersi l'hard disk, noi avremo sempre modo di recuperare la coppia delle nostre chiavi.

Nota che se perdete la vostra chiave segreta, non potreste più decifrare alcun messaggio crittografato con la corrispondente chiave pubblica, la quale invece è ancora viva e vegeta e in mano ai vostri corrispondenti. In un tale scenario dovreste generare una nuova coppia di chiavi, inviare ai vostri corrispondenti la vostra nuova chiave pubblica, e comunque non potrete piu' leggere tutta la posta crittografata ricevuta e inviata fino a quel momento, per questo e' importante fare una copia di sicurezza.

Per esportare la nostra chiave segreta, e' sufficiente andare nel menu file e scegliere Export Secret keys come mostrato qui:



Si aprira' una finestra dove selezionare la chiave segreta che volete esportare (in questo caso ce ne e' una sola che abbiamo precedentemente generato e quindi selezioniamo lei)

G Export Keys	[83
Select the keys you would like to export:		
Key	Key ID	
✓ Paolo Lombardi <paololombardi.it@gmail.com></paololombardi.it@gmail.com>	019E1B40	
Export all keys Save output to a file	<u>D</u> K <u>C</u> ancel	

Ci accertiamo che sia selezionato "Save output to file" e poi clicchiamo su OK.

Si aprira' la finestra sottostante in cui possiamo scegliere sia il nome che la posizione del file di testo che conterra' la nostra chiave segreta.



Come nome del file, consiglio di cominciare con "secret key" che vi ricorda quale tipo di chiave state esportando, per poi seguire con il vostro nome e quindi un testo che vi faccia capire a quale indirizzo e-mail tale chiave si riferisca. Nel mio esempio, digitero' "secret key paolo lombardi gmail" e poi clicchero' su Save

Cryptophane salva di default files con estensione .ASC che sono automaticamente aperti con Cryptophane stesso.

Un file .ASC e' un file di testo, per cui potete anche scrivere direttamente l'estensione .TXT quando scegliete il nome del file nella maschera sopra. Se aprite con Blocconote il file appena generato, vedrete i caratteri che compongono la vostra chiave segreta:



Questa intera procedura va chiaramente ripetuta anche per la chiave pubblica. Dal menu **file** di Crypthophane sceglierete **Export public keys** e quindi selezionerete dall'elenco quale chiave pubblica volete esportare, e poi sceglierete posizione e nome del file, che nel mio esempio questa volta sara' **"public key paolo lombardi gmail**", e anche stavolta se aprirete il file esportato con Blocconote, visualizzerete una finestra piena di caratteri, come potete vedere sotto:

