Lezione 11 modulo 3

Per quanto riguarda le tecniche matematiche, soprattutto ci concentreremo su quelle che sono tecniche crittografiche, quindi parleremo di crittografia. La crittografia ci consente di prendere un messaggio, noi parleremo di messaggi intendendo sempre le nostre sequenze di bit, e tramite un processo di codifica o 'encryption', in inglese, otterremo un messaggio, che è un messaggio cifrato che ha la proprietà di non poter essere ritrasformato nel messaggio originale a meno che non si applichi un'altra operazione di decifratura che ci consenta di riottenere il messaggio iniziale. Quando parleremo di crittografia, noi faremo questa operazione di cifratura e di decifratura e useremo delle funzioni matematiche e oltre ad usare funzioni matematiche che come vedremo saranno di due tipi, noi useremo anche qualcosa che viene chiamato 'chiave', quindi avremo le chiavi delle funzioni, chiave oppure chiavi (vedremo in alcuni casi avremo più di una chiave) delle funzioni, quindi la mia cifratura sarà in realtà l'applicazione di una funzione con una chiave e nella decifratura avremo una funzione, che potremo vedere che è la stessa o diversa, che è una chiave. Qui quello che noi andremo a vedere è come questo meccanismo generale si può realizzare per garantire diverse proprietà. A seconda del meccanismo utilizzato vedremo che potremo garantire una o più proprietà. Innanzitutto noi parleremo di due tecniche crittografiche: parleremo di crittografia 'Simmetrica' quando avremo una chiave che chiameremo 'segreta'. La crittografia, invece, 'Asimmetrica', in cui noi avremo una coppia di chiavi, quindi due chiavi legate una all'altra, che verranno utilizzate per cifrare e decifrare. Le chiavi verranno chiamate chiavi pubbliche, avremo nella coppia una 'chiave pubblica' e una 'chiave privata'. E noi vedremo poi successivamente che questa coppia di chiavi viene associata a un soggetto, a un agente. L'idea di questa coppia di chiavi è che noi avremo una chiave che appunto rimarrà privata, quindi conosciuta solo dal possessore della chiave, mentre l'altra, pubblica, vorrà dire che verrà distribuita e servirà per effettuare l'operazione inversa all'operazione che sarà stata effettuata con la chiave privata. Cominciamo a vedere il meccanismo della crittografia simmetrica: con la crittografia simmetrica noi abbiamo a disposizione un'unica chiave segreta, questo vorrà dire che quando noi abbiamo due agenti che parlano, li chiameremo A e B nel seguito, alcuni li chiamano Alice e Bob per ricordarsi dei nomi, questi agenti condivideranno questa chiave quindi entrambi conosceranno questa chiave segreta, quindi sarà un segreto fra le due parti. Vediamo il meccanismo rappresentato in questa figura: il mittente cifra il messaggio con la chiave segreta, ottiene il testo cifrato, decifra il messaggio con la stessa chiave e vediamo che alla fine otteniamo il messaggio originario. Quindi questo è lo schema che abbiamo visto all'inizio in cui abbiamo la stessa chiave, che è una chiave condivisa tra le due parti, per questo viene chiamato simmetrico perché utilizziamo la stessa chiave in entrambi i casi. Quello che è da osservare in questo caso è che ovviamente il fatto che A e B possano condividere appunto questa chiave segreta ha uno scopo principale che è quello di mantenere la segretezza del messaggio, quindi io voglio ottenere un messaggio che possa essere decifrato solo da chi possiede questa chiave. Quindi la proprietà che in questo caso andiamo a mantenere è la riservatezza. Per quanto riguarda la proprietà di autenticità del messaggio in questo caso si potrebbe pensare che anch'essa possa essere garantita da questo meccanismo, in realtà cosa succede? Se A manda un messaggio, lo cifra con questa chiave, viene ricevuto da B e B riceve questo messaggio pensando che sia ricevuto da A, avendo usato A appunto, avendo ricevuto un messaggio cifrato con questa chiave potrebbe pensare che effettivamente sia stato mandato da A. Questo è sicuramente vero però quello che può succedere è che venga violata una parte della autenticità del messaggio che abbiamo chiamato il 'non ripudio', B potrebbe creare un messaggio non mandato da A e far arrivare un messaggio non autentico e sostenere che l'abbia