Gli aspetti di sicurezza

Corso Specialista Sistemi Ambiente Web

Chi sono Alice e Bob?

- Alice e Bob sono due persone che desiderano comunicare tra loro in maniera „sicura“;
- Alice e Bob possono essere due persone fisiche (amanti), due ditte (partner commerciali), oggetti fisici (routers, host), applicazioni (emails),...
- Le spie sono impersonate da personaggi con nomi meno fissi (Trudy, Mallory,...)
- Questi personaggi vengono adoperati per rendere più concreti e vivaci gli esempi della materia.

La comunicazione sicura (1/7)

- Di quali elementi consiste la comunicazione sicura?
  - La riservatezza;
  - L‘autenticazione;
  - L‘integrità;
  - Il non-disconoscimento.

La comunicazione sicura: la riservatezza (2/7)

- La riservatezza: il contenuto dei messaggi scambiati deve essere accessibile solo ad Alice e a Bob. La riservatezza richiede una qualche forma di cifratura per evitare che un intruso possa leggere e comprendere il contenuto del messaggio che sia riuscito ad intercettare;
- La riservatezza del contenuto di un messaggio viene percepita sovente come l'elemento più importante nella comunicazione sicura, ma vedremo subito altri aspetti non meno importanti;

La comunicazione sicura: la riservatezza (3/7)

- Inoltre la riservatezza riguarda a volte non solo il contenuto dei messaggi scambiati tra due persone, ma anche il semplice fatto che queste due persone sono in contatto tra di loro!

La comunicazione sicura l'autenticazione (4/7)

- L'autenticazione: accertamento dell'identità della persona con cui noi scambiamo informazioni;
- Nei rapporti umani l'autenticazione è immediata e si fonda sovente su informazioni biometriche (riconoscimento visivo, riconoscimento voce), sul riconoscimento della scrittura,...
- Nei rapporti ufficiali (amministrativi) l'autenticazione ha luogo tramite documenti a noi rilasciati da autorità delegate per tale scopo: uffici comunali, questura, Kreisbüros...

La comunicazione sicura: l‘autenticazione (5/7)

- Nel caso di autenticazione in area tecnica (accesso a computer, accesso a risorse, accesso tramite rete di computers) le problematiche di autenticazione sono tutt‘altro che banali!
- Esse adoperano i protocolli di autenticazione (messaggi scambiati secondo procedure predefinite e verificabili).

La comunicazione sicura: l‘integrità (6/7)

- L‘integrità: assicura Alice e Bob che il file non sia stato oggetto di modifiche accidentali o volute durante il transito („autenticazione di messaggio“);
- Le tecniche adoperate vanno oltre a quelle adoperate per scopi puramente tecnici (checksum di Internet, CRC) e servono a coprire anche modifiche attuate per scopi fraudolenti;

La comunicazione sicura: il non-disconoscimento (7/7)

- Il non-disconoscimento: è un tema importante per le transizioni di tipo commerciale. L‘autore non può deve poter ripudiare di aver trasmesso un messaggio con un determinato contenuto.

La sicurezza in Internet

- La sicurezza in Internet è messa a repentaglio da diversi strumenti e metodi (ad esempio):
  - Packet sniffer;
  - Falsificazione indirizzi MAC;
  - Falsificazione indirizzi IP;
  - Attacchi: Denial of Service.

Packet sniffer (1/2)

- I packet sniffer: si tratta di programmi che ricevono in modo passivo i pacchetti che attraversano la scheda di rete e li memorizzano;
- La riscostruzione avviene per il tramite di programmi dedicati;

Packet sniffer (2/2)

- Presuppongono un ambiente di rete condiviso (p.es Ethernet) e intercettano i pacchetti in transito settando la scheda di rete nel modo “promiscuo”;
- L’uso di un’infrastruttura di rete locale basata su switches rappresenta una buona barriera per questo genere di tecniche di intrusione passiva.

Falsificazione indirizzo MAC

- Il PC attaccato riceve un indirizzo MAC fraudolento associato a l'indirizzo IP di una stazione della rete (ad es. server);
- In tal modo il computer attaccante registra i dati inviati dal computer attaccato al server;

Falsificazione indirizzo IP (1/2)

- Il PC mittente maschera la propria vera identità e si presenta con l'identità di un altro indirizzo IP;
- Il PC indirizzato verifica l'appartenenza dell'indirizzo IP ad un intervallo da lui riconosciuto come "amico", lo autentica e inizia lo scambio dati;
- Questo tipo di attacco (frode di indirizzo IP) mette in rilievo come gli indirizzi IP pubblici usati da una ditta sono materiale sensitivo!

Falsificazione indirizzo IP (2/2)

- La falsificazione dell'indirizzo IP viene in generale adoperata assieme ad altre tecniche di attacco ("denial of service");
- Esempio: un grande numero di host "innocenti" possono ricevere un pacchetto di "echo request" (ping) da un mittente con indirizzo falsificato. L'host il cui indirizzo IP e' stato falsificato riceverà un grandissimo numero di pacchetti "echo replay" mai richiesti.

Attacco: Denial of Service

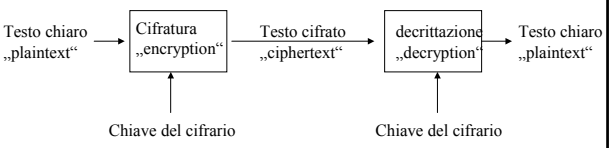
- Il server attaccato riceve un grandissimo numero di richieste per stabilire una connessione TCP (pacchetti con flag SYN settato e differenti indirizzi IP);
- Il server accetta la richiesta, alloca le necessarie risorse e chiede a sua volta al partner di aprire la connessione;
- A questa richiesta non viene mai data risposta!
- Il server resta bloccato dovendo gestire un grandissimo numero di connessioni.

Le tecniche crittografiche

Chi utilizza la crittografia?

- In altre parole chi ha interessa a mantenere riservato il contenuto dei messaggi scambiati:
  - I militari;
  - I corpi diplomatici;
  - I diaristi;
  - Gli amanti.

