Lezione 12 modulo 1

In questo modulo parleremo di integrità dei documenti e poi, successivamente, della firma digitale dei documenti. Ricordo che l'integrità è una proprietà che abbiamo associato alla sicurezza e sostanzialmente quello che dice questa proprietà è che vogliamo riuscire ad accorgerci se c'è stata una modifica non autorizzata di un documento. Questo può avvenire in varie fasi, come avevamo visto nei possibili attacchi, e quello che vogliamo, appunto, garantire è poter identificare possibili variazioni dei documenti che non siano state autorizzate. Qual è un problema che noi abbiamo? In generale, quando andiamo a considerare un intero documento, è che il nostro documento può essere, abbiamo detto, cifrato attraverso gli algoritmi di cifratura che abbiamo esaminato, ma in realtà questo documento tipicamente sarà composto da un certo numero di blocchi. Quello che andremo tipicamente a cifrare sarà il singolo blocco a cui applicheremo la nostra cifratura asimmetrica o simmetrica. Quello che può avvenire è che, come possibile alterazione del documento, io prenda un blocco e lo sostituisca con un altro, ad esempio che è già stato anch'esso cifrato, quindi diciamo un documento che ha caratteristiche simili e quindi, ad esempio, vado ad alterare un documento alterando un singolo blocco. E' chiaro che quando vado a fare le operazioni di decifratura, ad esempio quando utilizzo la chiave asimmetrica, io lavorerò sul singolo blocco e quindi se questo blocco è un blocco corretto, nel momento in cui viene sostituito qui, io andrò a verificare uno per uno i vari blocchi che compongono il documento e anche il blocco sostituito verrà verificato correttamente. Questo però, comunque, avviene in un caso in cui il documento è stato alterato perché ho sostituito un blocco con un altro e quindi l'integrità del documento non riguarda solo il singolo blocco, ma riguarda il fatto che l'intero documento sia rimasto integro. Qual è il problema che abbiamo qua? È che i documenti hanno una lunghezza variabile; noi abbiamo bisogno di uno strumento che ci consenta di andare a vedere se effettivamente l'intero documento sia stato alterato oppure no. Per supportare questo tipo di analisi, possiamo usare una tecnica, che è quella delle 'Funzioni di HASH', che applicate a un documento, consentono di ottenere quella che viene chiamata la 'impronta del documento', oppure 'Digest', che ha una lunghezza fissa, quindi qualunque sia la lunghezza del documento originario, la mia impronta avrà una lunghezza fissa e quindi io potrò, a questo punto, andare a verificare se all'interno del documento ci siano state ad esempio delle sostituzioni come dicevamo. Ovviamente, che caratteristiche deve avere questa funzione di hash? Abbiamo bisogno di alcune proprietà: la prima è la 'coerenza', naturale essendo una funzione e quindi io voglio che dati due documenti uguali, se vengono trasformati, effettivamente diano la stessa impronta; poi un'altra proprietà che è importante è la 'univocità'; anche un cambiamento anche molto piccolo del documento vogliamo che il risultato nell'impronta sia differente. Naturalmente, avendo l'impronta una lunghezza finita, dato un documento di qualunque lunghezza, questa avrà una probabilità molto bassa di avere una possibile impronta uguale dati due documenti diversi. Un'altra proprietà che ci interessa, è la 'non invertibilità': data l'impronta, non devo poter ricostruire il documento originario. Data una funzione con queste caratteristiche, una che tipicamente viene utilizzata negli standard è quella chiamata 'MD5', potrò fare la seguente operazione: dato un documento, da parte di un mittente, posso applicare la funzione di hash, ottengo l'impronta, il Digest del messaggio e trasmetto sia il messaggio sia il Digest, questi vengono ricevuti dal destinatario e il destinatario per controllare che il documento sia integro, applicherà il messaggio di nuovo, la stessa funzione di hash, otterrà un Digest localmente, lo confronterà col Digest ricevuto e se questi due Digest sono uguali, il messaggio è integro, altrimenti viene rifiutato. Ovviamente in questa operazione di verifica c'è ancora un problema: nel momento in cui abbiamo la trasmissione, qualcuno potrebbe modificare contemporaneamente sia il messaggio sia il Digest collegato e quindi quello che mi interesserà sarà proteggere il Digest del messaggio e quindi per avere effettivamente una garanzia di integrità avrò la necessità di proteggere questo Digest con delle tecniche crittografiche. Questo ci porterà a illustrare quelli che sono i meccanismi della firma digitale o firma elettronica. Noi sostanzialmente vogliamo garantire due proprietà: l'autenticità, ricordo che vuol dire che dobbiamo essere in grado di attribuire a un certo documento un certo autore e inoltre questo non potrà poi successivamente

