CORSO DI SICUREZZA DEI SISTEMI WEB E MOBILI

Modulo 4: Sicurezza dei Sistemi Web

Uso di GPG - Esercizi

GNU Privacy Guard (GnuPG o GPG) è un software libero progettato per sostituire la suite crittografica PGP. È completamente compatibile con gli standard OpenPGP dell'IETF ed è sostenuto dal governo tedesco. Viene rilasciato sotto la licenza GNU General Public License e fa parte del Progetto GNU. È già installato nella versione di Ubuntu che vi è stato suggerito di installare nella macchina virtuale da usare per le sessioni pratiche.

Il manuale `https://www.gnupg.org/gph/it/` contiene la sintassi dei comandi per cifrare, decifrare, firmare un messaggio, creare chiavi, inserirle nel *key ring* e firmarle. Per lo svolgimento dei prossimi esercizi fate riferimento al manuale.

1 Esercizi

1. Creare un file di testo `messaggio.txt` con un qualsiasi contenuto. Usando GPG:
   - cifrare il file con crittografia simmetrica usando algoritmi diversi (AES, 3DES e Blowfish), generando file diversi a seconda dell'algoritmo usato;
   - Decifrare i file generati al punto precedente.
2. Creare due nuovi utenti nel sistema, `Alice` e `Bob`. Per ciascun utente generare una coppia di chiavi da 1024 bit, inoltre fare importare ad `Alice` la chiave di `Bob` e viceversa far importare a `Bob` la chiave di `Alice`, verificando il *fingerprint* e firmando la chiave. In seguito:
   - Far inviare da `Alice` a `Bob` un messaggio cifrato con crittografia **asimmetrica**;
   - Far inviare da `Bob` ad `Alice` un messaggio sia cifrato che firmato. `Bob` deve decifrare il messaggio e verificare la firma.