Pretty Good Privacy

A cura di: *Sabarese Maria*
&
Scarano Gerardo

Corso di Sicurezza su reti 1999/2000
Prof. Alfredo De Santis

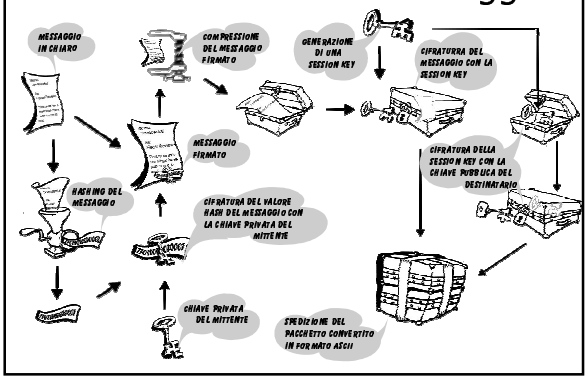
PGP: cos'è

- È un software di crittografia per la posta elettronica e la protezione dei file di uso personale.
- Creato e distribuito gratuitamente su Internet nel 1991, si è diffuso in tutto il pianeta.
- Oggi è diventato il software di crittografia per la posta elettronica più usato nel mondo.

PGP: cosa fa

- Permette di firmare una E-mail lasciando il testo in chiaro, oppure cifrarla senza firmarla, o fare tutte e due le cose insieme.
- Supporta funzioni di gestione di un disco virtuale cifrato (*PGP-disk*)
- Garantisce lo scambio di dati in maniera sicura su un canale insicuro (*PGP-vpn*)

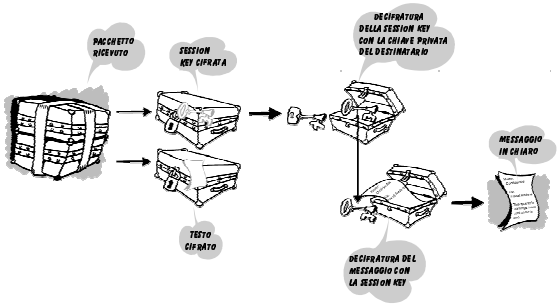
PGP: mandare un messaggio



PGP: un esempio

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.3 for non-commercial use
/K8xfzpEDp19J3tkItAjbBJstoXp18mAkKjX4t7eRdefXUkk+/lP
pclJc8zgH/1mBkQhVlwheylkGjqflOqe4/l6t7QZNtArJNVP/se
DiYRFtC+duJme+pGMw68sn8myKFXGktDIR0FNjiGk4JJyno
QHo21+mUQxaC2TiknYlaV+zEIHamuSfQu4y57oggFOSAog
mgar66psSoaMJFVEafUWd7lbnDvnkyHPZri7JpXblFFVxpqb
QRhvWkQVMy5JqoFCEuft080xYbdFAW2ymzgkbpo2BalCE
PLiRIQfE6y4L41nVhzlxnMKdhxmJ4VGqVhKqakVnd8UhsPv
515QfWoZAFuHa4YbL6bdXi3ZSY1XqtmnwRaWnVupK/Z6P
K+4gCrO9m0JQ6JnRRY+eY1+uygxm64XHTaCSfhW2rac2B
hsfJGqWdu8AlClplTeMFsY3wyzgJjbuenN9CtwiJAEYEGBE
CAAYFAjcXkTcACgkQluhy1aq5NlailQCcCquPR1Hfl5QvHjA
67mBvqCXTVuoAnAoTl/gqVOy2VezwHWO4pH3elJ5/=8kKG
-----END PGP MESSAGE-----

PGP: leggere un messaggio



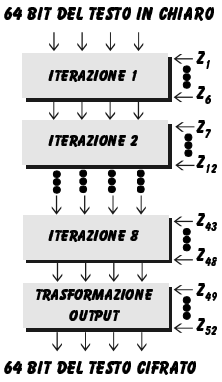
PGP: Un collage di algoritmi

Funzione	Algoritmi usati	Descrizione sintetica
Cifratura del messaggio	CAST,IDEA 3DES	Il messaggio è cifrato con un algoritmo a chiave simmetrica usando una session key generata dal mittente.
Scambio della session key	DH, RSA	La session key è cifrata con la chiave pubblica del destinatario
Firma digitale	RSA, MD5, SHA, DSS	Viene creato un codice hash di un messaggio che viene cifrato usando RSA con la chiave privata del mittente
Compressione	ZIP	Un messaggio è compresso per la memorizzazione e la trasmissione usando ZIP
Compatibilità e-mail	Conversione Radix-64	Un messaggio cifrato è convertito in una stringa ASCII usando la conversione Radix-64 per fornire trasparenza alle applicazioni e-mail
Segmentazione	Radix-64	PGP esegue la segmentazione e il riassemblaggio qualora la dimensione del messaggio sia proibitiva

