



CORSO P.G.P. - PRETTY GOOD PRIVACY

Manuali.net è lieta di presentare il corso di **P.G.P. Pretty Good Privacy**.

Come di consueto, in queste pagine troverai tutti i dettagli relativi al programma del corso, al suo docente, alle modalità di presentazione.

Le scadenze:

Data di inizio delle iscrizioni: **1 Aprile 2002**

Data di chiusura delle iscrizioni: **30 Aprile 2002**

Data di inizio corso: **3 Maggio 2002**

Per creare questi corsi non abbiamo fatto altro che metterci nei vostri panni e ci siamo domandati quale fosse il modo migliore per insegnare qualcosa al di fuori di ciò che già facciamo da qualche tempo. Per questo abbiamo deciso che il metodo migliore fosse organizzare corsi tramite servizi di newsletter e di affiancarli con altri strumenti che conosciamo tutti: **FORUM** e **CHAT**. Il taglio non è quello solito e noioso dell'approccio teorico, ma quello pratico del consiglio e dell'applicazione "vera". Quello cioè che da sempre trovate nelle nostre pagine web.

Altra condizione da rispettare per noi è stata la accessibilità per tutti: ragione per cui l'iscrizione ai corsi al livello base avviene ad un costo comparabile a quello di una tazza di cappuccino: meno di 1 € al giorno. Il pagamento potrà essere effettuato tramite carta di credito, bonifico bancario, oppure tramite conto corrente postale.

Il corso si articola in tre livelli progressivi di servizio. Il materiale inviato è comune a tutti i livelli. Acquistando il terzo livello, si acquista automaticamente anche il servizio del primo e del secondo livello.

Nelle pagine seguenti troverai tutti i dettagli del corso.

Per ordinare il corso, clicca su <http://www.manuali.net/corsionline/iscrizione.asp>

IL DOCENTE

Ing. Alessio Palma, nato a Pescara nel 1970; laureato in ingegneria elettronica presso l'Università degli Studi di L'Aquila. Attualmente è amministratore di una società, di cui è uno dei soci fondatori, operante nel settore della Information Technology. www.khet.net.

OBIETTIVI DEL CORSO

P.G.P. è un software scritto da Philip Zimmermann, il quale risolve abbastanza agevolmente ed efficacemente i problemi della segretezza, autenticazione, cifratura, firma digitale e compressione della posta elettronica. L'intero pacchetto è distribuito gratuitamente in rete, compresi i sorgenti. Sia la qualità che il prezzo hanno favorito la sua diffusione, attualmente esistono delle versioni di PGP anche per MAC oltre che Windows e Linux. Per le aziende che lo intendono adottare è disponibile una versione commerciale, la quale garantisce anche l'opportuna assistenza.

Molti pensano ingenuamente che nessuno possa leggere la loro posta elettronica, ma questa viaggia in chiaro su numerosi computer e l'idea della privacy è solo una falsa illusione. Potreste aver bisogno di inviare informazioni confidenziali per vari motivi: perchè avete un amante; perchè dovete inviare documenti che non devono cadere in mano alla concorrenza; oppure perchè volete solo impedire agli altri di farsi i fatti vostri. Sebbene supporti la firma elettronica, P.G.P. non può essere usato per firmare i documenti, almeno non secondo le direttive della nuova legge 340, ma i concetti e l'efficacia della cifratura e dell'autenticazione sono gli stessi.

Questo corso, composto di 30 lezioni divise in sette moduli, guida i partecipanti, passo dopo passo, ad usare e capire P.G.P. in tutte le sue funzionalità.

PROGRAMMA DEL CORSO

Benvenuti nel corso on line per l'apprendimento P.G.P. Di Philip Zimmermann, la suite di software per la gestione della privacy della posta elettronica. Il nostro corso si articola in 30 lezioni suddivise in sette Moduli; ogni lezione viene fornita in formato [.pdf] (un formato di documento del software Adobe Acrobat che permetterà di visualizzare i documenti multimediali) oppure, se i file sono di grandi dimensioni, gli stessi saranno a loro volta compressi in formato zip.