Visione di insieme dei termini crittografici



Chiave del cifrario

Chiave del cifrario

La crittografia ha lo scopo di mantenere nascosto, riservato il contenuto di testi; la crittoanalisi ha lo scopo di svelare ciò che la crittografia vuole tenere nascosto e le due discipline sono note assieme come crittologia

Le metodologie per decifrare un codice (1/2)

- Attacco della forza bruta:
  - consiste nell‘uso sequenziale di tutte le possibili chiavi;
- Attacco a solo testo cifrato:
  - nulla si conosce sul contenuto del messaggio in „testo chiaro“ e si deve lavorare esclusivamente sul „testo cifrato“;

Le metodologie per decifrare un codice (2/2)

- Attacco a testo chiaro conosciuto:
  - si conoscono porzioni del „testo chiaro“ da comparare con il „testo cifrato“;
- Attacco a testo chiaro scelto:
  - è possibile generare a piacere da qualsiasi „testo chiaro“ campioni di „testo cifrato“ .

Crittografia a chiave segreta (simmetrica)

- Si fonda sull'idea che i due partner debbano essere in possesso della medesima informazione (chiave segreta, "secret key") per poter codificare e decodificare i dati;

Crittografia a chiave segreta (simmetrica)

- I metodi antichi:
  - I metodi di sostituzione;
  - I metodi di transposizione;
- I metodi moderni:
  - DES (Data Encryption Standard), metà anni '70;
  - IDEA (International Data Encryption Algorithmus).

Un metodo di sostituzione che risale a Giulio Cesare (1/3)

- Giulio Cesare ha usato un codice che sostituiva ad ogni cifra quella che veniva 3 posti dopo nell'alfabeto :
  - d -> A, e -> B, f -> C,…z->W;
- Con il cifrario "Giulio Cesare" la parola "attacco" diventa "XQQXZZL";

Un metodo di sostituzione che risale a Giulio Cesare (2/3)

- Più in generale: Una lettera dell'alfabeto viene sostituita con la lettera situata k posti dopo (l'alfabeto viene considerato come una struttura circolare, cioè dopo la Z si ricomincia con la A);
- K rappresenta la chiave del cifrario;
- Quante chiavi differenti possiede questo metodo crittografico? Ipotesi: viene adoperato l'alfabeto italiano esteso…)

Un metodo di sostituzione che risale a Giulio Cesare (3/3)

- Nel metodo di Giulio Cesare vediamo già accennata l'idea di base delle tecniche crittografiche, quella di separare:
  - Il metodo;
  - La chiave.

Un altro metodo di sostituzione apparentemente più raffinato

- Un metodo apparentemente più raffinato si ottiene facendo corrispondere ad ogni lettera dell'alfabeto del testo chiaro un'altra lettera dell'alfabeto secondo uno schema casuale (l'ordine alfabetico non è più mantenuto);
- La chiave è la stringa delle lettere dell'alfabeto a cui le lettere dell'alfabeto del testo chiaro vengono fatto corrispondere;
- Per l'alfabeto italiano esteso è possibile stabilire 26! (si legge 26 fattoriale) chiavi!

Cifrario Monoalfabetico (1/2)

- Il metodo di Giulio Cesare e gli altri da esso derivati operano secondo il medesimo modello: Una lettera dell'alfabeto viene sostituita da un'altra lettera secondo uno schema predefinito (cifrario monoalfabetico);
- Questi testi possono essere analizzati e decodificati in maniera semplice con tecniche di valutazione statistica (tasso di ripetizione di determinate lettere, coppie di lettere, terne di lettere in una lingua e ricerca di tali frequenze nel testo cifrato).

Cifrario Monoalfabetico (2/2)

- In altre parole: il grado di "confusione" introdotto non è adeguato per resistere ad attacchi a "testo cifrato" focalizzati sulla ricerca di sequenze statistiche.

Cifrario Polialfabetico (1/2)

- Si adoperano differenti cifrari monoalfabetici con una sequenza di ripetizione definita (es. metodo di Vigenére)
- In tal modo si creano cifrari polialfabetici.

Metodo di Vigenére (2/2)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

I metodi di trasposizione (1/3)

- I cifrari di sostituzione conservano l'ordine dei simboli del testo chiaro, ma li camuffano;
- I cifrari di trasposizione riordinano le lettere del testo chiaro senza alterarle („trasposizione per colonne");

I metodi di trasposizione (2/3)

Mi sono stancato di lavorare alla Swisscom						
l	u	s	t	r	o	
m	i	s	o	n	o	
s	t	a	n	c	a	
t	o	d	i	l	a	
v	o	r	a	r	e	
a	l	l	a	s	w	
i	s	s	c	o	m	
mstvaioaaewmnclrsosadrlsoniaacitools						

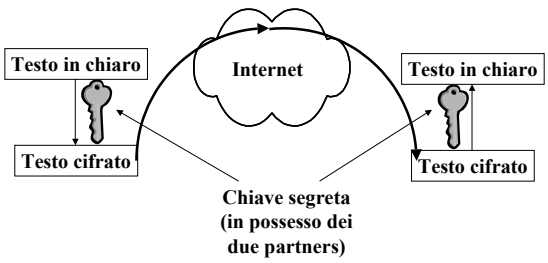
I metodi di trasposizione (3/3)

- I metodi di trasposizione possono essere applicati successivamente incrementando in tal modo il grado di „confusione“ del testo originario (testo piano) rispetto al testo cifrato.