Cast, Idea e 3-Des

- Operano su blocchi di 64 bit in modalità CFB
- CAST e IDEA hanno la taglia delle chiavi di 128 bit, quindi più resistenti agli attacchi a forza bruta, rispetto a Triple-Des che usa due chiavi a 56 bit
- CAST, usato per default, perché è veloce e **free**
- IDEA, preferito al 3-DES perché quest'ultimo viola le leggi sull'esportazione

Idea: struttura dell'algoritmo…



Idea: singola iterazione

Input 4 sottoblocchi di 16 bit e 6 sottochiavi

Output 4 sottoblocchi

Operazioni eseguite

moltiplicazione modulo $2^{16}+1$

addizione senza riporto modulo 2^{16}

or esclusivo

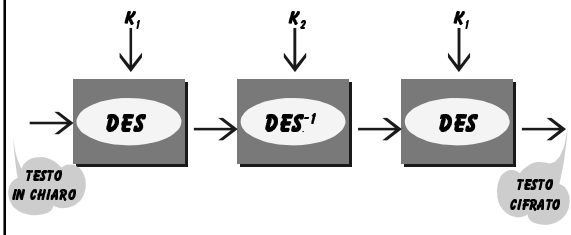
Idea: singola iterazione

Operazioni eseguite

- trasformazione che combina i 4 sottoblocchi in input con 4 sottochiavi per avere altri 4 sottoblocchi
- combinazione dei 4 sottoblocchi in input con l'or esclusivo per avere 2 sottoblocchi moltiplicati e addizionati con le altre 2 sottochiavi
- or-esclusivo dei 4 sottoblocchi della prima trasformazione con i 2 ottenuti dalla seconda.

Vantaggi trasformazione complessa dell'input che rende difficile la crittoanalisi.

3-Des



Vantaggi maggiore sicurezza

Svantaggi è meno efficiente del DES

Protocollo per lo scambio di chiavi Diffie-Hellman

- Lo scopo di questo algoritmo è quello di permettere a due utenti di scambiare una chiave in modo sicuro.
- La sicurezza di questo algoritmo è fondata sulla difficoltà di calcolare logaritmi discreti.
- Esistono due elementi pubblici comuni
  - q *numero primo*
  - α *radice primitiva di* Z_q^*

Diffie-Hellman:un esempio -1

Scambio di chiavi tra A e B:

Generazione delle chiavi di A

Selezione di un intero $X_A<q$ (X_A=chiave privata di A)

Generazione di $Y_A=\alpha^{X_A} \textit{ mod } q$ (Y_A=chiave pubblica di A)

Generazione delle chiavi di B

Selezione di un intero $X_B<q$ (X_B=chiave privata di B)

Generazione di $Y_B=\alpha^{X_B} \textit{ mod } q$ (Y_B=chiave pubblica di B)

Diffie-Hellman:un esempio -2

Scambio delle chiavi pubbliche tra A e B

$Y_A \leftrightarrows Y_B$

Calcolo della chiave comune da parte di A

$K = (Y_B)^{X_A} \textit{ mod } q$

Calcolo della chiave comune da parte di B

$K = (Y_A)^{X_B} \textit{ mod } q$

Diffie-Hellman: prova di correttezza

Proviamo che i calcoli di A e B producono lo stesso risultato:

$K = (Y_B)^{X_A} \textit{ mod } q$

$= (\alpha^{X_B} \textit{ mod } q)^{X_A} \textit{ mod } q$

$= (\alpha^{X_B})^{X_A} \textit{ mod } q$

$= \alpha^{X_B X_A} \textit{ mod } q$

$= (\alpha^{X_A})^{X_B} \textit{ mod } q$

$= (\alpha^{X_A} \textit{ mod } q)^{X_B} \textit{ mod } q$

$= (Y_A)^{X_B} \textit{ mod } q$

RSA: per cifrare

Utilizza una chiave pubblica *(e,n)* e una chiave privata *(d,n) dove*:

'n=pq', con 'p' e 'q' interi primi molto grandi, '*e*' e '*d*' sono calcolati come segue: $ed \equiv 1 \bmod [(p-1)(q-1)]$

Es.:

