**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.

**18) Nei record SSL esiste un campo per numeri di sequenza SSL?**

Falso, i numeri di sequenza vengono inseriti nel campo MAC insieme al MAC, cioè ora il MAC è un hash didati cui si aggiunge la chiave MAC MC e il numero di sequeza corretto.

**20) Qual è lo scopo dei nonce casuali nell’handshake di SSL?**

I nonce dell’handshake di SSL vengono utilizzati per impedire la ripetizione delle connessioni, ma in particolare ache per la creazione delle chiavi si sessione.

**21) Supponete di stare inviando un flusso di pacchetti dall’Host A all’Host B usando Ipsec. Generalmente viene stabilita una nuova SA per ogni pacchetto inviato nel flusso. Vero o Falso?**

No perché Sa è persistente quindi rimane attiva durante tutta l’intera sessione, quindi non viene stabilita una nuova.

**22) Supponete che sia in esecuzione TCP su IPsec tra il quartier generale e la filiale. Se TCP ritrasmette lo stesso pacchetto, i 2 pacchetti corrisondenti inviati da R1 avranno lo stesso numero di sequenza nell’intestazione ESP. Vero o falso?**

No, perché anche se utilizzo TCP i numeri di sequenza relativi a IPsec sono indipendenti da esso; quindi in questo caso aumentano e non rimangono uguali

**23) Una SA IKE e una SA IPsec sono la stessa cosa?**

Assolutamente no. Prima di tutto la SA IKE è bidirezionale, invece la SA IPsec è unidirezionale. Inoltre sulla SA IKE vengono scambiate le chiavi per la cifratura e l’autenticazione della SA IKE e anche il master secret che verrà utilizzato per calcolare le chiavi relative a SA IPsec. Infine nella SA IKE vengono stabilit gli algoritmi che devono essere utilizzati dalla SA IPsec.

**24) Considerate WEP per 802.11. Supponete che i dati siano 10101100 e che la sequenza di chiavi generate sia 1111000. Qual è il testo cifrato risultante?**

Devo fare lo XOR → 10101100 XOR 1111000= 11010100

**25) In WEP viene mandato in chiaro un IV per ogni frame. Vero o falso?**

Vero, il valori di IV cambia da un frame all’altro e viene inserito nel plaintext nell’intestazione di ogni frame cifrato da WEP.

**26) In cosa consiste il paradosso del compleanno e per quale motivo è importante per la sicurezza delle funzioni hash? Spiegarlo attraverso un esempio.**

Il paradosso del compleanno afferma che la probabilità che in un insieme di persone ce ne siano almeno due che festeggiano il compleanno nello stesso giorno è molto più alta di quella che potrebbe sembrare intuitivamente, tanto da sembrare paradossale. Il paradosso è importante nel calcolo dell'impronta di un documento tramite funzione hash perché, sapendo che se ho un documento e ho una funzione hash come ad esempio DES a 64 bit, è abbastanza difficile trovare un documento con la stessa impronta, tuttavia se considero un insieme grande di documenti la probabilità che ve ne siano almeno due con la stessa impronta è troppo alta e rende la funzione inadeguata.

Il paradosso è usato per quantificare la validità della funzione hash.

Quante persone bisogna scegliere a caso affinché con prob.>0.5 ci sia una persona con lo stesso mio compleanno? 183

Quante persone bisogna scegliere a caso affinché con prob.>0.5 ci siano almeno due persone con lo stesso compleanno? 23.

Prob(scelgo t elementi diversi fra n)=(1- (t-1)/n) (1- (t-2)/n).... (1- 2/n) (1- 1/n)= exp(-t(t-1)/2n)

con t =23 e n=365 si ottiene prob. > 0.5

**27) Su cosa si basa la sicurezza di un algoritmo a chiave pubblica? Descrivere brevemente gli aspetti principali di RSA.**

La sicurezza si basa sul fatto che la decodifica si compie con la conoscenza di ben due chiavi, di cui una è di dominio pubblico, mentre l’altra la possiede solo il ricevente delle informazioni. Dunque i due individui si scambiano messaggi crittografati senza essersi mai scambiati la chiave di codifica (come avviene per la crittografia a chiave simmetrica).

Kpri(Kpub(mess))=mess

RSA è il metodo più usato per realizzare algoritmi asimmetrici:

scelgo p

scelgo q

n=p\*q

z=(p-1)(q-1)

*encryption:*

scelgo ‘e’ tale che e<n, MCD(e,z)=1 (‘e’ e ‘z’ non hanno fattori

comuni)

*decryption:*

scelgo ‘d’ tale che e\*d mod z=1

la chiave pubblica è Kpub=(n,e)

la chiave privata è Kpri=(n,d)

cifratura: c=me mod n

decifratura: m= cd mod n

**28) Assumete che un KDC server o un CA server si guasti. Chi può comunicare in modo sicuro e chi no nei due casi?**

Nel KDC le chiavi segrete sono esplicitamente di sessione quindi vengono usate in quella sessione e poi buttate. Nel KDC poi non ci sono i CA. Utilizzando KDC non possiamo fare nulla senza le chiavi sengrete che ci date da KDC.

