Università di Genova
Facoltà di Ingegneria

Telematica 3

07. Sicurezza nelle reti di telecomunicazioni

Prof. Raffaele Bolla

Il problema della sicurezza

- Sicurezza fisica delle informazioni
  - rappresentava il principale problema prima dell'informatizzazione.
- Sicurezza dei computer
  - protezione automatica dei documenti contenuti all'interno dei computer;
    - » il problema diventa più complesso con l'introduzione delle reti di calcolatori.
- Sicurezza della rete
  - protezione dei dati scambiati tra due nodi terminali.

La sicurezza dei documenti elettronici

- Diversi meccanismi possono essere utilizzati per garantire l'autenticità e l'integrità di documenti cartacei.
- L'utilizzo di documenti elettronici rendono il problema più complesso:
  - un documento cartaceo originale è facilmente distinguibile da una fotocopia;
  - l'alterazione di documenti cartacei può lasciare tracce fisiche (macchie, abrasioni);
  - la validità di un documento cartaceo può essere riconosciuta tramite caratteristiche fisiche (firme, sigilli).

L'architettura di sicurezza OSI

***Security Architecture for OSI*: X.800**

- Autenticazione:
  - autenticazione delle entità *peer*;
  - autenticazione dell'origine dei dati.
- Controllo degli accessi.
- Segretezza dei dati:
  - segretezza della connessione;
  - segretezza non riferita alla connessione;
  - segretezza selettiva a campi;
  - segretezza del traffico.

L'architettura di sicurezza OSI

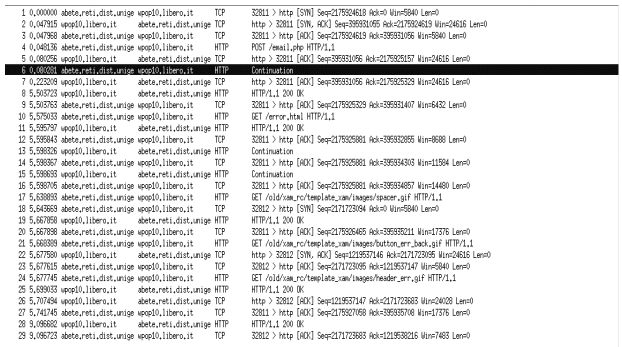
- Integrità dei dati:
  - integrità della connessione con recupero;
  - integrità della connessione senza recupero;
  - integrità della connessione selettiva a campi;
  - integrità non riferita alla connessione;
  - integrità non riferita alla connessione selettiva a campi;
  - non ripudiabilità:
    - » da parte dell'origine;
    - » da parte della destinazione.
- Disponibilità del servizio.

Sicurezza della comunicazione

Attacchi Passivi

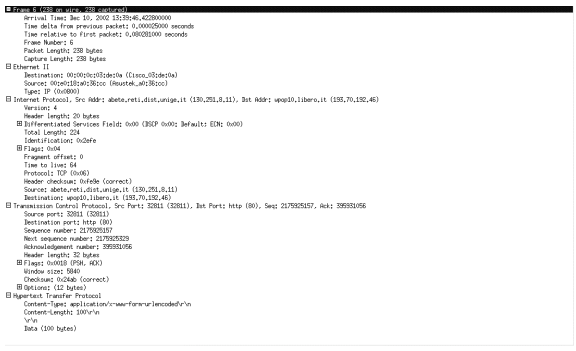
- **Accesso al contenuto**: venire a conoscenza di informazioni riservate.
  Ad esempio lo *Sniffing* (il fiutare) di pacchetti su LAN a mezzo condiviso.
- **Analisi del traffico**: senza analizzare i contenuti specifici, riconoscere l'entità dei comunicanti e tipo e frequenza dei messaggi.
- Sono difficili da rilevare, quindi si devono prevenire.

