SLIDE1: INTRO

Una prima distinzione da fare parlando di crittografia riguarda la tipologia. Essa infatti può essere simmetrica o asimmetrica

SLIDE2: CHIAVE SIMMETRICA

Nella crittografia a chiave simmetrica, chiamata anche a chiave privata, le operazioni di cifratura e decifratura avvengono mediante un algoritmo che adopera la medesima chiave per entrambe le operazioni. Si nota quindi che la chiave deve essere conosciuta da entrambi gli interlocutori. Questo pone in essere il cosiddetto problema dello scambio della chiave: se gli interlocutori non dispongono già della chiave, è necessario un canale sicuro per inviarsela, e internet non lo è, in quanto i pacchetti potrebbero essere intercettati.

SLIDE3: CHIAVE ASIMMETRICA

per porre rimedio a questo problema si possono adoperare tecniche crittografiche a chiave asimmetrica, dette anche a chiave pubblica. Grazie a queste tecniche vengono utilizzate due chiavi distinte per le operazioni di cifratura e di decifratura. Queste due chiavi vengono generate matematicamente in modo tale da permettere la decifratura solo alla chiave corrispondente a quella usata per la cifratura.

SLIDE4: COPPIA CHIAVI

Nella pratica ogni utente che intenda utilizzare la crittografia asimmetrica disponde di una coppia di chiavi, chiamate pubblica e privata. La tecnica prevede che l'utente mantenga segreta la propria chiave privata, mentre renda disponibile a chiunque quella pubblica. In questo modo chiunque voglia comunicare in maniera cifrata con un'altra persona deve applicare prima la propria chiave privata poi la chiave pubblica del destinatario, il quale, una volta ricevuto il messaggio, applicherà prima la propria chiave privata e poi la chiave pubblica del mittente. Questo assicura anche l'identità di mittente e destinatario, oltre alla confidenzialità del messaggio crittografato, in quanto solo i proprietari delle chiavi private correlate a quelle pubbliche utilizzate possono cifrare e decifrare il messaggio.

SLIDE5: C.A.

Sorge quindi un altro problema: dato che tramite apposite utility chiunque potrebbe generare la propria chiave e dichiarare un'identità falsa e grazie a questa eseguire degli attacchi, ad esempio di tipo Man in the Middle. Nasce quindi la necessità di un'autorità che garantisca l'identità degli interlocutori. A questo fine operano le Certification Authorities (chiamate anche C.A.): generano le coppie di chiavi che consegnano agli utenti, dei quali garantiscono l'identità

SLIDE6: VS

Alla luce di quanto appena esposto sembrerebbe preferibile adottare sempre algoritmi asimmetrici, dati i loro vantaggi. Tuttavia bisogna considerare vari fattori prima di operare la scelta: se è vero che le tecniche asimmetriche risolvono il problema dello scambio della chiave, è altresì corretto che sono computazionalmente più complesse, nonché leggermente più difficili da implementare negli applicativi. Quindi è necessario valutare la situazione. Per esempio, quando non si pone il problema dello scambio della chiave, la scelta di un algoritmo simmetrico dovrebbe prevalere.

SLIDE7: IBRIDA

nella pratica attuale spesso accade, come ad esempio nel protocollo SSL/TLS, che approfondirò successivamente, che si utilizzino tecniche crittografiche cosiddette ibride. Grazie a queste si possono combinare i vantaggi della crittografia asimmetrica e di quella simmetrica. Si utilizzano infatti tecniche asimmetriche per l'autenticazione degli interlocutori e per lo scambio di una chiave di sessione, che verrà utilizzata in seguito per cifrare e decifrare i messaggi con algoritmi simmetrici.