mandato A. In questo caso A andrebbe a fare un'operazione di rifiuto del messaggio, sosterebbe che il messaggio non è stato mandato in effetti da A e quindi la proprietà di autenticità di questo messaggio non può essere verificata e quindi noi con questo meccanismo non potremmo effettivamente avere diciamo una proprietà di autenticità, ma possiamo avere solo la riservatezza. Ovviamente ci sono alcuni problemi che si verificano nell'utilizzare questo meccanismo, che è un meccanismo che è noto da molto tempo, da secoli; è stato utilizzato in ambito militare già dai tempi di Cesare: che la chiave è una chiave segreta e il meccanismo funziona finché viene mantenuta la

segretezza della chiave, quindi c'è un problema di distribuzione di queste chiavi, che ovviamente vincola tutto il meccanismo. Parleremo quindi di distribuzione delle chiavi, ma questo chiaramente ad esempio è difficile da fare in rete e può essere utilizzato in rete solo accoppiato ad altri meccanismi di distribuzione che garantiscano effettivamente che la chiave rimanga segreta. Rispetto alle tipologie di algoritmi che si possono utilizzare per fare cifrature di questo tipo, noi ne vedremo soprattutto due, che possono poi, come vedremo, essere combinate fra di loro, la sostituzione. All'interno del messaggio noi abbiamo delle lettere, tipicamente questo verrà poi fatto sui bit, avremo dei meccanismi di sostituzione, faremo degli esempi con delle lettere alfabetiche. Cosa vuol dire? Che al posto di una lettera, noi ne metteremo un'altra. L'altro meccanismo che noi avremo è quello invece della 'trasposizione'. Trasposizione vorrà dire che il messaggio cifrato in realtà conterrà le stesse lettere che avremo nel messaggio originale, ma in un ordine diverso e quindi il testo cifrato sarà difficile da leggere all'interno della trasmissione e sarà invece facilmente decifrabile con la chiave. Vediamo qualche esempio di semplici sostituzioni e trasposizioni. Ovviamente i meccanismi vengono fatti con chiavi ben più complesse e con sostituzioni più complesse, ma per dare un'idea di cosa possiamo fare. Ad esempio una chiave=4, ci può dire, andiamo a trasporre di quattro lettere l'alfabeto, ad esempio l'alfabeto che inizia da A, lo facciamo iniziare la E: ogni volta che troveremo A andremo a scrivere E, come ad esempio vediamo in questo esempio nella parola ciao e quindi il mio messaggio cifrato mi porterà ad avere una cifratura del messaggio che ha delle lettere sostituite. Ovviamente in questo caso noi andiamo ad avere una chiave abbastanza semplice, è facile ricondurre, ricostruire la chiave in questo caso perché possiamo andare a provare tutte le possibili chiavi quindi possibili trasposizioni dell'alfabeto e troveremo facilmente il nostro messaggio. Ovviamente le chiavi di solito sono più complesse, sono insiemi di testi che vengono considerati. Ovviamente un altro problema che si può verificare è il fatto di andare a vedere la frequenza delle lettere all'interno delle parole per ricostruire delle parole solo in base alle frequenze, quindi ci sono tanti possibili attacchi ad algoritmi di questo tipo che vanno prevenuti con combinazioni come vedremo di tecniche. L'altra tecnica che appunto spesso viene poi considerata insieme alla sostituzione per avere degli algoritmi più robusti è quella di trasposizione o permutazione. Useremo la lettera poi P per questo tipo di blocco successivamente, che sostanzialmente prende un testo, ad esempio 'trasferire un milione' che vediamo qua, lo dispone secondo quella che nel nostro esempio è la lunghezza della chiave e poi verrà letto il testo a colonne: ad esempio se andiamo, usiamo la chiave anche per ordinare le colonne, le ordiniamo in ordine alfabetico, la prima colonna è quella indicata dalla lettera A e quindi leggeremo il testo a colonne, la seconda colonna nel nostro esempio è quella indicata dalla lettera I e quindi il nostro messaggio cifrato sarà composto da 'F-N-E, R-I-B' e così via... Ovviamente nota la lunghezza (tutto questo viene fatto solitamente a blocchi), nota la lunghezza della chiave del messaggio è possibile ricostruire dove spezzare il messaggio ricevuto per poter ricostruire il messaggio e posizionarlo a colonne secondo quel che è la lunghezza della