Sicurezza della comunicazione
Attacchi al contenuto - Esempio di sniffing



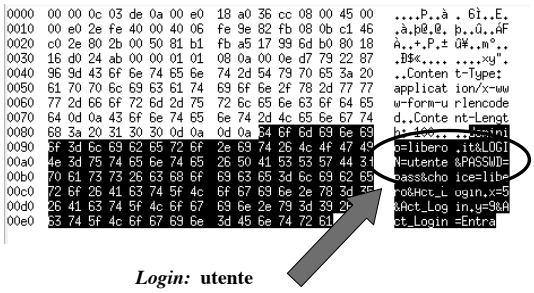
6.7

Sicurezza della comunicazione
Attacchi al contenuto - Esempio di sniffing



6.8

Sicurezza della comunicazione
Attacchi al contenuto - Esempio di sniffing



Login: **utente**

Password: **pass**

6.9

Sicurezza della comunicazione

Attacchi Attivi

- **Sostituzione**: farsi passare per un altro, ad esempio lo *Spoofing* (imbroglio) IP.
- **Replica**: cattura passiva e ritrasmissione successiva di un messaggio per ottenere effetti non autorizzati (ad esempio, un doppio versamento).
- **Alterazione**: modifica, ritardo o riordino dei messaggi.
- **Negazione del servizio**: inibizione dell'uso o della gestione di un sistema (anche dell'intera rete); ad esempio la soppressione di tutti i messaggi verso una destinazione o il sovraccarico di un sistema (singola macchina o intera rete).
- Possono sia essere rilevati e quindi fermati che prevenuti.

6.10

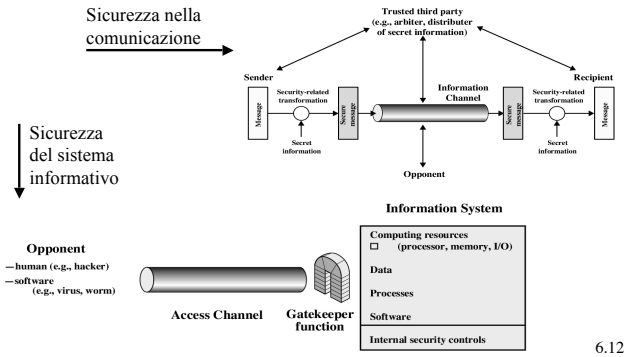
Sicurezza dei sistemi informatici

Attacchi ai sistemi informatici

- Consistono nel tentativo di accesso non autorizzato ad un sistema informativo.
- Si distinguono in genere due tipologie di attacchi:
  - **attacchi dimostrativi, non pericolosi, volti a dimostrare l'abilità dell'hacker;**
  - **attacchi criminali:**
    - » **minacce all'accesso delle informazioni, volte all'intercettazione o alla modifica di dati non propri;**
    - » **minacce ai servizi, per impedire l'utilizzo di determinati servizi agli utenti.**
- **Esempi di attacchi software sono virus e worm; possono essere introdotti nel sistema tramite**
  - **un software su un disco;**
  - **la rete.**

6.11

Modelli di sicurezza delle reti

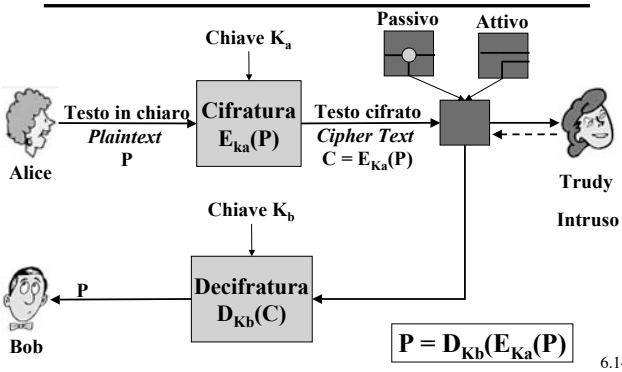


6.12

Parte I

Sicurezza della comunicazione

Riservatezza: Cifratura



Attacchi al testo cifrato

- Attacco al testo cifrato (*chipertext only*): chi attacca ha a disposizione solo la conoscenza di una certa quantità di testo cifrato.
- Attacco al testo in chiaro conosciuto (*known plaintext*): chi attacca conosce alcuni campioni di testo in chiaro e i corrispondenti messaggi cifrati.
- Attacco al testo in chiaro scelto (*chosen plaintext*): chi attacca ha la possibilità di criptare il testo in chiaro desiderato.

Attacchi al contenuto

- Per scardinare un algoritmo di cifratura esistono due tecniche:
  - Criptoanalisi: che si basa sulla natura degli algoritmi, su campioni, su caratteristiche statistiche di P.
  - Forza bruta.