I metodi moderni a chiave segreta

- I metodi moderni sfruttano le possibilità di calcolo dell‘hardware dedicato o del software e impiegano numerosi passi di sostituzione e trasposizione incrementando in tal modo la „confusione“ del testo originario

Cifratura a chiave segreta (simmetrica)



Data Encryption System (DES) (1/4)

- DES è stato accettato come standard per la cifratura digitale nel 1977 e confermato (per una ultima volta nel 1993) per altri cinque anni;
- DES appartiene alla famiglia dei cifrari a blocchi perchè vanno ad agire su blocchi di bit e non su singoli bit;
- DES relizza una serie di cicli di trasposizione e di sostituzione operando su blocchi di 64 bit (8 bytes) per volta, con una chiave di 64 bits (in reraltà 56 bits essendo 8 bits di parità);

Data Encryption System (DES) (2/4)

- Nel caso (quello più comune) in cui la quantità da cifrare è più lunga di 64 bits, i diversi blocchi vengono combinati tra loro (ad esempio chipher-block chaining);
- Una chiave di 56 bits non è più considerata adeguata oggi in rapporto alla potenza di calcolo disponibile (attacchi a forza bruta);

Data Encryption System (DES) (3/4)

- In tal caso è possibile far correre l'algoritmo ripetutamente prendendoi 64 bit all'uscita di una iterazione DES come ingresso della prossima iterazione DES adoperando ogni volta una chiave diversa (p.es. 3DES);
- La variante 3DES è oggi estremamente diffusa in e viene sostituita solo molto lentamente dal nuovo Advanced Encryption Standard (AES) Rijaendel;

Data Encryption System (DES) (4/4)

- In linea con le moderne teorie crittografiche l'algoritmo DES è pubblico e la criticità è posta nella chiave che non deve essere accessibile ad estranei.

International Data Encryption Algorithm (IDEA)

- IDEA è stato proposto nel1991 da Lai e Massey (Politecnico Zurigo) in alternativa a cifrari soggetti a disposizioni legislative americane;
- Come il DES è un cifrario a blocchi, ma ha una chiave di 128 bit.

Limitazione della chiave segreta in un contesto globalizzato (1/3)

- I due partners si devono "incontrare" per potersi scambiare l'informazione ("chiave segreta") da condividere;
- Nel 1976 Diffie ed Hellman dimostrarono con metodi matematici come sia possibile costruire una chiave privata senza "incontrarsi"!

Limitazione della chiave segreta in un contesto globalizzato (2/3)

- Una altra alternativa è quella di rivolgersi ad un Thrusted Third Parthy (TTP) che genera e distribuisce le chiavi ai due partners che devono comunicare tra loro;
- Il TTP viene anche definito Key Distribution Center (KDC) ;
- UN KDC puo' svolgere addizionalmente la funzione di "key escrow", ma ciò lo rende un obiettivo attrattivo;

Limitazione della chiave segreta in un contesto globalizzato (3/3)

- Il numero delle chiavi per comunicare tra partners aumenta secondo la legge matematica N * (N-1) / 2, dove N è il numero dei partners!

Gli altri aspetti della sicurezza con la chiave segreta (1/2)

- L'autenticazione : viene ottenuta in maniera indiretta in quanto il nostro partner condivide con noi una chiave segreta, non nota ad altri; cio' viene sfruttato in protocolli nei quali un partner sfida l'altro a cifrare (con la chiave segreta) numeri casuali;

Gli altri aspetti della sicurezza con la chiave segreta (2/2)

- L‘integrità: viene ottenuta trasmettendo assieme al messaggio la sua impronta digitale cifrata (e combinata con la chiave segreta);
- Il non-disconoscimento: l‘autore non puo disconoscere di aver trasmesso un file => non è ottenibile dalla cifratura a chiave segreta.

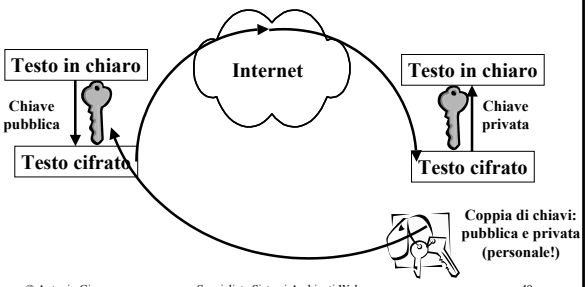
I metodi a chiave pubblica (asimmetrici) (1/8)

- Idea: viene adoperata una coppia di chiavi (“chiave pubblica” e “chiave privata”). Queste due chiavi sono legate tra loro nel processo matematico di generazione;
- Messaggi generati con la chiave pubblica possono essere letti solo con la chiave privata;
- Messaggi generati con la chiave privata possono essere letti solo con la chiave pubblica;

I metodi a chiave pubblica (asimmetrici) (2/8)

- Le leggi matematiche adoperate garantiscono che una persona non possa risalire computazionalmente dalla chiave pubblica alla chiave privata in maniera „elementare“;

I metodi a chiave pubblica (asimmetrica) (3/8)



I metodi a chiave pubblica (asimmetrici) (4/8)

- Con la crittografia a chiave pubblica la problematica della distribuzione della chiave segreta scompare di colpo;
- La chiave pubblica non è soggetta ad alcun vincolo di confidenzialità; anzi è interesse del possessore di farla conoscere ai propri partners;
- La chiave privata deve restare invece strettamente confidenziale e deve essere protetta con attenzione dal possessore pena la perdita della confidenzialità e la possibilità di perpetrare frodi;

I metodi a chiave pubblica (asimmetrici) (5/8)

- Similmente l'altra problematica della crittografia a chiave segreta, la crescita con legge quadratica del numero di chiavi segrete da gestire, che rende di fatto non praticabile l'uso della crittografia segreta in un ambito commerciale globale, è risolto: Una unica chiave pubblica per tutti i propri partners!

I metodi a chiave pubblica (asimmetrici) (6/8)

- Da notare: la crittografia a chiave pubblica presuppone comunque due coppie di chiavi per la comunicazione tra due partners (confidenzialità a due vie).