Mentre se utilizziamo CA ormai la chiave pubblica l'abbiamo acquisita e non cambia poi così spesso. CA rimane in piedi e KDC no

**29) Dovete realizzare un sistema per l'autenticazione in una rete aziendale non connessa ad Internet a cui accedono soli 5 utenti. Che soluzione proporreste? Motivare la risposta.**

Poiché ci sono solo 5 utenti, io lascerei stare l'autenticazione intesa in senso classico ed utilizzerei un sistema con chiavi private. Infatti il solo fatto che due utenti conoscano la chiave privata da loro condivisa, ci assicura l'autenticazione. L'unico problema delle chiavi private è lo scambio delle chiavi e il numero delle chiavi: problema aggirabile perché, appunto, ci sono solo 5 utenti!

**30)Per quale motivo per firmare un documento è necessario prima ottenerne l'impronta attraverso una funzione di hash? Quali caratteristiche deve avere una funzione di hash?**

Le firme hash possono essere utilizzate per la creazione di firme digitali in quanto permettono la rapida creazione di firme digitali anche per file di grossa dimensioni.

E’ infatti più conveniente eseguire con rapidità un hashing del testo da firmare e poi autenticare solo quello piuttosto che eseguire algoritmi complessi di crittografia asimmetrica su moli di dati molto grandi.

La funzione crittografica di HASH deve avere 3 caratteristiche fondamentali:

1. Deve essere estremamente semplice calcolare un HASH da qualunque tipo di stato.

2. Deve essere estremamente difficile o quasi impossibile risalire al testo che ha portato ad un dato HASH.

3. Deve essere estremamente improbabile che due messaggi differenti, anche se simili, abbiano lo stesso HASH.

**31) Per quale motivo il protocollo rappresentato in figura 8.19 è da ritenersi insicuro? A che tipo di attacchi è soggetto? Come lo si può rendere sicuro? In cosa consiste l’attacco man in the middle, e come può essere evitato?**

→ MAN IN THE MIDDLE E PROTOCOLLO ap5.0

questo attacco avviene quando si adotta il protocollo ap5.0

1) Alice contatta Roberto

2) Roberto gli manda un nonce R

3) Alice gli manda KA pri (R)

4) Roberto si procura la chiave pubblica di Alice KA pub

5) Roberto calcola KA pub (KA pri (R)) e verifica che

KA pub (KA pri (R))=R

*Questo protocollo ha dei pro e dei contro:*

Pro) i due estremi della comunicazione non condividono segreti.

Contro) Risulta più facile l’intrusione da parte di terzi.

Infatti Tommaso può fingere di essere Alice procedendo in questo modo:

1) Tommaso contatta Roberto

2) Roberto manda un nonce R ad Alice e Tommaso lo intercetta.

3) Tommaso manda KT pri (R) a Roberto

4) Roberto richiede la chiave pubblica di Alice K pub , ma questa richiesta viene intercettata da Tommaso che gli manda la sua: KT pub

5) Roberto senza saperlo calcola KT pub (KT pri (R)) e verifica che KT pub (KT pri (R))=R

La falla del protocollo di autenticazione ap5.0 appena descritta può essere sfruttata da un malintenzionato per interporsi nella comunicazione in modo del tutto trasparente.

Per Alice e Roberto l’autenticazione è andata a buon fine, così credono che ciò che uno spedisce l’altro riceve ma in realtà non è così. Possiamo rendere sicuro il protocollo di autenticazione ap5.0

tramite la certificazione della chiave pubblica.

**32) Descrivere graficamente un metodo per il calcolo dell'impronta di un documento che utilizza DES (e calcola impronte di 64 bit). Infine spiegare in dettaglio perché impronte di 64 bit non sono considerate sicure (indipendentemente dal metodo utilizzato per il calcolo).**

Il DES è a chiave simmetrica e questa è già una limitazione per le applicazioni di rete, in più, considerando che quello che lavora a blocchi di 64 bit ha una chiave di 56 bit, si capisce facilmente che è soggetto ad attacchi a forza bruta.

Essendo a 56 bit le possibili chiavi sono solo 2^56 = 72'057'594'037'927'936

Quando il DES fu approvato come standard nel 1976, realizzare allora un elaboratore capace di provare tutte le possibili chiavi in un tempo ragionevole sarebbe costato una cifra irragionevole.

Impronte di 64 bit non sono sicure, perché in 2^33 tentativi si trovano due documenti con la stessa impronta, cosa che non vogliamo assolutamente.