hle DBL Johnsk Yam Hop BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.4.11 (Wingw32) MQGIBEGFtdwRBACVKA5GKeGvXhl4tB0/Vy76AV4bfaXlJVyStq+j35e5HzyV+hu LewD55x+Zelylpf2atew /krmkvZFWWIBSAF6A7moSQNh3tmv6gP4KsUdp1toIx vsdTaw9Hx3fch8255YA3G9KpvHHOSW15KeV2Y5yyXoUccsmu1oy1tx3rywcGkYT1 GerYXphL, Ovbgvj+ggYKXDD/iXlhV91IzcuB2V2YFEXmHOGVH+KF5GcW12F0 XuLUj28ZN1JKGXQDRdJY8fW3TmNjOnig4wGujGzfhtp75j028rpxKhrM4N3CmHd KA47wk3fch82C3VAG0KJY8fW3TmNjOnig4wGujGzfhtp75j028rpxKhrM4N3CmHd GerW22mV03J91b2/TGKC8bL47OnuXrV91ExcuB2V2FEXmHOGDP1pXxLRUKYPE LdYONja01JHTa2014205Gy10278aYN9014VT/GJPhmBz00CbgrUgCVbG8gTG9t Umry2GkgPHBhD2xvbG9TmFYZGKUAR2211AwWU72FDrb1BBRAgA18QJ0hbxC AhsjBgs5CACDAgYVCAIJCgEFgIDAQIeAQIXgAAKCRC1Rp+A24bQ1gQaJ0b0yM gfBX83UAyAeV95jXBH2LACeNICyVHTbXsUMDxUY21FDrb1BBRAgA18QJ0hbxC AhsjBgs5CACDAgYVCAIJCgEFgIDAQIEAQIXgAAKCRC1Rp+A24bQ1gQaJ0b0yM gfBX83UAyAeV95jXBH2LACeNICyVHTbXsUMDxUF1JjVwCTurGSAQBETOW13BAE ANJ0ZwSImE2n69MquXlWnYCQGFFL2hq+HrPPHk29XNFV7gdAyU7Cd5h1XxSG45 fdV7qdyxerf/AbtC1h658V7p6d6XkK6g0QUM01Pv00JR4PkXKMe3H2dOruEWm Zf21++vjK31TayHv2BCLLMy2JU0D83tGpLgeRAGg2YBZAAWGA/95bMrVsBAA0125 fTwqPhyS0gV6V/rC/W1Dr074jG020CUP111Ppr1ADXNG0HBEgq7TBTEN0XF1Nu +v6E5V8qX2KtetH9IXH71x03La8E6HSH3LIrW4JBU0JhXsGAB20J0bXcAN5HAA0325 /VGHB httALKQAn146PV1URI0SCeGtV+n2HCX1HXXtAJSHm/S76UsAy2e29Qg1KI3WKTE 2q=	🔄 public key paolo lombardi gmail.asc - Notepad
BEGIN PGP PUBLIC KEY BLOCK version: GnuPG v1.4.11 (Wingw32) mQGiBEGFtdwRBACVKA5GKeGvXhJtB0/VyTGAY4bfax]JvyStq+j35e5Hzyv+hvL LezwJ5s+PZely1pF2aEwE/krmRvZFMv3BsAF647mo5qNh3tmv6qP4KsU4DFioTvX vsdTaw9Hx3fcR255YA3G9KpvHh09WISKEVZYSyXOUCCSmUDy1tx37wgGVK vvUj2Z8Xh1GK25YA3G9KpvH09WISKEVZYSyXOUCCSmUDy1tx37wgGVK vvUj2Z8Xh1GK25YA3G9KpvH09WISKEVZYSyXOUCCSmUDy1tx37wgGVK vvUj2Z8Xh1GK25QF43G5KJ5KSCJ2VFF48A2CJ1 tgFY7KpnL/DvDgvj+qq7kX0D/ix1nv91IZzCuR5U2YPEKmH0oCVH+KrEScwiZfF0 vvDp3/4p+XigE0V63[BKCChpXtn100i34v6U]g2fThpZ5jD2EpxKbrM4A3CHHd cKA47wk3fqnvC2c4GFF4d681mxkP0IACFUrX401JYqA2PU2KUTFNXNd219+DFV1 vvDp3/4p+XigE0V63[BKCChpXtn105j7vbC1pyCqHKkmAa7L2CQQQXKV7]4E56 GMve2zmTV03L51B2/TGKCB8H.4r0mv2Y0A6537rmKyDF7480[Gp0]pXxLRUKA7PB tmry2GkCpHBhD2xvbC9FYmHj2GkuAR2211hawMv22tF0h1BBRAga3[B0]Dh2x