Questo l'elenco dei moduli del corso, ed il loro contenuto:

Modulo 1 - 8 lezioni

Introduce il lettore alla crittografia, illustra il problema degli algoritmi basati su chiave privata ed i vantaggi indotti di quelli a chiave pubblica. Al termine del modulo il candidato ha perfettamente chiare le idee su a cosa servono e come si usano le chiavi pubbliche e private.

1. Necessità della crittografia

Perché la crittografia è importante, chi ha ostacolato la sua diffusione. Brevi cenni ai vari protocolli Internet.

2. Alcune classiche forzature ai sistemi di cifratura precedenti.

Si illustrano i classici schemi di attacco, principalmente basati su analisi statistiche.

3. Matematica della nuova crittografia

La matematica dietro i moderni sistemi di crittografia, sono illustrati i metodi matematici che garantiscono la sicurezza.

4. CAST, AES TripleDES, IDEA, Twofish

Algoritmi disponibili per la cifratura.

5. Certificati X.509

Cosa sono ed a cosa servono.

6. Cos'è PGP, L'autore di PGP Philip Zimmermann.

Chi e perché ha scritto PGP.

7. I keyserver: la infrastruttura di PGP.

PGP necessita di alcuni servizi on line per poter funzionare, chi li gestisce e come funzionano.

8. Come e dove prelevarlo.

PGP è disponibile per numerose piattaforme, alcune indicazioni sul dove prelevare la propria versione e la documentazione.

Modulo 2 - 6 lezioni

Vengono illustrate le operazioni da compiere per poter generare e gestire le chiavi pubblica e privata. Sono coperti tutti gli aspetti relativi alla autenticazione del proprietario di una chiave pubblica. Si mostra anche come impostare il server in modo da poter ottenere una copia delle chiavi in caso di cancellazione involontaria.

9. Preparare una coppia di chiavi

Guida alla generazione della propria coppia di chiavi.

10. Gestione della coppia di chiavi

In questa lezione sono illustrate le procedure per cambiare le impostazioni associate alla propria coppia di chiavi.

11. Mettere al sicuro la propria chiave privata

E' importante che la propria chiave privata non finisca nelle mani sbagliate, ma è anche importante potersi assicurare l'accesso ad essa. In questa lezione si indica come impostare le protezioni per accedere in modo sicuro alla propria chiave privata ed, eventualmente, impostare un keyserver per il ripristino della stessa.

12. Distribuire ed ottenere una chiave pubblica

La distribuzione della chiave PUBBLICA è di vitale importanza, in questa lezione si illustrano quali sono i metodi.

13. Gestire i portachiavi

Le chiavi pubbliche sono raccolte in portachiavi, questa lezione indica come prelevare, sia da un keyserver che da una e-mail, una chiave pubblica e copiarla in locale per gli usi successivi.

14. Verificare l'autenticità

Un problema molto importante che si pone è riuscire ad identificare chi è il possessore della chiave pubblica ricevuta. In questa lezione viene illustrata la procedura.

Modulo 3 - 4 Lezioni

Vengono illustrate le procedure per cifrare e/o firmare un documento oppure un file.

15. Firma e cifratura

Differenze tra firma, cifratura e firma + cifratura.

16. Messaggi di posta elettronica

In questa lezione si illustra come PGP interagisce con alcuni client di posta elettronica e come con essi si cifra o/e firma un documento.

17. Allegati dei messaggi di posta elettronica

Gestione degli allegati nei messaggi di posta elettronica. Oltre alla semplice cifratura si fanno osservare i principali rischi di sicurezza nel trattamento di documenti segreti.

18. I file e le cartelle

Gestione dei documenti protetti. Oltre ad avere necessità di software appropriato, come per esempio PGP, si rende necessario anche dotarsi di precauzioni hardware tra cui, per esempio, i lucchetti per i lettori di floppy disk.

Modulo 4 - 2 lezioni

In queste lezioni si indica come essere certi sull'identità del mittente e come decifrare documenti o file protetti.

19. Messaggi di posta elettronica

Gestire la decifratura e controllo della firma. Cosa fare in caso di Bad-signature.

20. Gestione degli allegati

Precauzioni nella decifratura di allegati segreti. Cenni agli SDA. Nella lezione sono trattate le procedure per la decifratura e verifica dell'identità del mittente.