C	messaggio in chiaro
$P=C^e \bmod [(p-1)(q-1)]$	cifratura del messaggio
$S=P^d \bmod [(p-1)(q-1)]$	decifratura del messaggio

otteniamo S=C

RSA: per firmare

(E,N)=CHIAVE PUBBLICA
(D,N)=CHIAVE PRIVATA

C	messaggio in chiaro
H=hash(C)	hash del messaggio
$P=H^d \bmod [(p-1)(q-1)]$	valore hash cifrato
F=P||C	messaggio firmato
$S=P^e \bmod [(p-1)(q-1)]$	

se S=hash(C) allora è verificata l'autenticità del messaggio

DSS

- E' basato sulla difficoltà di calcolare logaritmi discreti.
- Fa uso di una funzione hash
- I parametri pubblici usati sono:
  - *P* numero primo compreso in $[2^{L-1},2^{L}]$
  - *G* divisore primo di P-1 compreso in $[2^{159},2^{160}]$
  - $Q=H^{(P-1)/Q}$ mod P con H compreso in [1,P-1]
- Numero segreto K compreso in (0,q)

Chiave privata **X** — INTERO CASUALE COMPRESO IN (0,Q)

Chiave pubblica **Y** — $Y= G^{x}$ MOD P

DSS, firma e verifica

Per *firmare* un messaggio M sono eseguiti i passi seguenti:

- $r=(G^{k} \bmod P) \bmod Q$
- $s=(k^{-1}(H(M)+xr)) \bmod Q$
- firma=(r,s)

H(M) GENERA IL CODICE HASH DI M

Per eseguire la verifica sono eseguiti i passi seguenti:

- $w=s^{-1} \bmod Q$
- $u_1=(H(M)w) \bmod Q$ $\quad u_2=rw \bmod Q$
- $v=((G^{u_1}y^{u_2}) \bmod P) \bmod Q$
- Verifica che sia valida la relazione v=r

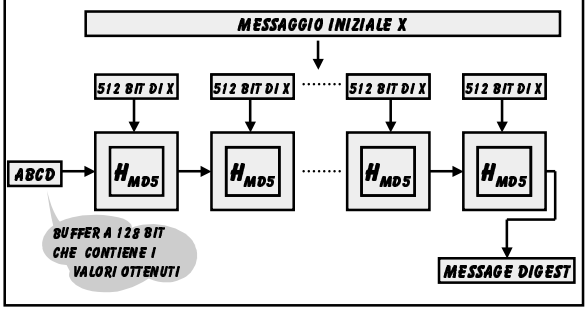
Firma: quando

La firma è eseguita prima della compressione per due motivi:

1) Se memorizziamo solo il messaggio, ogni qualvolta viene richiesta la verifica della firma si deve ricomprimere il messaggio per verificarne l'autenticità.
2) Firmando un messaggio compresso si vincolano tutte le implementazioni del PGP ad uno stesso algoritmo di compressione.

MD5

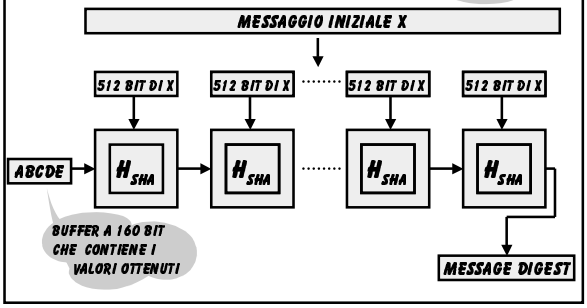
Input testo di lunghezza arbitraria
Output message digest di 128 bit



Secure Hash Algorithm

Input testo di lunghezza arbitraria
Output message digest di 160 bit

USATO NELLE NUOVE VERSIONI DI PGP



Compressione

PGP comprime il testo in chiaro prima di cifrarlo.

Vantaggi

- Risparmio di tempo nella trasmissione
- Aumenta la sicurezza della cifratura
- Crittoanalisi più difficile poiché un messaggio compresso ha meno ridondanza di quello originario.

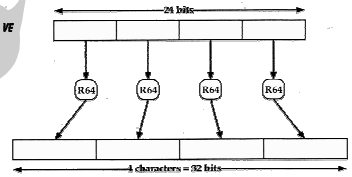
Algoritmo di compressione dati Zip

- PGP comprime secondo la routine freeware ZIP.
- Tale scelta dipende dalla disponibilità del codice sorgente, dalla velocità e dall'ottimo rapporto di compressione.
- PGP non comprime i file già compressi ma segnala ciò alla decifratura.

ASCII Armour Radix-64

- PGP utilizza il formato ASCII RADIX-64 per testi cifrati, poiché alcuni sistemi di posta elettronica gestiscono messaggi soltanto in formato ASCII
- Converte il testo espandendo gruppi di 3 byte in 4 caratteri ASCII

QUESTA ESPANSIONE DI CIRCA IL 33% NON È GRAVE PERCHÉ IL FILE ERA STATO GIÀ COMPRESSO IN MISURA MAGGIORE PRIMA DI ESSERE CIFRATO.