Ah5]BgsScAcDAgrVCAIJCgEFEgIDAQIeAQIXgAAKCRCf1Rp+Az4b0j0gA10b0yM gfEX83UAyAeV95jxBMLACHV7yDFTbSvImSvLV21FPohVBRAga3[B0]Dh2x Ah3JdvzWSImE2n69MqxX1mvCgOFFL2hQ+HrPPHk29xhfV7gdAyU7tG45h1XxSG45 fMvmZypgV6V/rk/inr07j6j002020u111Ppr11DxvCUrDef10771B00X6Hb1FTmw zf21++vjK31IayHv2BCLLMy2]U0D89tGpLgeRAGg2YB2AAMGA/95bMrXG5h7Tmw rTQepHs0123XkvLe171x031&8866Sh+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v915l0VkGeKT rTQepHs0123XkvLe171x031&886G5h+1Lrw4JbvU1/ispE5m0v92229Qg1K13wKTE 2q== =9Lq1 END PGP PUBLIC KEY BLOCK	File East Format View Help
mggi BEGFE dwRBAC WKA5GK GEGVK Did EBD/YJ TGAYd PT AV JET + 35 SH2JYV+hUL LezW J5S+Y22113 PT 23 atomic /rmw127KWJ 35 AFG ATO SANAJT WKG PT AS LUADF 10 TIX VGP VS PML / DV BJY 12 CH 2000 SANAJT WKJ STAF ATO SANAJT WKJ PT AS LUADF 10 TIX GFY VS PML / DV BJY 12 CK 2000 SANAJT VS	BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.4.11 (Mingw32)
END PGP PUBLIC KEY BLOCK	mQG18E6FtdwRBACVKA5GKeGvxhj4tB0/vyT6AY4bfax]JvyStq+j35e5HzyV+hvL Le2wJ5s+P2e1y1pf2atwE/krmKVZFMwJ8AF647mo5qNh3tmv6qP4KsUdDF1drVX vsdTaw9Hx3fcn825YA369KVHH05W18KVZY5WyU0UcCsmU10y1X3rywGdYT1 tgFY7KpnL/bvBgvJ+qq7KXDD/iX1NV91IZzCURSU2YPEKmHb0GVh+krE5cw12ff0 vyU1g28Zv1kg0P4g7KXDD/iX1NV91IZzCURSU2YPEKmHb0GVh+krE5cw12ff0 vohpA/4p+Xig50v6Rj8KoThyXtn0af;FVvC1pytGHRKWna7UzCQ0qXk0714Es6 GMwe2zmvu03L91b2/TGkc08hL4r0mwZvb0kb37rmKyDFr4B01GpD1pKxLRUKN7E d1Y0Nja01jHTz20142D5gyj0278AvH0914Y7(3pHm8zovCb04)J4Es6 GMwe2zmvu03L91b2/TGkc08hL4r0mwZvb0kb37rmKyDFr4B01GpD1pKxLRUKN7E Ahsj8gs1CacDaqYcA1JGsFG1DAQT4CH4PHP4K2NV2FtF01BBMRAga18g20hbXc Ahsj8gs1CacDaqYcA1JGsFG1DAQT4CH4PHP4K2NV72GFL0H3D4D4 gqf8X8JuAyaeV95jXBWZ1ACeN1CyWhTbxsUmoxuF11jWcCturE05AQ0Er0MJ3BA fdy7dyNzmf2n69MqxWINYCg0FFL2h4HrPPHk2NVFV7G4DJ1Zd6J5h1XxSG45 fdy7dqVxexrf/Abtc1h6587vp6ddswKk6gQUXm01pv0owJR4pwXKMe3H2doru6Mm sfwxm7ypqY6V/hc/WIn07AjG0c20vUP11pPr14DXNG0HBhEgrq7TBtF0N0xfhTm sfwxm7ypqY6V/hc/WIn07AjG0c20vUP11pPr14DXNG0HBhEgrq7TBtF0N0xfhTm sfwxm7ypqY6V/hc/WIn07AjG0c20vUP11bpr14DXNG0HBhEgrq7TBtF0N0xfhTm sfwxm7ypqY6V/hc/WIn07AjG0c20vUP11bpr14DXNG0HBhEgrq7TBtF0N0xfhTm sfwxm7ypqY6V/hc/WIN07AjB9YCH1B9YKAJ3BMJ2AJ2B0J0hbxcAhsMAA0EJ/VGHB
	END PGP PUBLIC KEY BLOCK