chiave usando la stessa chiave, quindi andremo a mettere il messaggio ricevuto nelle colonne secondo le lettere indicate dalla chiave e potremo ricostruire il messaggio. Ovviamente questi sono meccanismi appunto in cui, in un caso sostituisco una lettera, anche qui per ricostruire il messaggio userò la stessa chiave, dovrò usare la trasposizione dell'alfabeto di tipo inverso e quindi sostituisco quando dovrò decifrare la lettera con lo stesso meccanismo che abbiamo visto prima quando troverò una lettera E, so che dovrò andare a prendere la lettera A nell'alfabeto. Questi sono dei meccanismi che mi consentono di cifrare i messaggi con un'unica chiave: cifro e decifro con la stessa chiave. Li posso combinare utilizzando alternativamente dei blocchi di trasposizione e dei blocchi di sostituzione utilizzando quindi sequenze di questi blocchi per cifrare un messaggio in ingresso, tre terne e un'uscita. Con questo sistema sono stati prodotti degli algoritmi robusti come l'Advanced encryption standard che viene comunemente utilizzato nell'ambito della cifratura simmetrica. Quello che è da notare è che questi blocchi possono essere utilizzati facilmente all'interno di un sistemato hardware e quindi io posso realizzare negli hardware dei sistemi di cifratura e quindi avrò la caratteristica di avere queste operazioni svolte in un mondo molto veloce. Quindi utilizzando la cifratura simmetrica avremo lo svantaggio di avere un'unica chiave e il problema di distribuirla, ma avremo il vantaggio di poter realizzare dei sistemi hardware che fanno queste operazioni di cifratura molto

velocemente. Passiamo adesso a un altro meccanismo che viene comunemente utilizzato per quanto riguarda la gestione appunto delle proprietà di riservatezza e autenticità dei documenti e che utilizza due chiavi: abbiamo detto parleremo di cifratura di tipo asimmetrico. Allora quando abbiamo una cifratura di tipo asimmetrico noi sostanzialmente abbiamo detto avremo 2 chiavi: abbiamo una chiave privata per uno stesso soggetto, una chiave privata e una chiave pubblica. E avremo questa coppia di chiavi applicata, associata a un unico agente, quindi la chiave privata di A e la chiave pubblica di A. Se vogliamo realizzare una comunicazione tra due agenti potremmo avere bisogno di più coppie di chiavi a seconda delle proprietà che vorremmo garantire. Ad esempio l'agente B potrà anch'esso avere una chiave privata e una chiave pubblica. Il meccanismo funziona nel seguente modo: noi utilizzeremo per cifrare il nostro messaggio una delle due chiavi, chiamiamola adesso per semplicità la chiave 1, otterremo un messaggio cifrato, per decifrare useremo la seconda chiave della coppia, chiamiamola chiave 2, dove chiave 1 e chiave 2 faranno parte della stessa coppia di chiavi, potremo utilizzare appunto le chiavi che sono associate ad A o B a seconda delle proprietà di sicurezza che vogliamo ottenere. Vediamo adesso un'applicazione di questo esempio: quindi quello che vedete qui, la differenza principale che abbiamo rispetto all'algoritmo simmetrico è che abbiamo innanzitutto una chiave che è dichiarata pubblica, quindi non ho problemi di distribuzione di questa chiave e avremo coppie di chiavi associate ai soggetti, anziché chiavi segrete condivise fra soggetti. Vediamo, dicevo, un'applicazione di questo tipo di cifratura: abbiamo in questo caso un messaggio, il messaggio viene cifrato utilizzando la coppia di chiavi che appartiene a B; quindi stiamo usando la chiave privata di B e la chiave pubblica di B. Ovviamente l'ipotesi è che la chiave privata di B rimanga sempre in capo a B, quindi non venga distribuita. Quando stiamo usando queste chiavi, se il messaggio parte da A, potrò usare solo la chiave pubblica di B per poter cifrare il messaggio. In questo modo, ottengo un messaggio cifrato; ho usato la chiave pubblica di B, chi potrà leggere questo messaggio? Chi possiede la chiave privata di B, quindi solo B potrà leggere il messaggio che è stato inviato, quindi ovviamente è da sottolineare l'importanza di tenere riservata la chiave privata di B perché il meccanismo funzioni. Che proprietà avrò ottenuto in questo caso? Anche in questo caso, come nella cifratura simmetrica, abbiamo ottenuto la riservatezza. Abbiamo però