I metodi a chiave pubblica (asimmetrici) (7/8)

- La crittografia a chiave pubblica presenta proprietà che la rendono appropriata non solo per realizzare la riservatezza, ma anche per la firma digitale (autenticazione della persona e del contenuto del messaggio, non-ripudiazione dei documenti), basilare per lo sviluppo del commercio elettronico;

I metodi a chiave pubblica (asimmetrici) (8/8)

- I metodi a chiave pubblica non vengono oggi considerati alternativi a quelli a chiave segreta, ma complementari;
- In considerazione dei minori tempi di calcolo la cifratura a chiave segreta continua ad essere adoperata usando la critttografia a chiave pubblica per lo scambio della chiave segreta;

La cifratura RSA (1/2)

- La cifratura a chiave pubblica si identifica con il metodo RSA (Ron Rivest, Adi Shamir, Leonard Adlemann)
- Nel metodo RSA vanno tenute distinte le due componenti:
  - La generazione della coppia di chiavi tra loro collegate matematicamente (pubblica, privata);
  - L'uso delle due chiavi per la cifratura e decifratura.

La cifratura RSA (2/2)

- La lunghezza della chiave per la crittografia a chiave pubblica non ha relazione con la lunghezza della chiave per la crittografia a chiave segreta;
- RSA richiede oggi una lunghezza di 1024 e 2048 bit;

I metodi di codifica ibridi

- I metodi di codifica ibridi vengono oggi adoperati in Internet per sfruttare i vantaggi dei metodi a chiave pubblica e chiave privata;
- Il mittente genera una chiave segreta valida limitatamente alla sessione in corso;
- Il ricevente riceve il messaggio cifrato con la chiave e la chiave medesima cifrata con la sua chiave pubblica.

Firma digitale (1/5)

- La firma apposta sotto un documento è verificabile, non falsificabile, non ripudiabile;
- La firma digitale deve fornire un equivalente elettronico della firma apposta sotto i documenti;
- La crittografia a chiave pubblica si presta in maniera ottimale per autenticare un documento e raggiungere un grado di sicurezza anche superiore alla firma ordinaria;
- Per la firma digitale viene adoperata la cifratura RSA (in senso inverso) e il metodo DSA;

Firma digitale (2/5)

- Il messaggio viene firmato da Alice codificandolo con la propria chiave privata; Bob lo potrà verificare decodificandolo con la chiave pubblica di Alice;
- Questa procedura non è pratica perchè è lenta e produce un grande volume di dati;
- Idea per un‘alternativa: si calcola l‘impronta digitale del documento tramite una funzione di hash („message digest“) e si codifica con la chiave segreta solo l‘impronta;

Firma digitale (3/5)

- (Passo 1) Si fa corrispondere al messaggio una sua “versione compressa” adoperando la funzione hash;
- (Passo 2) Alice firma digitalmente il “messaggio compresso” (lo codifica con la propria chiave privata) e lo invia con il messaggio in testo chiaro a Bob;
- (Passo 3) Bob riceve i due messaggi e genera dal messaggio in testo chiaro la versione compressa adoperando la medesima funzione di hash che Alice;

Firma digitale (4/5)

- (Passo 4) Bob verifica la firma di Alice decodificando con la chiave pubblica di Alice il "messagio compresso" ricevuto.
- (Passo 5) Bob compara il "messaggio compresso" da lui generato con quello ricevuto e verificato (decodificato con la chiave pubblica di Alice); se essi sono identici Bob considera il messaggio in testo chiaro ricevuto come autentico di Alice e non alterato nel contenuto.

Firma digitale (5/5)

- I passi 3, 4, e 5 sono noti come "verifica" della firma digitale;
- Alice non potrà in futuro ripudiare il messaggio trasmesso in quanto la versione compressa (quasi impronta digitale del messaggio) è firmata con la sua chiave privata.

La funzione di hash (1/5)

- Come viene ottenuto un „messaggio compresso"?
- Generare la versione compressa del messaggio („message digest") presenta similarità con i metodi per generare la checksum Internet, proiettando un messaggio di lunghezza arbitraria in una stringa di lunghezza prefissata (hash);

La funzione di hash (2/5)

- Questa stringa rappresenta „un‘impronta digitale“ del messaggio e viene definita valore di hash o checksum crittografico;
- L‘Internet checksum non si presta per la firma digitale in quanto è computazionalmente facile trovare un secondo documento con la stessa impronta;

La funzione di hash (3/5)

- La funzione “hash” deve soddisfare a queste condizioni:
  - Non e’ computazionalmente possibile dato un valore hash, costruire un messaggio il cui hash corrisponda a tale valore (funzione non invertibile);
  - Non e’ computazionalmente possibile dato un messaggio avente un valore hash costruire un secondo messaggio avente il medesimo hash (funzione debolmente priva di collisioni);
  - Non e’ computazionalmente possibile trovare due messaggi aventi il medesimo valore hash (funzione fortemente priva di collisioni);

La funzione di hash (4/5)

- Espresso ancora in termini differenti si puo’ dire che il ”message digest” protegga il messaggio originario;

Gli algoritmi per l'hash (5/5)

- Gli algoritmi oggi diffusi per generare l'hash:
  - MD5 (Message Digest), output a 128 bit, di Ron Rivest
  - SHA-1 (Secure Hash Algorithm), output a 160 bit
- Questi algoritmi accettano come ingresso messaggi di lunghezza arbitraria e forniscono in uscita un valore di lunghezza costante (si parla di "impronta digitale").

Una osservazione: il paradosso del compleanno

- Quante persone bisogna scegliere a caso affinchè con Prob > 0.5 ci sia una persona con lo stesso mio compleanno? Risposta:183;
- Quante persone bisogna scegliere a caso affinchè con Prob > 0.5 ci siano almeno due persone con lo stesso compleanno. Risposta: 23!

La necessità di un intermediario di fiducia (1/6)

- La crittografia a chiave pubblica supera la difficoltà della crittografia a chiave segreta attinente lo scambio della chiave in modo riservato, ma …
- La crittografia a chiave pubblica soffre di una criticità attinente il legame tra identità di una persona e la sua chiave pubblica; tale criticità è nota nella letteratura come l'attacco dell'uomo in mezzo ("man-in-the-middle");

La necessità di un intermediario di fiducia (2/6)

- Esempio:
  - Trudy "l'uomo in mezzo" ordina una pizza al negozio di Alice che accetta ordini elettronici dando come recapito quello di Bob;
  - Trudy firma il messagio in modo digitale (adopera la propria chiave privata) e invia il messaggio ad Alice aggiungendo la propria chiave pubblica, in modo che la firma possa essere verificata;
  - Alice verifica la firma e esegue l'ordine inviando a Bob una pizza mai ordinata!