Segmentazione

- La maggior parte dei servizi e-mail su Internet proibisce l'invio di messaggi più lunghi di 50000 o 65000 byte.
- RADIX-64 spezza il messaggio in blocchi sufficientemente piccoli da poter essere spediti separatamente, ponendoli in file con estensione ".as1", ".as2", ".as3", ecc.
- Il compito di concatenare questi file nel giusto ordine in un file più grande è affidato al software del destinatario.

Numeri casuali: Perché?

- Generare le chiavi RSA
- Fornire il valore seme iniziale per il generatore di numeri pseudocasuali
- Fornire un input aggiuntivo durante la generazione del numero pseudocasuale

Numeri casuali: Come?

- Allocazione di un buffer di 256 byte non inizializzato.
- Memorizzazione dell'istante in cui inizia l'attesa per la digitazione di un tasto.
- Memorizzazione dell'istante in cui il tasto è digitato e valore del tasto digitato.
- Cifratura del valore nel buffer con le informazioni precedentemente ricavate.
- Ripetizione delle tre precedenti operazioni per un numero finito di volte.

LE VERSIONI INTEGRATE CON WIN9x MEMORIZZANO LA POSIZIONE E I MOVIMENTI E DEL MOUSE

Numeri pseudocasuali: Perché?

- Per generare la session key.
- Generazione dei vettori di inizializzazione per la cifratura a cipher feedback.

Numeri pseudocasuali: Come?

- L'algoritmo è basato sull'ANSI X9.17
- Prende in input il messaggio e "randseed.bin"
- Usa una chiave a 112 bit e tre applicazioni di 3-DES per un totale di 9 cifrature DES
- Restituisce in output: randseed.bin aggiornato, 16 byte che costituiscono la session key e 8 byte che sono il vettore di inizializzazione

E' IL FILE DI SEME USATO DA PGP

ALCUNE VERSIONI USANO IDEA

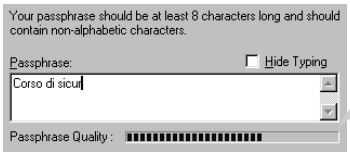
Generazione delle chiavi

- PGP offre la possibilità di scegliere fra diversi formati possibili, fino a 2048 bit (RSA) nelle versioni più recenti.
- Il programma chiederà poi di digitare la passphrase al fine di proteggere il keyring privato.
- Tutte le volte che si vorrà usare la chiave segreta bisognerà digitare la passphrase che dovrà essere conservata gelosamente.

UNA PASSPHRASE È LA VERSIONE ESTESA DI UNA PASSWORD, E IN TEORIA, PIÙ SICURA.

Scelta della Passphrase

- La passphrase può contenere spazi, numeri caratteri e punteggiatura, al fine di essere il praticamente impossibile da individuare, con una ricerca esaustiva, ma deve essere facile da ricordare



PGP CALCOLA L'INDICE DI BONTÀ DELLA PASSPHRASE MENTRE SI DIGITA

Attacchi a Forza Bruta

La tabella indica una stima dello sforzo richiesto per fattorizzare alcune chiavi pubbliche generate dal PGP:

1ANNO-MIPS È UN ANNO DI CALCOLO ININTERROTTO CON UNA MACCHINA DELLA POTENZA DI 1 MIPS (ESEGUE 1 MILIONE DI ISTRUZIONI AL SECONDO).

Dimensioni della chiave in bit		Anni MIPS necessari per la fattorizzazione
768	Sicurezza commerciale	200.000.000
1024	Sicurezza alto livello	300.000.000.000
2048	Sicurezza militare	300.000.000.000.000.000.000

Key ring

Il PGP considera due strutture dati per ogni utente:

- *Private Key Ring* usato per memorizzare la coppia di chiavi, pubblica e privata, dell'utente, dove però la chiave privata è cifrata con una passphrase nota solo all'utente.
- *Public Key Ring* Usato per memorizzare le chiavi pubbliche delle persone note all'utente.

Campi del public key ring

L'ORA IN CUI È STATA GENERATA O INSERITA UNA CHIAVE

CHIAVE PUBBLICA

IL PROPRIETARIO DELLA CHIAVE

FIRMA PER LA CHIAVE

Time Stamp	Key ID	Public key	Owner trust	User ID	Key legitimacy	Firma	Signature Trust

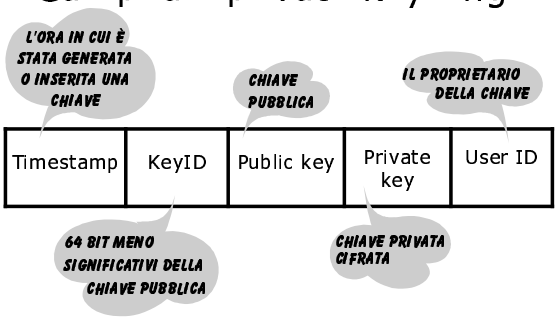
64 BIT MENO SIGNIFICATIVI DELLA CHIAVE PUBBLICA

FIDUCIA NEL PROPRIETARIO DELLA CHIAVE

FIDUCIA NELLA CHIAVE

FIDUCIA NELLA FIRMA

Campi del private key ring



Chiavi pubbliche e keyserver

Per ottenere la chiave pubblica di qualcuno si può chiedere direttamente alla persona interessata…

…oppure si possono usare i *keyserver*.

