**Capitolo 8**

**1) Quali sono le differenze tra riservatezza e integrità del messaggio? Si può avere una senza l’altra? Argomentate la risposta.**

La riservatezza si intende che solo il mittente e il destinatario sono in grado di comprendere il contenuto del messaggio che viene trasmesso, quindi è *necessario* cifrare il messagio per renderelo incomprensibile ad altri. Per integrità si intende che il contenuto del messaggio trasmesso non subisca, durante la trasmissione, alterazioni dovute a manipolazioni. Si può avere una senza l’altra ma in questo modo non verrà assicurata una comunicazione sicura tra diversi utenti.

DA CONFRONTARE

**2) Le entità di Internet, quali router,switch,DNS e web server nonché i sistemi periferici, hanno spesso la necessità di poter comunicare in modo sicuro. Date 3 esempi di entità con questa necessità**.

1) Un consimatore che trasmette il suo numero di carta di credito a un web server pre effettuare un acquisto

2) Un cliente che interagisce online con la propria banca

3) Soggetti che richiedono comunicazione sicura potrebbero far parte integrsnte dell’infrastruttura di rete. Nel caso del DNS, un malintenzionato può attivamente interferire ,controllare o danneggiare la ricerca e aggiornamento di un DNS provocando danni su Internet.

**3) Qual è un importante differenza fra un sistema a chiave simmetrica e uno a chiave pubblica dal punto di vista del servizio?**

Nei sistemi a chiave simmetrica due utenti che vogliono scambiarsi i messaggi hanno un unica chiave privata che condividono tra di loro,che utilizzano per cifrare e decifrare il messaggio trasmesso.

Nei sistemi a chiave pubblica gli utenti hanno ognuno 2 chiavi: una pubblica e una privata. La chiave pubblica la conoscono tutti, invece la privata è unica per ogni utente e non è condivisibile.

Se Alice deve inviare un messaggio a Bob, essa utilizzarà la chiave pubblica di Bob per cifrare il messaggio e Bob utilizzerà la sua chiave privata per decifrarlo.

**4) Supponete che un intruso disponga di un messaggio cifrato e della sua versione decodificata. Avvalendosi di queste conoscenze può organizzare un attacco al testo cifrato, un attacco con testo in chiaro noto o un attacco con testo in chiaro scelto?**

Un attacco con testo in chiaro scelto, dato che in questo caso l’intruso è ha ottenuto la forma cifrata di un testo a lui noto. Per esempio se Trudy intercetta un messaggio di Alice che contiene tutte le lettere dell’alfabeto,allora può decifrare lo schema crittografico.

**5) Considerate un cifrario a 8 blocchi. Quanti possibili blocchi ha? Quante associazioni esistono? Se consideriamo Ogni associazione come una chiave, quante possibili chiavi ha questo cifrario?**

Numero possibile di blocchi 2^8=256

Numero associazioni 2^8=256

Numero di possibli chivavi di questo cifrario sono 2^8!=256!

**6) Supponete che *N* individui vogliano comunicare tra di loro utilizzando la cifratura a chiave simmetrica e che il messaggio fra due persone,i e j,siano visibili a tutti i componenti del gruppo, che non sono però in grado di decodificarli. Quante chiavi sono necessarie nell’intero sistema? Considerate ora la chiave pubblica. Quante chiavi sono richieste in questo caso?**

1) N/2 chiavi dato che nella crittografia simmetrica due utenti quando vogliono scambiarsi il messaggio condividono la stessa chiave segreta.

2) 2\*N chiavi,ogni utente avrà un chiave pubblica e una privata, in questo modo tutti possono codificare messaggio con la chiave pubblica del destinatario e il destinatario può decodificare messaggio con la sua chiave privata

**7) Supponete n=10000 a=10023 e b=10004. Usate una delle uguaglianze dell’aritmetica in modulo per calcolare velocemente (a\*b) mod n**

(a\*b)mod n = [(a mod n) \* (b mod n)] mod n = 92

**8) Supponete di voler cifrare il messaggio 10101111, codificando il numero in notazione decimale corrispondente. Qual è?**

10101111=1+4+16+32+64+128=245

**9) In che modo l’hash di un messaggio fornisce miglior controllo dell’integrita rispetto ai checksum, come quello di Internet?**

Le funzioni hash prendono in input un messaggio di lunghezza variabile e danno in output un stringa di lunghezza prefissata, (risulta impossibile trovare 2 messaggi diversi che abbiamo come output della funzione hash la stessa stringa di lunghezza prefissata) che poi verrà cifrata con la chiave segreta del mittente, creando cosi il digest che il destinatario andrà a decifrare ritornando la funzione hash che dovrà,a sua volta, confrontare con la funzione hash creata a partire dal messaggio di invio (plaintext), verificandone cosi la corrispondenza.