La necessità di un intermediario di fiducia (3/6)

- Punto cruciale: certezza del legame tra la persona (entità) e la sua chiave pubblica;
- I certificati digitali facilitano la verifica del legame tra chiave pubblica e l'entità;
- Un certificato digitale ha le caratteristiche di un documento di riconoscimento ufficiale (p.es patente di guida) ed è formato da due parti, una parte testuale, cioè leggibile, e il corrispondente "hash" firmato in modo digitale dalla CA;

La necessità di un intermediario di fiducia (4/6)

- Il certificato digitale presuppone di delegare ad un „intermediario di fiducia" la verifica del legame tra una persona e la sua chiave pubblica;
- La fiducia nell'ente certificatore viene per cosi dire trasferita sul soggetto certificato;

La necessità di un intermediario di fiducia (5/6)

- Più in generale gli utenti hanno i seguenti bisogni:
  - Poter scaricare chiavi pubbliche (verificabili) di agenti mercantili operanti in rete e di altri partners con cui desiderano scambiare informazioni riservate; -bisogno di utilizzatore
  - Poter far certificare la propria chiave pubblica e poterla collocare in rete a disposizione dei propri partners; - bisogno di soggetto
  - Essere tenuti informati sull'eventuale prematuro ritiro di certificati; - bisogno di utilizzatore;

La necessità di un intermediario di fiducia (6/6)

- Creazione e gestione dei certificati digitali è il compito di sistemi noti come Public Key Infrastructure (PKI);
- I due PKIs più diffusi sono oggi X.509 e Pretty Good Privacy (PGP);
- X.509 è nato come una raccomandazione dell'ITU e ulteriori sviluppi sono stati svolti dall'IETF; esso ha un carattere di maggiore ufficialità che PGP e su di esso vengono concentrati numerosi sforzi.

PKI X.509 (1/8)

- All'interno di PKI X.509 è possibile distinguere una Certification Authority, (CA) per la creazione e la gestione dei certificati (Software) ed una Registration Authority (RA) per la verifica delle generalità dei richiedenti ed altri compiti amministrativi (Entità umana);
- La CA presenta una certa analogia con il Key Distribution Center della crittografia a chiave segreta;

PKI X.509 (2/8)

- Il primo passo nella fase di vita di un certificato digitale è la verifica dell'identità del richiedente;
- La verifica puo' essere eseguita con operazioni di differente complessità e differente costo;
- La verifica a distanza per il tramite di posta elettronica o di carta di credito porta a certificati „di basso profilo", che non forniscono „dimostrazione dell'identità" (citato VeriSign);

PKI X.509 (3/8)

- La verifica di persona con documenti di identità viene richiesta per certificati di „alto profilo"; la PKI può delegare la verifica ad una „registration authorithy" (RA) locale;
- Se la PKI non genera la coppia di chiavi (pubblica, privata) , essa deve verificare che il richiedente possieda la chiave privata corrispondente alla chiave pubblica da certificarsi („protocolli di sfida");

PKI X.509 (4/8)

- Lo standard X.509 definisce i campi di un certificato digitale e regola le procedure alle quali un a CA deve sottostare;

PKI X.509 (5/8)

- I seguenti campi sono obbligatori:
  - Numero versione X.509;
  - La chiave pubblica dell'oggetto del certificato insieme all'indicazione dell'algoritmo della chiave;
  - Numero di serie del certificato;
  - Identificatore unico dell'oggetto (distinguished name)
  - Periodo di validità del certificato;
  - Identificatore unico dell'ente emittente il certificato
  - Firma digitale dell'ente emittente;
  - Identificatore dell'algoritmo di firma digitale;

PKI X.509 (6/8)

- Una CA possiede una chiave privata con cui essa firma digitalmente i certificati ed una propria chiave pubblica (certificata!) con cui i propri clienti verificano la firma digitale dei certificati emessi dalla CA;
- All'inizio della catena („catena di fiducia") si trova una „CA radice" che certifica se stessa per il tramite di un „certificato radice" in cui l'ente emittente e il soggetto certificato coincidono!

PKI X.509 (7/8)

- La memorizzazione dei certificati e della chiave pubblica non presenta criticità particolari e vengono adoperati server dedicati;
- I certificati possono essere revocati prima del tempo di scadenza (esempi: uscita di un collaboratore da una ditta; chiave privata compromessa);
- I certificati revocati vengo inseriti in una lista "certificate revocation list " (CRL) con gestione in modalità polling o in modalità push;

PKI X.509 (8/8)

- Una Certification Authority pubblica le proprie direttive interne in un documento intitolato Certification Practice Statement (CPS);
- In tale documento viene regolato come i clienti vengono autenticati, come i certificati vengono emessi, ecc.

Pretty Good Privacy (1/6)

- Pretty Good Privacy (PGP) è una PKI che rinuncia all'idea della gestione centralizzata dei certificati;
- Philip Zimmermann, il padre di PGP, voleva dare alla collettività la possibiltà di scambiare informazioni in maniera protetta;
- Philip fu coinvolta durante gli anni 90 in una lunga serie di inchieste da parte delle autorità americane quale mercante di armi per aver messo a disposizione in Internet i metodi di cifratura di PGP;

Pretty Good Privacy (2/6)

- La differenza chiave tra X.509 e PGP:
  - in X.509 l'oggetto del certificato è in generale diverso da chi emette il certificato;
  - in PGP l'oggetto del certificato coincide sempre con chi emette il certificato (Autocertificazione);

Pretty Good Privacy (3/6)

- I seguenti campi sono obbligatori:
  - Numero versione PGP;
  - La chiave pubblica dell'oggetto del certificato insieme all'indicazione dell'algoritmo a cui la chiave si riferisce;
  - Informazioni di identità;
  - Firma digitale del proprietario del certificato;
  - Periodo di validità del certificato;
  - Algoritmo preferito di cifratura simmetrica per la chiave;

Pretty Good Privacy (4/6)

- Firme digitali apposte da persone che hanno verificato la validità dell'asserzione del certificato;

Pretty Good Privacy (5/6)

- Come si crea la fiducia nel certificato attestante il legame tra chiave pubblica ed entità?
- Per il tramite di atti di fiducia diretta (tra coppie di persone) che a poco a poco cresce in una „trust network" (rete di fiducia)!