I keyserver

- Sono particolari server presenti su Internet, dedicati al deposito e al prelievo delle chiavi pubbliche, in rete tra loro, per cui ogni chiave immessa in un server viene diffusa anche sugli altri.
- Per ricevere o inserire chiavi bisogna inviare un'e-mail all'indirizzo del keyserver.

Revocare una chiave

- Se le chiavi fossero compromesse bisognerebbe generare un certificato di "chiave compromessa" per avvisare che la chiave pubblica non è più valida.
- Questo certificato è firmato con la chiave che si vuole revocare. Il PGP installerà il certificato nel Keyring di chiunque lo riceva impedendo l'uso della chiave compromessa.

Web of trust: Cos'è?

- PGP si basa su una gestione decentralizzata, in cui ciascuno si rende responsabile certificando una firma o un'altra.
- Non bisognerebbe mai certificare una chiave di cui non si è perfettamente sicuri perché se fosse fasulla si comprometterebbe la "**ragnatela di fiducia**" (**Web of trust**) che PGP mira a creare.

Web of trust: Come funziona?

Quando una nuova chiave entra nel keyring si calcola il campo *key legitimacy*….

Time Stamp	Key ID	Public key	Owner trust	User ID	Key legiti macy	Firma	Sign ature Trust

…in base ai valori dei campi signature trust delle persone che hanno firmato questa chiave.

Web of trust: Come funziona?

Quando una nuova chiave entra nel keyring si calcola il campo *key legitimacy*….

PGP chiede all'utente di inserire due valori x e y….

…calcola la somma pesata dei valori di trust assegnando 1/x alle firme fidate e 1/y a quelle non note.

Web of trust: Come funziona?

- se il totale delle somme pesate è 1
- se almeno una firma è completamente fidata

ALLORA

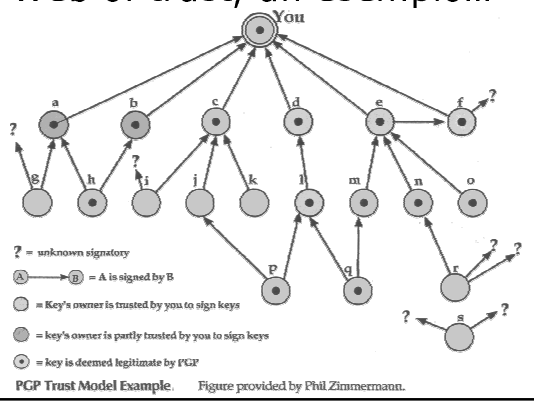
- Il valore del campo key legitimacy viene posto pari a 1

Time Stamp	Key ID	Public key	Owner trust	User ID	**1**	Firma	Sign ature Trust

Livelli di trust

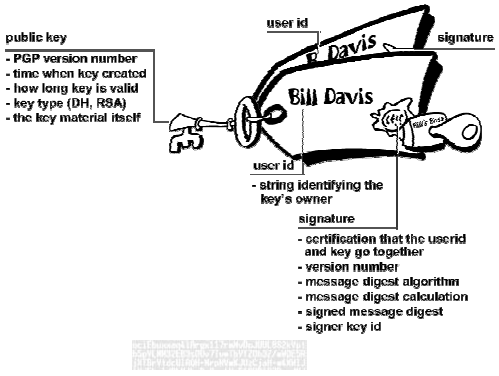
- Ci sono quattro livelli di fiducia che si possono assegnare alla chiave pubblica in un key ring:
  - o *Completamente fidato*
  - o *Parzialmente fidato*
  - o *Non fidato*
  - o *Non noto*
- Tutte le chiavi firmate con la propria chiave sono valide.

Web of trust, un esempio…



PGP Trust Model Example. Figure provided by Phil Zimmermann.