A questo punto potete trasferire su un memory stick esterno la coppia di chiavi che avete appena salvato per sicurezza, e potete anche inviare via mail ai vostri corrispondenti il file relativo alla chiave pubblica, perche' solo da quel momento loro potranno finalmente inviarvi messaggi e file crittografati.

Come utilizziamo le chiavi pubbliche dei nostri amici?

Cosi' come noi invieremo ai nostri amici la chiave pubblica che ci siamo appena preparati al paragrafo precedente, anche loro faranno la stessa cosa! Immaginiamo che il nostro amico Mario ci abbia inviato una mail con allegata la sua chiave pubblica nel file "**public key mario.asc**". Come prima cosa noi salveremo il file sul nostro disco, e poi per poter utilizzare la chiave per crittografare messaggi, dovremo importarla dentro Cryptophane. L'importazione e' un processo molto simile alla esportazione, infatti bastera' andare nel menu **file** e scegliere **Import keys** come mostrato:

File)		
	Encrypt	Ctrl+E	
	Sign		
	Encrypt and Sign	Ctrl+S	
	Decrypt	Ctrl+D	
	Verify Signature	Ctrl+V	
	Message	Ctrl+M	
	Import Keys		Þ
	Export Public Keys		
	Export Secret Keys		
	Evit	Ctrl+0	

Si aprira' una ulteriore finestra in cui dovete localizzare il file della chiave pubblica che vi ha spedito Mario.



A questo punto vi bastera' selezionare il file e cliccare su Open per importare la chiave:



Notate che nei dettagli della chiave leggiamo anche l'indirizzo email di Mario per il quale la chiave e' stata creata. Ora troveremo elencata la nuova chiave di Mario tra le chiavi pubbliche disponibili in Cryptophane.

Name	E-mail	Trust	Sias	Created	Expires	Kev ID	_
⊢Mario Rossi	mario@prova.it		1	2011-09-30		82A9A71F	
Paolo Lombardi	paololombardi. it@gmail.com	Ultimate	1	2011-09-30		019E1B40	

Anche noi siamo elencati nella lista delle chiavi pubbliche perche'anche noi siamo dei possibili destinatari di messaggi di posta crittografata. In parole semplici, quando noi crittograferemo un messaggio, dobbiamo scegliere quali chiavi pubbliche utilizzare perche' solo le corrispondenti chiavi private potranno decodificare il messaggio; ne viene che se codifichiamo un messaggio per Mario usando solo la sua chiave pubblica, una volta codificato noi stessi non saremo piu' in grado di decodificarlo indietro! Per permettere questo, dovremo codificare il messaggio per Mario usando sia la sua chiave pubblica e' presente nell'elenco delle chiavi pubbliche installate in Cryptophane che e' infatti l'elenco delle chiavi per le quali noi possiamo codificare un messaggio.

Nota che per visualizzare le nostre chiavi segrete installate in Cryptophane (chiaramente una per ciascun indirizzo email per cui abbiamo creato una coppia di chiavi), e' sufficiente andare nel menu **View** e scegliere **Secret Keys**.

View	/	
	Folders	
\checkmark	Expired Keys	
	Comments	
✓	Hints	
•	Public Keys	
	Secret Keys	
	Icons	
۲	Details	
	Refresh	F5

Come garantiamo una chiave?

Ora che abbiamo ricevuto e installato la chiave pubblica di Mario, dobbiamo garantire a Cryptophane che quella chiave e' proprio quella di Mario. Questa procedura che si chiama "Trust" consiste in pochi semplici passaggi: nella finestra principale di Cryptophane fate un click sulla chiave pubblica di Mario in modo che sia evidenziata, poi dal menu **Keys** scegliete **Sign Selected Key**.

	Keys
	Properties of Selected Key
<	Sign Selected Key
	Edit Trust of Selected Key
	Delete Selected Key
	Generate Revocation Certificate for Selected Key
	Search Keyserver
	Get Key from Keyserver
	Refresh from Keyserver
	Send to Keyserver
	Generate Secret Key

Si aprira' una finestra in cui vi viene chiesto di garantire che il Fingerprint (spiego piu' avanti nel manuale il perche' di questa richiesta) della chiave pubblica di Mario e' proprio di Mario, e una volta attivato il segno di spunta nel box "I have checked the above fingerprint..." dovete semplicemente cliccare sul pulsante I am Positive e poi inserire la vostra passphrase.

