CIFRATURA ASIMMETRICA

In questo paradigma di cifratura gli end-point condividono pubblicamente le rispettive chiavi PUBBLICHE in modo tale che chiunque possa CIFRARE dati ma solo il destinatario effettivo, tramite la propria chiave PRIVATA, sia poi in grado di DECIFRARE il messaggio. In questo paradigma quindi invece il ruolo delle chiavi private e pubbliche, nel senso che qui si cifra con la pubblica mentre la firma viene generata con la privata.

Per costruzione, il modello RSA si presta bene ad entrambe le operazioni poiché, essendo bidirezionale, basta utilizzare la chiave adeguata per cifrare/firmare.

In reti molto grandi non è praticabile distribuire a tutti le chiavi pubbliche di ogni utente, nonostante questo non sia un rischio dal punto di vista della sicurezza.

Bisogna poi tenere in conto che la cifratura asimmetrica è CONSIDEREVOLMENTE PIÙ LENTA della cifratura simmetrica.

Solitamente quindi la cifratura asimmetrica è usata in combinazione con la cifratura simmetrica per creare SCHEMI IBRIDI

In generale comunque è una buona pratica definire protocolli e standard diversi per cifratura e firma, anche se RSA si presta ad entrambi gli usi. In particolare poiché le garanzie di cifratura e firma sono diverse, si sono specializzati gli algoritmi di padding per proteggere i protocolli da attacchi molto specifici contro uno o l'altra garanzia.

CIFRATURA ASSIMMETRICA IBRIDA

Come detto, nelle applicazioni reali non si utilizza quasi mai la cifratura asimmetrica per cifrare i dati.

L'algoritmo genera una CHIAVE SIMMETRICA che viene poi cifrata tramite KEY PAIR asimmetrico. La chiave così cifrata viene condivisa con l'altro end point. Il traffico poi viene cifrato in modo simmetrico.

Questo rende le prestazioni accettabili anche per grandi moli di dati poiché la cifratura asimmetrica è molto pesante.

Anche la cifratura asimmetrica è intrinsecamente NON SICURA in alcuni scenari, come ad esempio: NON LO SAPREMO MAI PERCHÈ NON HA REGISTRATO LA RISPOSTA PER FARE IL SIMPATICO. Ad ogni modo il paradigma ibrido è sempre da preferire.