Struttura di un certificato



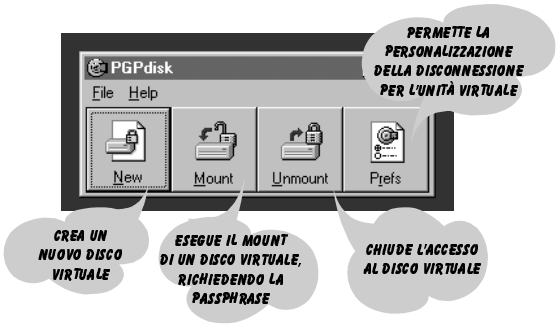
PGP: cosa fa

- Permette di firmare una E-mail lasciando il testo in chiaro, oppure cifrarla senza firmarla, o fare tutte e due le cose insieme.
- Supporta funzioni di gestione di un disco virtuale cifrato (PGP-disk)
- Garantisce lo scambio di dati in maniera sicura su un canale insicuro (PGP-vpn)

PGPdisk: cos'è?

- Riserva una parte del disco alle informazioni private creando un file cifrato con le funzioni di un disco virtuale.
- Per accedere a queste informazioni bisogna eseguire il mount.
- Tutti i dati e le applicazioni sono inaccessibili a meno che non si conosca la passphrase.

PGPdisk: che faccia ha?



PGP: cosa fa

- Permette di firmare una E-mail lasciando il testo in chiaro, oppure cifrarla senza firmarla, o fare tutte e due le cose insieme.
- Supporta funzioni di gestione di un disco virtuale cifrato (PGP-disk)
- Garantisce lo scambio di dati in maniera sicura su un canale insicuro (PGP-vpn)

PGP-vpn: cos'è?

Virtual Private Networks (VPN) consente la trasmissione sicura di informazioni su Internet.

- Estende il concetto di *intranet* (internal network) o macchina individuale attraverso Internet, creando un *tunnel* privato e personale.
- Usa un "tunneling protocol" e la cifratura per proteggere i dati dal momento in cui lasciano il mittente al momento in cui arrivano al destinatario

PGP: sul tuo desktop

PGP:come funziona

ANCHE SE LE VERSIONI PIÙ RECENTI SONO INTEGRATE CON WINDOWS SUPPORTANO COMUNQUE L'UTILIZZO A RIGA DI COMANDO

```
Pretty Good Privacy(tm) Version 6.5.2
(c) 1999 Network Associates Inc.
Uses the BSafe(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.


Usage summary:
To encrypt a plaintext file with recipent's public key, type:
   pgp -e textfile her_userid [other userids] (produces textfile.pgp)
To sign a plaintext file with your secret key:
   pgp -s textfile [-u your_userid]          (produces textfile.pgp)
To sign a plaintext file with your secret key, and then encrypt it
   with recipent's public key, producing a .pgp file:
   pgp -es textfile her_userid [other userids] [-u your_userid]
To encrypt with conventional encryption only:
   pgp -c textfile
To decrypt or check a signature for a ciphertext (.pgp) file:
   pgp ciphertextfile [plaintextfile]
To produce output in ASCII for email, add the -a option to other options.
To generate your own unique public/secret key pair:   pgp -kg
For help on other key management functions, type:    pgp -k
For help on group management functions, type:    pgp -g


C:\Programmi\Network Associates\PGP>_
```

Legge USA sui prodotti crittografici: Settembre 1998

Da gennaio 1999 è possibile esportare liberamente:

- algoritmi di cifratura simmetrica (DES, CAST, ecc.) con chiave fino a 56 bit;
- algoritmi simmetrici per lo scambio di chiavi con chiavi fino a 112 bit;
- algoritmi asimmetrici per lo scambio di chiavi con chiavi fino a 1024 bit.

Legge USA sui prodotti crittografici: 14 Gennaio 2000 1/3

- Prodotti crittografici con chiavi di lunghezza qualsiasi, possono essere esportati liberamente **senza licenza** verso qualunque stato tranne Cuba, Iran, Iraq, Libia, Sudan, Syria e Corea del Nord.
- Le telecomunicazioni e gli Internet provider possono usare ogni prodotto crittografico senza licenza per fornire servizi di cifratura, invece, per le agenzie governative è necessaria una licenza.

Legge USA sui prodotti crittografici: 14 Gennaio 2000 2/3

- BXA dovrà classificare i prodotti *già precedentemente esportati, ed ora modificati* revisionando la loro funzionalità.
- Il codice sorgente disponibile al pubblico, e per il quale non è necessario alcun pagamento per la licenza, può essere esportato senza revisioni tecniche.
- Tutti gli altri tipi di codice sorgente possono essere esportati dopo una revisione tecnica.