Dim. chiave	# di chiavi possibili	Tempo (1 crifr./μs)	Tempo (10^6cifr./ μs)
32	$2^{32} = 4{,}3x10^9$	35,8 min.	2,15 ms
56	$2^{56} = 7{,}2x10^{16}$	1142 anni	10,01 ore
128	$2^{128} = 3{,}4x10^{38}$	5,4 10^{24} anni	5,4 10^{18} anni
168	$2^{168} = 3{,}7x10^{50}$	5,9 10^{36} anni	5,9 10^{30} anni

Algoritmi di sostituzione

- È una tecnica antica (Giulio Cesare);
- ogni lettera o gruppo di lettere è sostituito da un altra lettera o gruppo di lettere
  - l'algoritmo di Cesare consiste nella sostituzione di ogni lettera con la terza che segue in ordine alfabetico;
  - generalizzando, si può pensare di sostituire ogni lettera con la *k-esima* successiva, k rappresenta in questo caso la chiave dell'algoritmo;
  - un miglioramento consiste nel "mappare" ogni lettera in un'altra (sostituzione monoalfabetica):

testo in chiaro:	a b c d e f g h i j k l m n o p q r s t u v x y w z
testo cifrato:	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

  - in questo caso le possibili chiavi sono $26! \approx 4x10^{26}$ (provando 1 chiave ogni nanosecondo ci vorrebbero 10^{10} anni per provarle tutte).

Altri algoritmi di sostituzione

- Playfair
  - cifratura monoalfabetica di digrammi.
- Hill
  - basata sull'utilizzo di un certo numero di equazioni.
- Polialfabetica
  - utilizzare più cifrature monoalfabetiche;
  - tecnica di Vigenère: ogni singola lettera di una chiave, lunga quanto il testo, determina la cifratura monoalfabetica da utilizzare.

Algoritmi di sostituzione

- Possono essere scardinati con la criptoanalisi:
  - conoscendo una piccola parte di testo cifrato,
  - nota la frequenza statistica delle singole lettere o gruppi di esse,
  - conoscendo alcune parole che probabilmente sono presenti nel testo.
- Le regolarità del linguaggio possono essere nascoste utilizzando algoritmi di compressione del testo originale.

Algoritmi di trasposizione

- Gli algoritmi di sostituzione scambiano i simboli ma ne mantengono l'ordine.
- Gli algoritmi di trasposizione, al contrario, mantengono i simboli ma ne modificano l'ordine.

Chiave →

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Testo in chiaro:
pleasetransferonemilliondollarstomyswis
sbankaccountsixtwotwo
Testo cifrato:
AFLLSKSOSELAWAIATOOSSCTCL
NMOMANTESILYNTWRNNTSOWDP
AEDOBUOERIRICXB

Algoritmi di trasposizione

- Per scardinarli è necessario sapere che si tratta di una trasposizione
  - si può verificare controllando la frequenza delle diverse lettere.
- Si ipotizza il numero di colonne
  - meglio se si conoscono possibili parole presenti;
  - si devono riordinare le colonne;
  - si possono usare informazioni statistiche su blocchi di più lettere.

One-time pad

- Si prenda una sequenza di bit casuale, lunga quanto il testo da cifrare.
- Il testo cifrato viene ricavato dall'operazione di XOR tra la chiave e il testo.
- Questo algoritmo è immune da attacchi:
  - la teoria dell'informazione afferma che non c'è più nessuna informazione nel messaggio cifrato, in quanto tutti i testi in chiaro hanno la stessa probabilità di corrispondere a quel particolare messaggio.
- Ci sono evidenti svantaggi:
  - la chiave non può essere memorizzata;
  - la chiave può essere molto lunga;
  - la lunghezza massima del testo codificato è limitata dalla lunghezza della chiave.

Meccanismi di cifratura

- Si possono classificare i diversi meccanismi di cifratura un due grandi insiemi:
  - Meccanismi a **chiave simmetrica**
    - » $K_A = K_B = \mathbf{K}$, si usa la stessa chiave sia per la cifratura che per la decifratura;
    - » **DEA, T-DEA, RC4**, Blowfish, RC5.
  - Meccanismi a **chiave asimmetrica**
    - » chiave pubblica (cifratura, K_A) e chiave privata (decifratura, K_B);
    - » **RSA** (Rivest, Shamir e Adleman).

Cifratura a chiave simmetrica

- $K_A = K_B = \mathbf{K}$: una sola chiave
- Tradizionalmente si basava su algoritmi semplici (come la sostituzione e la trasposizione).
- Oggi la tendenza è di utilizzare algoritmi talmente complessi la cui conoscenza è inutilizzabile per la decodifica senza la chiave.
- Deve rispettare due requisiti per essere sicura:
  - Robustezza dell'algoritmo: anche conoscendo l'algoritmo ed avendo campioni di testo in chiaro e cifrato, l'intruso non deve essere in grado di decifrare il testo e scoprire la chiave
  - Mittente e destinatario devono poter ottenere in modo sicuro la chiave e custodirla efficacemente.