signitey		
You are about to sign the	key:	
Mario Rossi <mario ID 82A9A71F</mario 	@prova.it>	
Fingerprint D385 716C	AEBC 46A7 9DBF 801E 3F92 5D51 82A	9A71F
Sign key with secret key:	Paolo Lombardi <paololombardi.it@gma< td=""><td>ail.com></td></paololombardi.it@gma<>	ail.com>
	ID 9FD51A7E019E1B40 (created 2011-	09-30)
By signing this key, you ar completely sure that this k	e testifying to the entire cryptographic cor ey belongs to the person indicated in the	mmunity that you are key name above.
You can be certain by cor to read out their key's fing	ntacting the key owner by phone or in per erprint. If it is the same as above, the key	son and getting them is the same.
T I have checked th	e above fingerprint with the key owner an	d they match.
Lam POSITIVE that thi	s key belongs to its indicated owner	Cancel

Si aprira' una finestra di conferma che tuttavia, per via di un baco del programma, mostra l'icona e il titolo di errore.



Come crittografiamo una mail?

Supponiamo che vogliate scrivere un messaggio crittografato per Mario. Dal menu File di Cryptophane, scegliete Message



Si aprira' una finestra in cui potete scrivere direttamente o incollare il vostro messaggio. Osservate che il testo qui non e' formattabile cioe' grassetto, corsivo, dimensione del carattere, font, colore del carattere, etc. sono tutte caratteristiche che vanno perse. In caso vogliate inviare un testo formattato, allora dovete scriverlo in Word, ad esempio, salvare tale testo come un file, e quindi inviare il file come allegato crittografato in un modo che vedremo a seguire. Ora voglio mostrarvi come inviare un semplice testo.

🕄 Enter Message	23
Copy and paste the message to encrypt, decrypt, sign or verify below:	
Qui possiamo scrivere direttamente, oppure incollare, il messaggio che intendiamo crittografare. Una volta completato, possiamo cliccare su OK	
<u> </u>	<u>C</u> ancel

Una volta scritto o incollato il testo che volete inviare a Mario, cliccate su Ok e si aprira' una finestra in cui dovrete selezionare le chiavi pubbliche per le quali volete crittografare il messaggio, e chiaramente avrete a disposizione le sole chiavi elencate precedentemente nella finestra di Cryptophane.

Dutput into file: C:\Users\PLOMBA~1\AppData Encrypt with shared passphrase (symmetric encr Encrypt with public kay Encrypting your data will ensure only the recipients of	NLocal\Temp\CryE5	7C.tmp data.
Filter	I Allo	w untrusted recipie
User ID	Key ID	Created
	82A9A71F	2011-09-3
Mario Rossi (mario@prova.it) Paolo Lombardi (paololombardi.it@gmail.com)	019E1B40	2011-09-3
Mario Rossi (mario@prova.it> Paolo Lombardi (paololombardi it@gmail.com>	019E1B40	2011-09-30
M Mario Rossi (mario@prova.tb) Paolo Lombardi (paololombardi i@gmail.com) ∢	019E1B40	2011-09-3
Mario Rossi (mario@prova.tb) Paolo Lombardi (paololombardi ik@gmail.com) * [019E1B40	2011-09-30 was not tampered
M Mario Rossi (mario@prova.it) Paolo Lombardi (paololombardi #@gmail.com) (Sigm with secret key Signing your data allows your recipients to verify the Sigm with private key. Paolo Lombardi (paololombardi)	data came from you and ardii@gmail.com>	2011-09-34 was not tampered
Mario Rossi (mario@prova.it) Paolo Lombardi (paololombardi #@gmail.com) Guide the secret key Signing your data allows your recipients to verify the Sign with private key: Paolo Lombardi (spaololomb C Uptut file contains gata and signature	data came from you and	2011-09-31 was not tampered

Selezionate la chiave di Mario e la vostra chiave (altrimenti, come gia' spiegato, non potrete piu' decodificare indietro il messaggio che avete voi stessi inviato!) e poi cliccate su Ok.