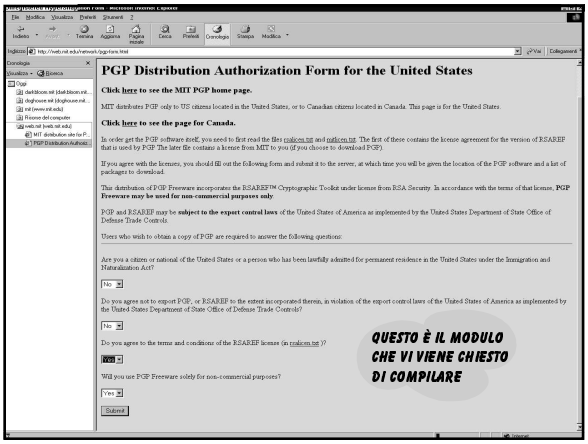
Legge USA sui prodotti crittografici: 14 Gennaio 2000 3/3

- Coloro i quali esportano prodotti crittografici devono presentare all'amministrazione del BXA una copia del codice sorgente.
- Coloro i quali esportano devono dare informazioni generali sui prodotti stranieri sviluppati per la vendita commerciale usando codice sorgente commerciale
- I prodotti stranieri sviluppati usando codice sorgente di origine americana non necessitano di autorizzazione per l'esportazione.

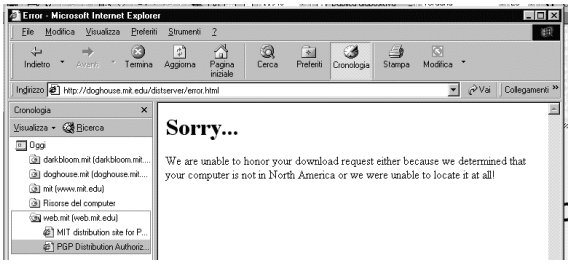
Dove trovare il PGP

Tutte le versioni di PGPi si possono trovare all'indirizzo: www.pgpi.com

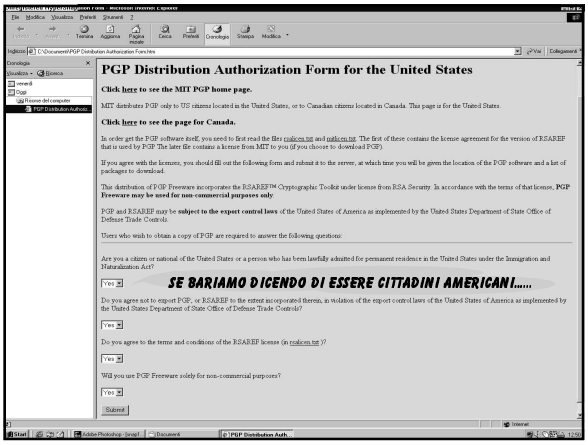
Alla luce della nuova legislatura ***sarebbe*** possibile scaricare la versione PGP6.x dal *MIT distribution site for PGP* all'indirizzo: www.mit.edu/network/pgp.htm

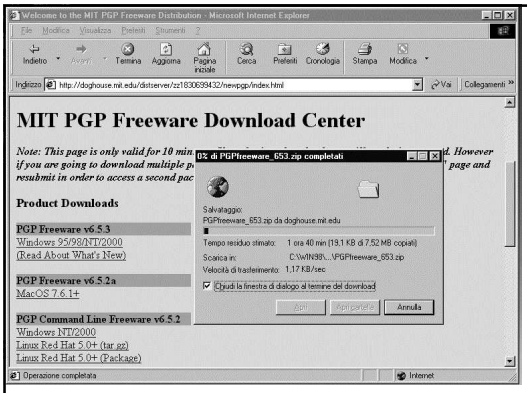


OK Proviamoci!



Ecco cosa vi appare se tentate di scaricare il PGP dal MIT. *MA...*





... e poi dicono che gli americani non sono svegli!!!

Quale versione scegliere -1

- *PGP 2.3a* E' la versione classica di PGP, usata fino al 1998. Non supporta chiavi più lunghe di 1280 bit e può dare problemi se usata con file cifrati con le versioni più recenti.
- *MIT PGP 2.6.2* E' la versione "US-Only", rilasciata e distribuita dal MIT. Queste le sue restrizioni:
  - o Genera messaggi non leggibili dalle versioni precedenti alla 2.5
  - oUsa le librerie RSAREF per la crittografia a chiave pubblica protette da brevetto negli Stati Uniti
  - oNon gestisce firme generate da versioni di PGP 2.2 e precedenti

Quale versione scegliere -2

- *PGP 2.6.2g* E' la versione "ribelle" di PGP, supporta chiavi fino a 4096 bit, non usa RSAREF e risolve alcuni problemi della versione 2.6.2

G STA PER "GUERRILLA"

- *PGP 2.6.3i* Per tutti coloro che *non* risiedono negli USA è universalmente considerata sicura oltre che legale, di Stale Schumacher. E' basata sul codice sorgente della MIT PGP 2.6.2 e modificata per l'uso internazionale. Le differenze sono:
  - o non usa le librerie RSAREF
  - o è compatibile con tutte le versioni precedenti
  - o corregge alcuni problemi della versione 2.6.2

I STA PER "INTERNAZIONALE"