risolto un problema: il fatto che otteniamo la riservatezza con una chiave pubblica di B che può essere facilmente distribuita, appunto è pubblica e può essere distribuita a chiunque, mentre invece la chiave privata di B rimane solo in capo a B e quindi non verrà distribuita, quindi non ho più il problema di una chiave che deve essere distribuita in modo segreto. Vediamo adesso un secondo caso, che è il seguente: cosa succede se uso invece le chiavi di A? Quindi una chiave privata di A e una chiave pubblica di A? Ovviamente non ha molto senso che A cifri con la sua chiave pubblica perché nessuno potrebbe leggere il suo messaggio, quindi quello che A farà in questo case è cifrare con la sua chiave privata. Chi potrà leggere questo messaggio? Ovviamente la chiave pubblica è pubblica, quindi tutti potranno leggere questo messaggio, tutti quelli che hanno questa chiave, ma l'idea qua non è quella di mantenere la riservatezza, quindi non abbiamo la riservatezza del messaggio, ma utilizziamo questo meccanismo per fare un'altra cosa: quando leggiamo il messaggio usiamo la chiave pubblica di A, quindi possiamo decifrare questo messaggio nel momento in cui abbiamo il messaggio M noi sappiamo che questo è stato cifrato da A che è l'unico possessore, di nuovo l'ipotesi che la chiave privata non venga distribuita a nessun altro, che è l' unico possessore di questa chiave A e quindi in questo caso io ho un messaggio autentico. In questo modo abbiamo ottenuto una proprietà che prima non riuscivamo a ottenere perché A non potrà dire di non avere mandato questo messaggio perché solo A potrà aver cifrato il messaggio utilizzando la sua chiave privata. Ovviamente come vedremo poi dovranno esserci dei meccanismi di garanzia che devono essere messi in atto per quanto riguarda ad esempio il fatto che si può verificare cosa succede se viene rubata una chiave privata, ci dovranno essere dei meccanismi anche qui di gestione di questi aspetti, però in questo momento diciamo che abbiamo una proprietà che è la proprietà di autenticità. Torneremo sull'autenticità perché in questo momento stiamo pensando a blocchi, tenete presente che qua stiamo pensando a prendere un blocco e il nostro messaggio è un blocco solo, quindi cifro e decifro un blocco solo mentre invece poi noi vorremo un messaggio fatto da più blocchi e quindi vorremo anche garantire l'integrità. In questo momento stiamo garantendo l'autenticità del singolo blocco con

questo meccanismo, come vedremo sull'integrità avremo bisogno anche di qualcos'altro. Ovviamente cosa succede? Abbiamo detto che qua non possiamo mantenere in questo modo la riservatezza ma cosa possiamo fare se vogliamo avere un messaggio sia riservato che autentico utilizzando questo meccanismo? Io posso combinare quelle che sono le due cifrature, posse cifrare con la chiave privata di A per avere l'autenticità di questo messaggio, con la chiave pubblica di B per ottenere un messaggio che venga trasmesso in modo riservato, quindi qua abbiamo la trasmissione del messaggio in questa fase, quando il ricevente B riceve il messaggio, dovrà applicare la decifratura nel corrispondente ordine: quindi prima decifrare con la sua chiave privata e poi decifrare con la chiave pubblica di A per riottenere il messaggio originale. Quindi in questa fase sostanzialmente andiamo a garantire la riservatezza del messaggio e in questa parte andiamo a garantire l'autenticità del messaggio. Abbiamo visto quindi che con la cifratura asimmetrica possiamo garantire riservatezza e autenticità, abbiamo risolto alcuni aspetti relativi alla distribuzione delle chiavi, però c'è un problema, il problema che algoritmi di questo tipo sono basati su delle funzioni matematiche complesse, tipicamente possono essere proprietà geometriche di oggetti oppure l'elevazione a potenza e quindi la loro realizzazione sarà computazionalmente onerosa e richiederà una quantità di calcolo, di risorse di calcolo maggiore che nel caso precedente e non può essere implementata via hardware. Quindi andremo ad avere un meccanismo che è conveniente rispetto ad alcuni punti di vista e soprattutto rispetto alle proprietà che possiamo garantire, ma paghiamo questo con una onerosità di calcolo che dovremo gestire opportunamente.