In caso non abbiate garantito la chiave pubblica di Mario oppure non vogliate farlo, allora dovete sempre tenere abilitato il segno di spunta "Allow Untrusted Recipients".

La finestra dove avete scritto il messaggio,ora conterra' la sua versione crittografata che voi potete copiare e incollare in una mail per Mario oppure potete salvare su file cliccando sul pulsante **Save to File** e quindi inviare il file in allegato a Mario.

G Output		23
Comparing States and		ш
Save to File The above data has been copied to the clipboard.	<u>0</u> K	•

Nota che per crittografare un file anziche' una messaggio di testo, la procedura e' molto simile, semplicemente dovete cliccare sul comando **Encrypt** nel menu **File** di Cryptophane.

Come decrittografiamo una mail?

Supponiamo che abbiate ricevuto una email da Mario in cui una parte del testo sia un messaggio crittografato. Innanzitutto selezionate tutto il testo crittografato e copiatelo negli appunti (CTRL+C) poi dal menu File di Cryptophane, scegliete Message

	File)		_
		Encrypt	Ctrl+E	
		Sign		
		Encrypt and Sign	Ctrl+S	
		Decrypt	Ctrl+D	
		Verify Signature	Ctrl+V	
<		Message	Ctrl+M	5
<		Message Import Keys	Ctrl+M	>
<		Message Import Keys Export Public Keys	Ctrl+M	
<		Message Import Keys Export Public Keys Export Secret Keys	Ctrl+M	

Si aprira' una finestra in cui potete incollare (CTRL+V) il testo crittografato da Mario, e quindi premendo Ok vi verra' richiesta di inserire la passphrase della vostra chiave pubblica:

Enter Passphrase	X
Enter passphrase for user: Paolo Lombardi <paololomba ID 019E1B40 (created 2011-09-30</paololomba 	rdi.it@gmail.com>))
]	<u>D</u> K <u>C</u> ancel

Se inserite la passphrase correttamente, la finestra precedente ora conterra' il messaggio di Mario perfettamente leggibile. Nota che per decrittografare un file anziche' una messaggio di testo, la procedura e' molto simile, semplicemente dovete cliccare sul comando **Decrypt** nel menu **File** di Cryptophane.

Come autentichiamo una mail?

La procedura per firmare una mail e' molto simile a quella per crittografarla, cambia solo dove mettiamo il segno di spunta nella finestra di scelta delle chiavi pubbliche.

	Local\Temp\Cry79	7.tmp	
Output into file: C:\Users\PLOMBA~1\AppData\	Local\Temp\Cry7A	8.tmp	
Encrypt with shared passphrase (symmetric encrypt	tion)		
Encrypt with public key			
Encrypting your data will ensure only the recipients che	cked below can read	the data.	
Filter	E Allo	w untrusted recipie	nts
User ID	Key ID	Created	1
Mario Rossi <mario@prova.it></mario@prova.it>	82A9A71F	2011-09-30	_
Paolo Lombardi (paololombardi it@gmail.com)	019E1B40	2011-09-30	
			Þ
Sign with secret key			•
Signing your data allows your recipients to verify the data	ata came from you and	was not tampered	• ∧vitl
Your contracts spectral and spectral an	ata came from you and di.it@gmail.com>	was not tampered	► witt
Sign with secret key Signing your data allows your recipients to verify the da Sign with private key: Paolo Lombard spaolombar Output life contains gata and signature	tta came from you and di.it@gmail.com>	was not tampered 019E1	► witi
Sign with secret key Sign with secret key Sign with private key. Paolo Lombard' (paolombard Output file contains plaintext data and signature Output file contains plaintext data and signature	ata came from you and di it@gmail.com>	was not tampered 019E1 created 2011-05	► witt ■ 34(-30

La firma (in inglese **Signature**) di un messaggio di testo e' un blocco di caratteri speciali che viene aggiunto in fondo al messaggio il quale resta perfettamente leggibile (per questo si dice "firma in chiaro").