È LA PRIMA ESPORTATA IN MANIERA LEGALE DAGLI STATI UNITI IL CODICE SORGENTE DI È STATO ESPORTATO COME LIBRO, SENZA INFRANGERE ALCUNA RESTRIZIONE CONTENUTA NELLE LEGGI SULLA ESPORTAZIONE

Quale versione scegliere -3

- *PGP 5.0* Rappresenta una nuova generazione per PGP. Aggiunge molte nuove caratteristiche, tra le quali il supporto di altri algoritmi di crittografia oltre RSA e IDEA. La 5.0 è la prima versione totalmente integrata con le interfacce grafiche di Windows 95/NT e Macintosh. La versione per Unix è a riga di comando.
- *PGP 5.0i* È l'ultima versione internazionale di PGP consente di gestire le chiavi RSA ma utilizza Diffie-Hellmann e DSS

Quale versione scegliere -4

- *PGP 6.0* Crea chiavi di dimensione minima di 1024 bit, lasciando libera scelta sull'utilizzo di Diffie-hellman/DSS ed RSA e integra, solo nelle versioni commerciali, PGP-disk e PGP-vpn
- *PGP 6.5.3* È l'ultima versione ufficiale scaricabile dal sito del MIT, risolve piccoli bug delle versioni precedenti, PGP-disk e PGP-vpn sono presenti anche nella versione freeware

Intervista a:

Philip Zimmermann

l'ideatore del PGP
Roma, 26/03/1999

http://www.mediamente.rai.it/home/bibliote/intervis/z/zimmermann.htm

Philip Zimmermann

Roma, 26/03/1999

- Lei è il creatore del software PGP. Ci può spiegare che cos'è?

Risposta

PGP significa Pretty Good Privacy. È un software di crittografia per la posta elettronica e la protezione dei file di uso personale. L'ho creato nel 1991 e l'ho mandato gratis su Internet. Si è diffuso in tutto il pianeta e oggi è diventato il software di crittografia per la posta elettronica più usato nel mondo.

Philip Zimmermann

Roma, 26/03/1999

- È possibile rompere il PGP? Quanto ci si metterebbe?

Risposta

C'è sempre la possibilità che magari qualcuno conosca il modo di decifrare senza dover provare tutti i codici possibili. Magari si riesce a trovare dei punti deboli negli algoritmi di crittografia.

Ma gli algoritmi che usiamo col PGP sono i migliori che siano stati pubblicati nelle riviste universitarie sulla crittografia. Sono stati revisionati nella maniera più scrupolosa da molti crittoanalisti; Per provare tutti i codici possibili, ci vorrebbe un tempo più lungo della storia del pianeta Terra usando tutti i computer esistenti al mondo.

Philip Zimmermann

Roma, 26/03/1999

- Lei sta lavorando con una grande società che ha comprato il suo prodotto. Ha paura che il governo si impossessi del suo sistema?

Risposta

Molte persone mi chiedono se il PGP sia un sistema crittografico ancora inattaccabile. Ora che una grossa società ne ha il controllo, molti temono che la sua inattacabilità sia stata compromessa. Dopo tutto quello che ho passato non c'è pericolo che io permetta a qualcuno di compromettere la sicurezza crittografica del PGP.

Philip Zimmermann

Roma, 26/03/1999

- Quali problemi ha avuto con la giustizia americana?

Risposta

Dopo che ebbi pubblicato nel 1991 il PGP, le autorità vollero sapere come avesse potuto uscire dal paese.

La tecnologia di crittografia era considerata allo stesso modo di altre tecnologie militari a meno che non si abbia un permesso speciale dal Governo. Naturalmente io non avevo un permesso speciale.

Philip Zimmermann

Roma, 26/03/1999

- ***Continua***
  Si trattava di software freeware pubblicato all'interno degli Stati Uniti. Ma quando si pubblica qualcosa su Internet è impossibile che rimanga all'interno di un paese. Arriva tranquillamente dappertutto, così le autorità hanno pensato che si trattasse di una violazione delle leggi americane sull'esportazione e la polizia criminale ha condotto indagini per tre anni. Alla fine, dopo centinaia di conferenze-stampa, hanno deciso di chiudere il caso perché sarebbe stato un errore politico perseguirmi per aver pubblicato qualcosa su Internet.

Bibliografia

- W. Stallings, *Network and internetwork security,* Prentice Hall 1995
- B. Scheneier, *Applied cryptography*, Wiley 1996
- J. Nechvaltal, *Public Key cryptography*, IEEE Press 1992
- *PGP User's Guide*, www.ifi.nio.no
- *PGP Documentation*, Network Associates 1999, www.nai.com
- Aggiornamenti e Link da: www.crypto.com, www.crypto.org, www.cdt.org, www.bxa.com.