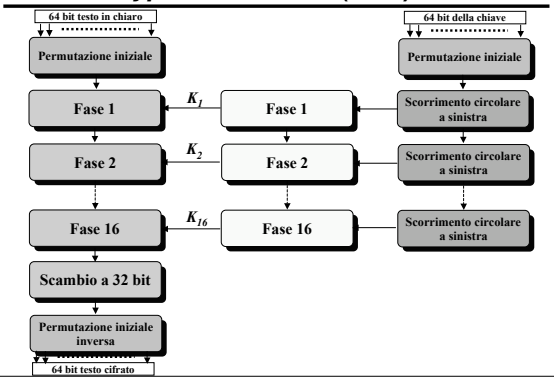
Cifratura a chiave simmetrica

- Si possono distingue due altre categorie:
  - **Cifratura a blocchi**
    - » Viene eseguita su blocchi di dati (e.g., 64 o 128 bit).
    - » Nel sua forma base si tratta in sostanza di un meccanismo a sostituzione.
    - » Meccanismi standard: DES (DEA, T-DEA) e AES.
    - » Differenti modalità di funzionamento (Concatenazione).
  - **Cifratura a flusso**
    - » Combina il flusso di dati da codificare con un *Keystream* per realizzare la cifratura bit a bit.
    - » Rappresenta una realizzazione pratica del meccanismo *One-Time Pad*.
    - » Meccanismi standard: RC4.

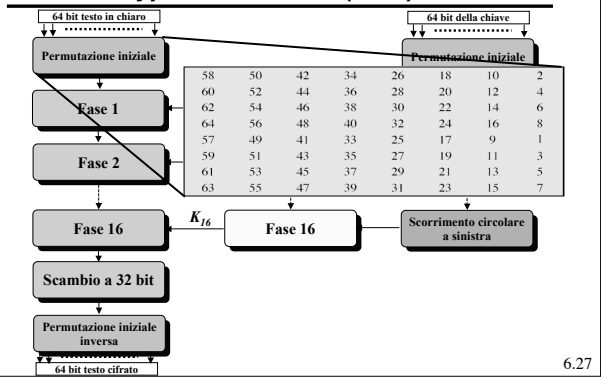
Cifratura a chiave simmetrica
Data Encryption Standard (DES)

- Nasce nel 1977 e viene aggiornato nel 1993,
- E' stato adottato dal U. S. *National Bureau of Standard* (oggi *National Institute for Standard and Technology*, NIST)
- L'algoritmo vero e proprio si chiama *Data Encryption Algorithm* (DEA):
  - opera su blocchi da 64 bit;
  - usa una chiave da 56 bit;
  - si compone di 19 stadi:
    - » una prima permutazione;
    - » 16 stadi parametrizzati da una variante della chiave K_i, i=1,..,16;
    - » uno scambio dei 32 bit destri con i sinistri;
    - » una permutazione inversa alla prima.

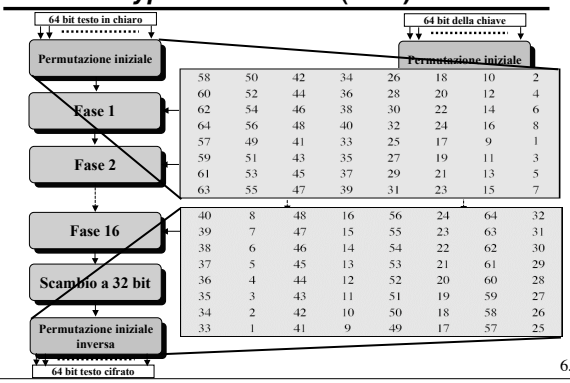
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



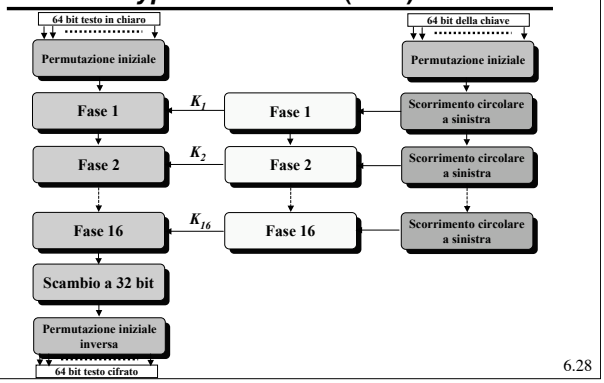
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