Pretty Good Privacy (6/6)

- Gli utenti PGP hanno la possibilità di depositare copie dei propri certificati in banche dati da cui gli utilizzatori li possono scaricare;
- La revoca del certificato è a carico del proprietario o persona delegata.

Attacchi ai certificati digitali

- Attacchi ai certificati digitali sono possibili con le modalità seguenti:
  - Far certificare una identità falsa presentando una documentazione falsificata;
  - La CA si comporta in maniera fraudolenta;
  - Sostituzione di chiave pubblica nel computer della persona attaccata;
  - Ottenere la chiave privata di una CA.

S/MIME (1/3)

- MIME (Multipurpose Internet Mail Exchange) ha esteso la specifica iniziale RFC822 per il formato dei messaggi di posta elettronica;
- In RF822 il messaggio è definito con una struttura fatta di una intestazione e da un corpo;

S/MIME (2/3)

- Il blocco di intestazione è fatto di linee (linee di intestazione) costruite da “tag”, doppio punto, valore del tag e uno o piu’ parametri (opzionali);
- S/MIME ha introdotto nuove varianti per il tipo ed il sottotipo come segue:

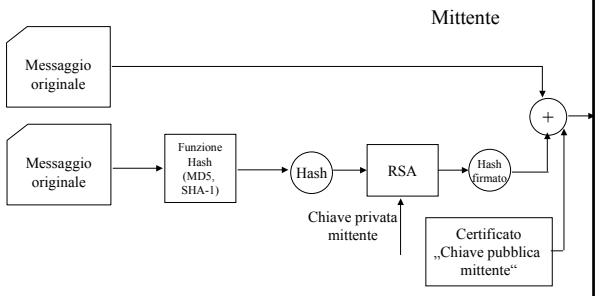
S/MIME (3/3)

Tipo	Sottotipo	Parametro Smime	Descrizione
Multipart	Signed		Un messaggio firmato in testo chiaro fatto di due parti: messaggio e e firma.
Application	Pkcs7-mime	signedData	Una entità S/MIME firmata.
Application	Pkcs7-mime	enveloppedData	Una entità S/MIME cifrata.
Application	Pkcs7-mime	degenerate SignatedData	Una entità contenente solo certificati a chiave pubblica.
Application	Pkcs7-signature		
Application	Pkcs10-mime		Messaggio richiesta di registrazione certificato.

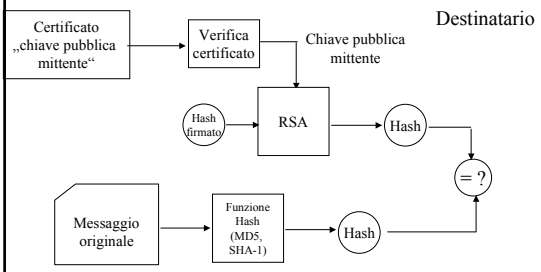
S/MIME: Firma digitale (1/3)

- Firma digitale: presuppone che il mittente possegga una coppia di chiavi (privata & pubblica) e che la chiave pubblica sia certificata secondo lo standard X.509;
- Il SW del client genera l’hash del messaggio (funzione di hash!), la codifica con la chiave privata e la combina con il messaggio originale;

S/MIME: Firma digitale (2/3)



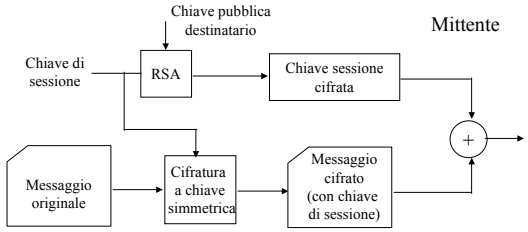
S/MIME: Firma digitale (3/3)



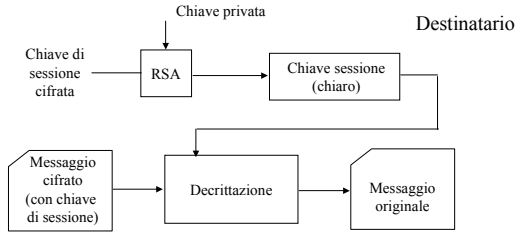
S/MIME: Cifratura (1/3)

- Cifratura: presuppone che il mittente possegga la chiave pubblica del destinatario (certificato digitale);
- Il SW del client genera una chiave di sessione (“usa e getta”), cifra il messaggio con questa chiave di sessione, che poi viene cifrata con la chiave pubblica del destinatario (“avvolgere la chiave”);

S/MIME: Cifratura (2/3)



S/MIME: Cifratura (3/3)



S/MIME e i Clients Email

- S/MIME è supportato da Outlook, Outlook Express, Netscape;
- L'utente ha la possibilità di configurare il Client per la firma/cifratura di tutti i messaggi in uscita o puo' configurare il singolo messaggio;
- L'agenda di Outlook e di Outlook Express consente la gestione dei certificati dei propri partners;
- Il proprio certificato è memorizzato nell'archivio certificati del browser.