Tale blocco di caratteri speciali viene calcolato da Cryptophane in funzione della nostra chiave segreta e dei caratteri che compongono il messaggio originale. In caso anche un solo carattere del messaggio originale cambiasse, anche un solo spazio venisse aggiunto, Cryptophane calcolerebbe un blocco di caratteri speciali diverso dal precedente.

Quando uno riceve un messaggio autenticato (o firmato), Cryptophane non fa altro che verificare la corrispondenza biunivoca tra messaggio originale e caratteri speciali e ci garantisce che tale messaggio non e' stato alterato in alcun modo.

Un esempio di messaggio "firmato in chiaro" con PGP potrebbe essere il seguente:

```
-----BEGIN PGP SIGNED MESSAGE-----
Ciao Mario,
Ho firmato questo messaggio cosi' puoi verificare che l'ho scritto io e
non e' stato modificato da nessuno!
Ti saluto!
Paolo
-----BEGIN PGP SIGNATURE-----
iQA/AwUBNr84La1N2hTAk0JyEQIIFQCgi7JsVwZ/5TAZK/9cWGxu/uUWOBcAmwTA
pTIY3wiNKqPWMflTir+yzyz+ =kxr6
-----END PGP SIGNATURE-----
```

Cosa sono i Keyservers?

I keyservers sono dei database di chiavi pubbliche accessibili a tutti al fine di aggiungere la propria chiave o di trovare quella di un utente. Sono come una sorta di pagine gialle delle chiavi pubbliche dove chiunque può andare e cercare la chiave pubblica di Mario Rossi e, a patto che il signor Rossi l'abbia spedita al keyserver precedentemente.

Inviare la propria chiave a un keyserver e'molto semplice, e' sufficiente cliccare su "**Send to keyserver**" dal menù **Keys** di Cryptophane. Con altrettanta semplicita' e' possibile cercare la chiave pubblica di un utente, incollo senza spiegarla la finestra che compare selezionando "**Search keyserver**" sempre dal menu **Key**

G Search Keysen	/er			
Search keyserver for key	pgp.mit.edu			▼ <u>S</u> earch
User ID		Crea	red Key ID	Туре
Add Selected K	(eys			<u>C</u> lose

Che cosa e' il Fingerprint di una chiave?

Il fingerprint e' una sequenza di 32 cifre ricavate dalla chiave pubblica e che la identifica in modo univoco.

Doppiocliccando su una chiave nella finestra principale di Cryptophane, si apre una finestra che mostra le proprieta' della chiave stessa, tra cui il fingerprint.

Incollo a seguire un esempio di tale finestra delle proprieta':

Paolo Lombardi	8			
Paolo Lombardi <paololombardi.it@gmail.com></paololombardi.it@gmail.com>				
 Fingerprint: 00CC C97A A299 BC7B 2074 26A7 9FD5 1A7E 019E 1B40 Key ID: 019E1840 Key uses: Signing Key top: Public Primary Key Key approximation 2014 th D5A Created: 2011-09-30 User trust: Ultimate Exprise: (no expity) Calculated trust: Ultimate				
Signatures:				
Paolo Lombardi paololombardi #@gmail.com 019E1B40				
Sub keys:				
Key Type Key ID				
Public Secondary Key 1024 bit ElGamal 93BEE4BF				
	e			

A cosa serve il fingerprint?

Serve perche' quando Mario ci ha spedito via mail la sua chiave pubblica e noi l'abbiamo aggiunta al nostro Cryptophane, ancora non siamo sicuri che sia la chiave effettivamente di Mario perche' qualcuno avrebbe potuto sostituire la chiave allegata alla mail di Mario lungo il tragitto (abbiamo gia' detto che la posta elettronica e' intrinsecamente insicura).

Per fare questa verifica ci bastera' telefonare a Mario e chiedergli il fingerprint della sua chiave, in modo che se coincide con quello della chiave che abbiamo ricevuto via mail, allora siamo certi che quella e' veramente la sua chiave, e possiamo cosi' alzare il livello di Trust come visto precedentemente in questo manuale.