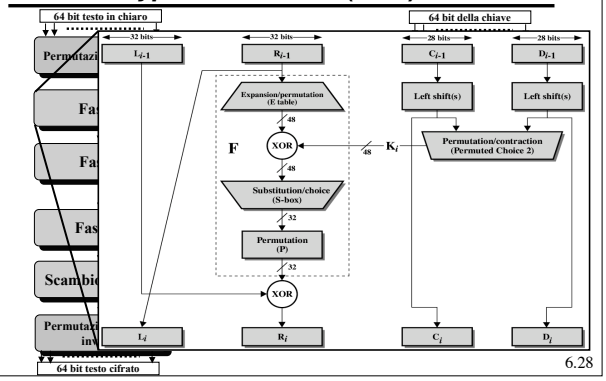
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



Cifratura a chiave simmetrica
Data Encryption Standard (DES)

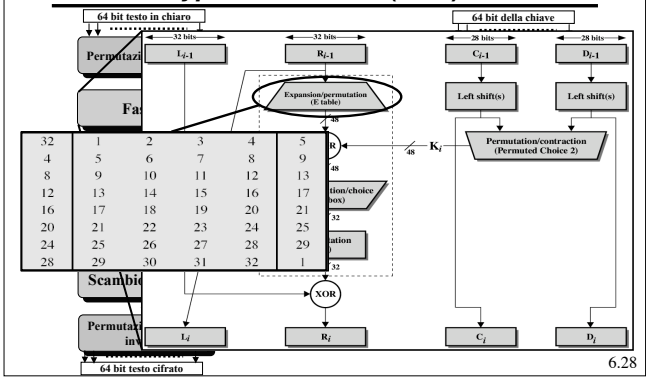


Cifratura a chiave simmetrica
Data Encryption Standard (DES)



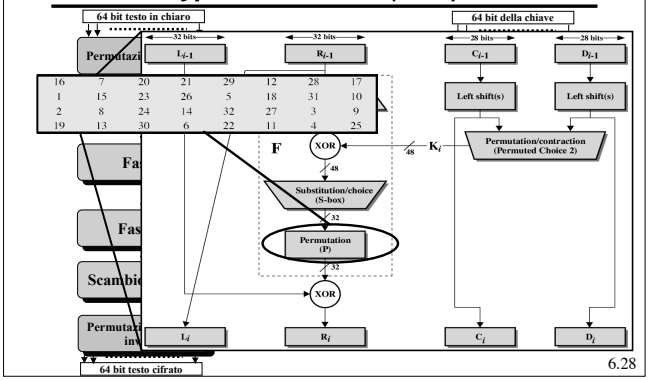
6.28

Cifratura a chiave simmetrica
Data Encryption Standard (DES)



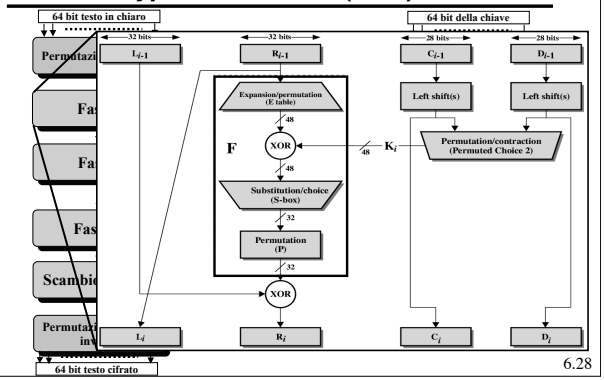
6.28

Cifratura a chiave simmetrica
Data Encryption Standard (DES)



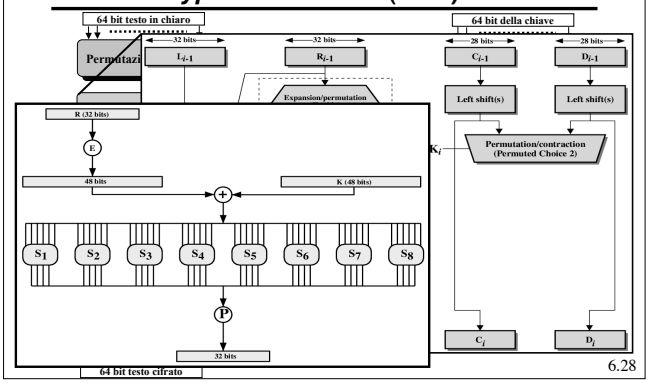
6.28

Cifratura a chiave simmetrica
Data Encryption Standard (DES)