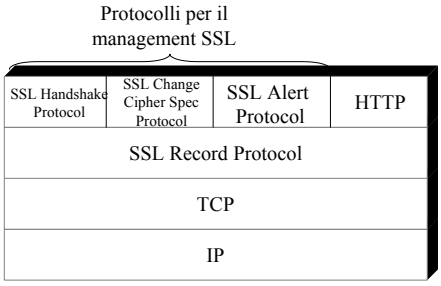
Secure Sockets Layer (SSL) (1/9)

- Visione d'insieme:
  - Bob clicca su una pagina sicura, ospitata dal server di Alice (il protocollo per accedere a tale pagina è „https“);
  - Ha luogo una fase di negoziazione tra client (browser) e server;
  - Terminata questa fase client (browser) e server dispongo di una chiave di sessione con la quale vengono autentificati e cifrati i messaggi scambiati tra di loro;

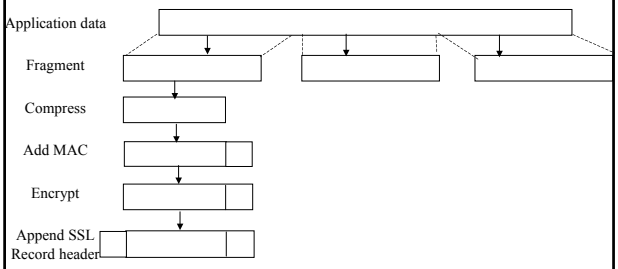
Secure Sockets Layer (SSL) (2/9)

  - SSL rappresenta un livello ulteriore tra livello di trasporto e livello applicativo per lo scopo della sicurezza;
- SSL è nato per iniziativa di Netscape ed è giunto nel frattempo alla versione 3.0;
- Lo standard IETF derivato da SSL è chiamato TSL (Transport Secure Layer) e può essere considerato come un SSL v. 3.1;

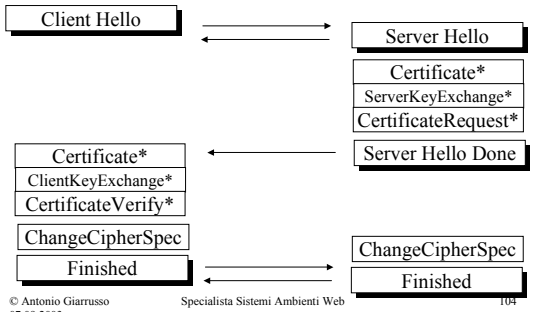
Secure Socket Layer (3/9)



Secure Socket Layer (4/9)



Secure Socket Layer (5/9)



Secure Sockets Layer (SSL) (6/9)

- Prima fase, Negoziato funzioni crittografiche:
  - Il browser invia al server la versione SSL preferita, le preferenze crittografiche (CipherSuites), gli algoritmi di compressione disponibili;
  - Il server invia al client i parametri da adoperare: versione SSL, il metodo per lo scambio delle chiavi e le funzioni crittografiche (CipherSuite) e i metodi di compressione da adoperarsi per la connessione;

Secure Sockets Layer (SSL) (7/9)

- Seconda fase, Autenticazione server e chiavi server
  - L'andamento di questa fase dipende dalle scelte fatte a riguardo dello scambio chiave;
  - Se richiesto dal CipherSuite, il server invia al client il proprio certificato X.509, le chiavi che il cliente deve adoperare, richiedere eventualmente la richiesta certificato del client;

Secure Sockets Layer (SSL) (8/9)

- Terza fase: Autenticazione cliente e chiavi client
  - Il browser soddisfa una eventuale richiesta di certificato X.509 da parte del server, trasmette le chiavi, genera il Pre-Master secret, una chiave segreta di sessione, conferma della autenticità del proprio certificato;
  - Al termine della fase 3 client e server sono in grado di generare il premaster-secret dal quale vengono generate le diverse chiavi per cifratura, MAC e inizializzazione degli algoritmi;

Secure Sockets Layer (SSL) (9/9)

- Quarta fase, Finale
  - Il browser informa il server che da ora in poi i messaggi saranno cifrati con la chiave di sessione e comunica in un separato messaggio (cifrato) la fine della fase di negoziazione;
  - Il server informa il browser che da ora in poi i messaggi saranno cifrati con la chiave di sessione e comunica in un separato messaggio (cifrato) la fine della fase di negoziazione;
- La sessione SSL ha inizio, tutti i messaggi vengono autenticati e cifrati con le rispettive chiavi di sessione

IP Security (IPSec)

IPSec Generalità (1/4)

- IP security (IPSec, IPsec) è un insieme di protocolli finalizzati a realizzare una comunicazione sicura a livello di rete;
- La famiglia dei protocolli IPsec è un tema assai complesso ed è definito in più di una dozzina di RFCs.
- Due RFC fondamentali sull'argomento sono l'RFC 2401, che descrive l'architettura funzionale, e l'RFC 2411, che fornisce un quadro d'insieme dei documenti di definizione;

IPSec Generalità (2/4)

- IPsec può fornire riservatezza e/o autenticazione a livello di rete;
- In altre parole la riservatezza non riguarda un'applicazione od un protocollo particolari veicolati tramite IP (TCP, UDP, ICMP), ma tutti i contenuti trasportati nei pacchetti IP;
- Parimenti l'host di destinazione può autenticare i messaggi in ricezione acquistando confidenza sul mittente del pacchetto;

IPSec Generalità (3/4)

- IPsec realizza gli elementi della riservatezza e della autenticazione di messaggio tramite due protocolli:
  - Authentication Header (AH) protocol
  - Encapsulation Security Payload (ESP) protocol
- Il protocollo AH offre autenticazione di messaggio (autenticità del mittente ed integrità);
- Il protocollo ESP offre riservatezza, autenticazione ed integrità;

IPSec Generalità (4/4)

- Ciascuno dei due protocolli (AH, ESP) può essere adoperato
  - direttamente tra due hosts che parlano IPSec (modo trasporto);
  - tra due gateways (firewall, router) che che parlano IPSec dietro ai quali si trovano hosts connessi in rete locale (modo tunnel);

IPSec Management (1/3)