Internet Checksum consiste nel trattare i caratteri come byte e sommarli a blocchi di 4. Il problema di questo checksum sta nel fatto che una stringa diversa potrà avere lo stesso checksum di una precendente, cosa che accade in maniera veramente rara con le funzioni hash.

**10) Potete decifrare l’hash di un messaggio per ottenere il messaggio originale? Argomentate la vostra risposta.**

La funzione hash è una funzione difficile da invertire. L'unico modo per ricreare i dati di input dall'output di una funzione di hash ideale è quello di tentare una ricerca forza-brut di possibili input per vedere se vi è corrispondenza.

**11) Considerate una variazione dell’algoritmo MAC nel quale il mittente invia (m,H(m)+s), dove H(m) + s è la concatenazione di H(m) +s. Tale variazione è corretta? Motivare la risposta.**

No, perché fare H(m)+s è diverso che fare H(m+s). La prima è una semplice concatenazione, la seconda risulta essere lo XOR tra messaggio m e secure secret s.

**12) Che cosa significa che un documento firmato deve essere verificabile e non falsificabile?**

Vuol dire che si deve consentire di dimostrare che un certo documento sia davvero stato firmato proprio da quella data persona (verificabile) e che solo lei poteva realizzarlo (non falsificabile)

**13) In che modo l’hash di un messaggio firmato con chiave pubblica fornisce una firma digitale migliore rispetto al messaggio cifrato con chiave simmetrica?**

DA CHIEDERE

**14) Supponete che Alice abbia un messagio pronto per essere inviato a chiunque lo richieda. Migliaia di persone lo vogliono,ma desiderano essere sicure dell’integrità del messaggio. In questo caso pensate sia meglio uno schema basato su MAC o sulla firma digitale?**

MAC, questo perché in questo caso dato che le persone sono molte, non conviene utilizzare la firma digitale che risulta essere più onerosa dato che deve richiedere l’infrastruttura di chiave pubblica PKI sottostante con le relative autorità di certificazione CA. Il MAC non utilizza ne chiave pubblica ne privata, ma basta aggiungere la chiave autenticazione (share secret) e prendiamo l’hash del risultato.

**15) Qual è lo scopo di un Nonce nei protocolli di autenticazione end-point?**

Nonce è numero di protocollo usato per assicareal ricevente che il mittente è ancora attivo.

**16) Perchè si dice che il Nonce è un valore che compare solo una volta? Nella vita di chi?**

Supponiamo che Alice debba inviare un messaggio a Bob. Bob sceglie il Nonce, R, e lo trasmette ad Alice. Alice utilizza la chiave simmetrica segreta che condivide con Bob, KA-B , per decodificare il Nonce,e gli ri-invia il valore risultante KA-B (R). Bob decifra il messaggio ricevuto e se il nonce è quello da lui inviato allora Alice è autenticata. Nonce compare solo una volta, cioè per verificare che quell’utente sia attivo e di conseguenza per l’autenticazione di esso e come visto è richiesto dal destinatario del messaggio.

**17) Supponete che Bob riceva messaggio PGP da Alice. Come fa Bob a essere sicuro che sia stata Alice a creare il messaggio, piuttosto che, per esempio, Trudy? PGP usa un MAC per l’integrità del messaggio?**

PGP usa la [crittografia a chiave asimmetrica](https://it.wikipedia.org/wiki/Crittografia_asimmetrica), nella quale il destinatario del messaggio ha generato precedentemente una coppia di chiavi collegate fra loro; una chiave pubblica ed una [privata](https://it.wikipedia.org/wiki/Chiave_privata). La chiave pubblica del destinatario serve al mittente per cifrare una chiave di sessione per un algoritmo di [crittografia simmetrica](https://it.wikipedia.org/wiki/Crittografia_simmetrica); questa chiave viene quindi usata per cifrare il testo in chiaro del messaggio. Molte chiavi pubbliche di utenti PGP sono a disposizione di tutti dai numerosi key server PGP sparsi per il mondo, che operano come mirror reciproci.

Il destinatario di un messaggio protetto da PGP decifra prima la chiave si sessione inclusa nel messaggio usando la sua chiave privata. Decifra poi il testo usando la chiave di sessione con l'algoritmo simmetrico. L'uso di due cifrature è giustificato dalla notevole differenza nella velocità di esecuzione tra una cifratura a chiave asimmetrica ed una a chiave simmetrica.

PGP inoltre fornisce anche un meccanismo di certificazione della chiave pubblica, diverso da quello convenzionale CA. Le chiavi pubblice di PGP sono verificate attraverso una rete di fiducia.