ripudiare il documento e ricordo anche che abbiamo l'autore del documento col non ripudio, ricordiamo anche che l'autenticità include anche al suo interno l'integrità. Quindi voglio lavorare non sul singolo blocco ma sull'intero documento. Abbiamo detto partiremo dalla funzione di hash che ci trasformerà il nostro documento in un Digest, ma dovremo aggiungere una cifratura in questo documento e ovviamente quello che ci interessa è attribuire un autore nel fare questa operazione, quindi utilizzeremo le chiavi asimmetriche. Ricordo che ciascun partecipante che ha un'interazione può avere una coppia di chiavi, una pubblica e una privata. Vediamo adesso come funziona la firma digitale: innanzitutto avremo due fasi, una fase di 'creazione della firma' e poi avremo una fase di 'verifica della firma'. Ovviamente su due parti A e B, la creazione verrà fatta da una parte che è il mittente e la verifica da parte di chi riceve il documento firmato. Cos'è la firma? La firma è una trasformazione con la funzione di hash che viene cifrata. Abbiamo detto usiamo la cifratura asimmetrica, quindi in questo caso useremo la chiave privata di chi manda il messaggio. Ricordo che questa è riservata, è di proprietà del mittente ed è riservata nel senso che non viene ceduta ad altri e quindi ci può legare un certo messaggio all'autore di questo messaggio. Quello che ottengo da queste operazioni viene chiamata 'firma digitale'. La firma digitale viene inviata insieme al documento, quindi quando avrò la trasmissione, avrò due parti: una parte che sarà inviata in chiaro oppure potrà essere cifrata se vorrò anche la riservatezza, ma non è questo l'oggetto diciamo dell'operazione che stiamo facendo adesso e una parte che è la firma che è cifrata con la chiave privata di A. Questo è un documento firmato, quindi il documento che ha queste due parti. Cosa farà chi riceve il messaggio? Dovrà verificare che effettivamente il documento sia autentico. Per fare questo riceverà appunto questi due componenti: il messaggio, il documento originario, la firma che viene inviata e farà le operazioni inverse rispetto a quello che era stato fatto nella fase di generazione di impronta, poi cifratura da parte del mittente sulla firma digitale. Quindi prima avrò la decifratura con la chiave pubblica corrispondente a quella privata di A, ottengono in questo modo un Digest che è quello che è stato effettivamente inviato da parte del mittente. In parallelo prenderò il documento, genererò il Digest del messaggio, confronterò i due Digest ricevuti e quindi, a questo punto, nel caso siano uguali, io posso considerare valida questa firma. Ovviamente quello che è importante è che data la coppia di chiavi, abbiamo detto, abbiamo una chiave pubblica e una chiave privata associate a un certo agente, quindi avremo una chiave pubblica di A e una chiave privata di A; dobbiamo garantire in effetti che la chiave privata sia effettivamente quella associata ad A e dobbiamo anche garantire che non sia stata rubata e quindi che sia ancora valida. Questo ci porterà a un discorso successivo che è quello di 'gestione delle chiavi', quindi quello che dovrò fare quando voglio verificare la firma è, sì verificare effettivamente che la firma sia valida con questo meccanismo, ma anche verificare che in effetti sia ancora valida la chiave associata ad A, che è una chiave pubblica, abbiamo detto può essere distribuita liberamente appunto in quanto pubblica, può essere anche inviata insieme al messaggio nella fase di invio del documento firmato, ma quello che devo anche garantire è che effettivamente questa chiave sia ancora valida. Quindi vedremo successivamente quali sono i meccanismi per fare queste operazioni di verifica che sono necessarie perché effettivamente una firma digitale possa avere anche un valore ad esempio legale. Chiudiamo questo modulo illustrando quindi le caratteristiche della firma digitale: innanzitutto abbiamo detto che andiamo a garantire autenticità, compresi gli aspetti importanti di 'non ripudio' e anche di 'verifica dell'integrità del documento'. Un'altra caratteristica della firma digitale che è diversa dalla firma autografa associato ai documenti firmati cartacei, è nel fatto che è diversa per ciascuno dei documenti e quindi non può essere copiata, nel senso che io non posso prendere la firma associata a un documento e associarla ad un altro perché ovviamente nella operazione di verifica vedrò che poi i Digest generati sono diversi, quindi questo mi dà delle garanzie anche in più rispetto alla firma autografa che può essere ovviamente copiata e quindi falsificata.