- Una Security Association (SA) è definita da 3 parametri:
  - Security Parameter Index (SPI);
  - Indirizzo IP di destinazione;
  - Security Protocol Identifier: AH, ESP;
- La SA è unidirezionale: per una trasmissione nelle due direzioni vanno definite due SAs
- Un Security Association Database (SAD) fornisce per ogni SA i corrispondenti parametri di specifica;

IPSec Management (2/3)

- Security Policy Database (SPD) è un database delle politiche di traffico che analizza il traffico IP, lo filtra sulla base di selettori e lo mappa in una o più SAs;
- Il selettore opera sulla base di campi del protocollo IP e campi di protocollo di livello superiore (esempi: indirizzi IP, intervalli di indirizzi IP, numero di porta, ecc.)
- In funzione del valore assunto dal selettore la politica puo' decidere di
  - cancellare il traffico senza autorizzazione
  - bypassare IPSec
  - applicare IPSec con la SA appropriata;

IPSec Management (3/3)

- In concreto il traffico in uscita viene elaborato secondo le regole seguenti:
  - I campi del pacchetto IP definiti dal selettore vanno comparati con la definizione della SPD che punterà su 0 o su una SA;
  - Determinare eventualmente la SA ed il suo SPI;
  - Eseguire il processing necessario (AH, ESP);

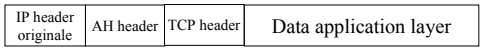
Authentication Header (1/5)

- Questo protocollo permette la verifica della autenticazione di messaggio (integrità & autenticazione) dei dati trasmessi;
- L'autenticazione è basato su di un codice di autenticazione dei messaggi (MAC), che richiede l'uso di una chiave segreta condivisa dai due partners;

Authentication Header (2/5)

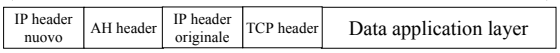
Modalità trasporto

Autenticato esclusi i campi mutabili dell'intestazione IP originale

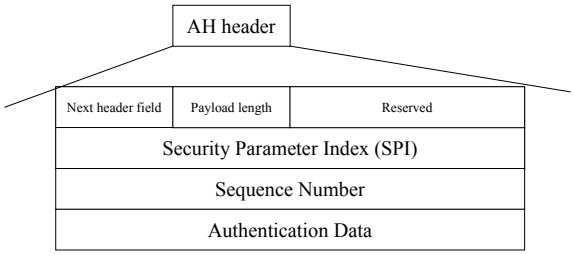


Modalità tunnel

Autenticato esclusi i campi mutabili dell'intestazione IP nuova



Authentication Header (3/5)



Authentication Header (4/5)

- Next header: indica qual è il protocollo veicolato (ESP o TCP, ad esempio);
- Payload length: indica la lunghezza dell'header espressa in parole di 32 bit;
- Riservato: non adoperato;
- Sequence Parameters Index (SPI): identificatore della Security Association;
- Numero progressivo del pacchetto (per un dato SPI);

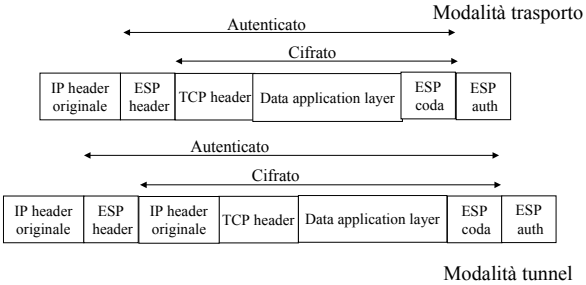
Authentication Header (5/5)

- Authentication data: contiene il MAC (Message Authentication Code) del pacchetto;

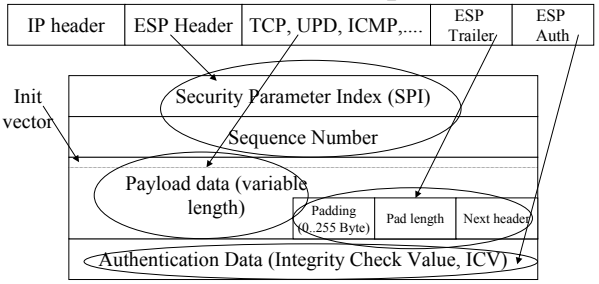
Encapsulating Security Payload (1/7)

- Questo protocollo permette ad IPSec di fornire servizi di confidenzialità dei dati. Puo‘ anche fornire opzionalmente un‘autenticazione dei dati;

Encapsulating Security Payload (2/7)



Encapsulating Security Payload (3/7) – modo trasporto



Encapsulating Security Payload (4/7)

- Security Parameter Index (SPI): identificatore della Security Association;
- Numero progressivo del pacchetto (per un dato SPI);
- Payload: dati trasportati;
- Padding: riempimento;
- Pad length: lunghezza pad;
- Next header: indica qual è il protocollo veicolato TCP, ad esempio);

Encapsulating Security Payload (5/7)

- Authentication data: firma digitale del pacchetto;

Encapsulating Security Payload (6/7)

- Encapsulation Security Payload (ESP) in modo trasporto:
  - L'header ESP viene collocato tra il payload del pacchetto IP e l'intestazione IP;
  - Il campo protocollo del pacchetto IP è posto al valore 50;

Encapsulating Security Payload (7/7)

  - Il pacchetto viene instradato dai router secondo le regole usuali sulla base dell'indirizzo iP di destinazione;
  - L'host finale processa il pacchetto secondo le direttive del protocollo ESP negoziate con l'host partner;
  - Dopo la decodifica il payload viene inoltrato al livello superiore o a ICMP;

Internet Key Exchange

- L'uso dei protocolli AH e ESP deve essere proceduto da due fasi:
  - Nella prima (IKE1) i due partners negoziano una connessione sicura (SA) da adoperarsi per lo scambio degli algoritmi e delle chiavi;
  - Nella seconda (IKE2) i due partners negoziano gli algoritmi e le chiavi da adoperarsi per ciascuna delle SA richieste dalla SPD;