Modulo 5 - 5 lezioni

Vengono prese in considerazione le opzioni avanzate di PGP.

21. Wipe

Cancellazione sicura dei file.

22. PGP impostazioni avanzate

Tutte le opzioni PGP di livello avanzato.

23. SDA

Invio di file cifrati con PGP verso utenti che non hanno installato il PGP. In questa lezione si indica come procedere per la composizione degli SDA.

24. PGP ed ICQ

Messaggi in tempo reale e PGP. Impostazione ed uso di PGP con ICQ.

25. PGPdisk, certificati X.509, PGP firewall, PGPVPN.

In questa lezione sono illustrate le caratteristiche della versione commerciale di PGP, sono anche indicate le procedure per l'impostazione degli stessi.

Modulo 6 - 2 Lezioni

In questo modulo si tratta l'uso di PGP sui sistemi Linux, tutte le procedure illustrate nei precedenti moduli rimangono validi, ma il modo di attuarle è leggermente differente.

26. Installare PGP su Linux

Guida all'installazione di PGP su Linux

27. Uso di PGP su Linux.

Esecuzione delle procedure in ambiente Linux indicate nei precedenti moduli

Modulo 7 - 3 Lezioni

Il quadro legislativo italiano e la nuova legge sull'obbligo dell'uso della firma elettronica in Italia. Il corso termina con la bibliografia ed una serie di indirizzi web che riportano alle fonti utilizzate in questo corso.

28. La legge Bassanini

Documentazione sulla legge Bassanini.

29. Obbligo per le imprese di usare la firma elettronica per inviare i propri documenti verso il registro delle imprese.

Uno sguardo alle problematiche che sono state introdotte dall'obbligo.

30. Bibliografia e panoramica web sul problema.

MODALITA' DEL CORSO

I TRE LIVELLI DI SERVIZIO

Abbiamo definito tre moduli di servizio per chi aderisce ai nostri corsi. Il secondo modulo comprende il primo, mentre il terzo comprende i primi due.

PRIMO MODULO

L'utente riceverà ogni giorno nella propria casella email fornita all'atto dell'iscrizione una lezione completa, comprendente, nel caso di peso complessivo eccessivo del materiale, alcuni link ad aree protette del sito www.manuali.net

Nel caso in cui la casella mail sia piena o il vostro provider abbia qualche problema tecnico, ogni giorno sul sito potrete trovare la lezione completa da scaricare via web senza alcun problema. Comunque è consigliato utilizzare una casella di posta elettronica email.it

Il costo di accesso a questo modulo di corso è pari a Euro **18,00 IVA compresa**. Non ci sono limiti al numero di iscrizioni fino all'inizio del corso. Effettuata l'iscrizione riceverete una mail automatica di conferma. Vi ricordiamo che la vostra iscrizione sarà considerata valida solo nel momento in cui ci giungerà comunicazione del perfezionamento del tipo di pagamento prescelto.

SECONDO MODULO

Oltre a quanto previsto nel primo modulo, l'utente potrà intervenire in forum di discussione diviso in trenta temi quante sono le lezioni. Il moderatore del forum (aperto per 15 giorni dopo l'invio dell'ultima lezione) sarà il docente, il quale vi risponderà pubblicamente al più presto. Il prezzo del secondo modulo è pari a Euro **36,00 IVA compresa**. In questo caso, per consentire al docente di offrire un servizio il più completo possibile, il numero di iscritti non sarà superiore a 200.

TERZO MODULO

Nel terzo modulo di servizio, oltre a quanto compreso nei primi due, è previsto l'accesso alla chat agli orari (max una o due ore) che verranno comunicati ogni giorno, durante i quali il docente sarà disponibile per parlare con voi. Inoltre agli iscritti sarà fornita la mail personale del docente per comunicare privatamente. Il prezzo del terzo modulo è pari a Euro **54,00 IVA compresa**. In questo caso, per consentire al docente di offrire un servizio il più completo possibile, il numero di iscritti non sarà superiore a 20.

Per ordinare il corso, clicca su <http://www.manuali.net/corsionline/iscrizione.asp>