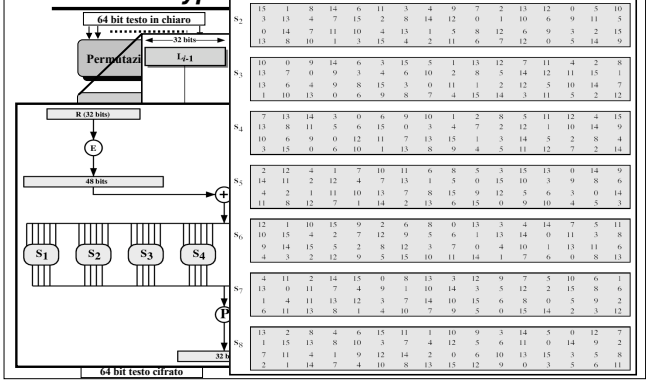
6.28

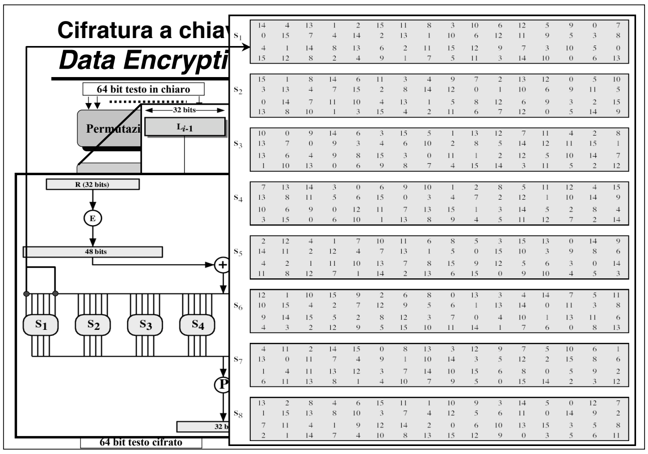
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



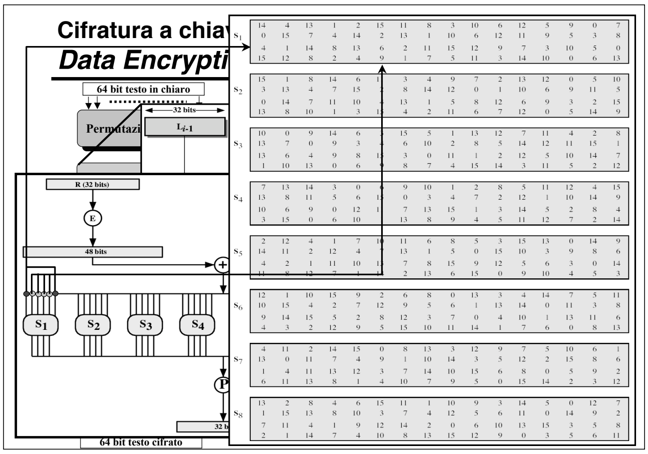
6.28

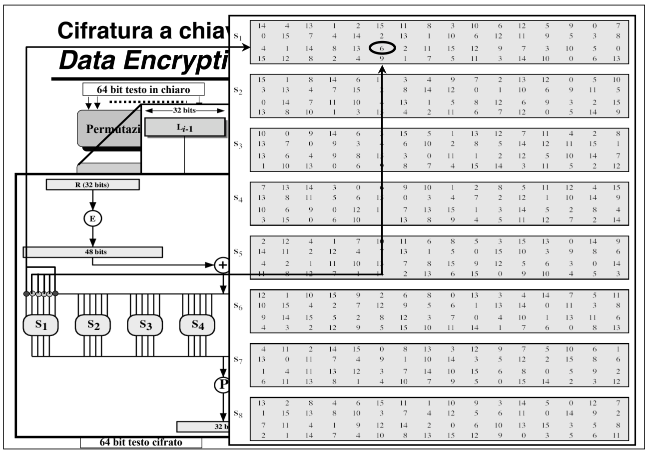
Cifratura a chiave simmetrica
Data Encrypti

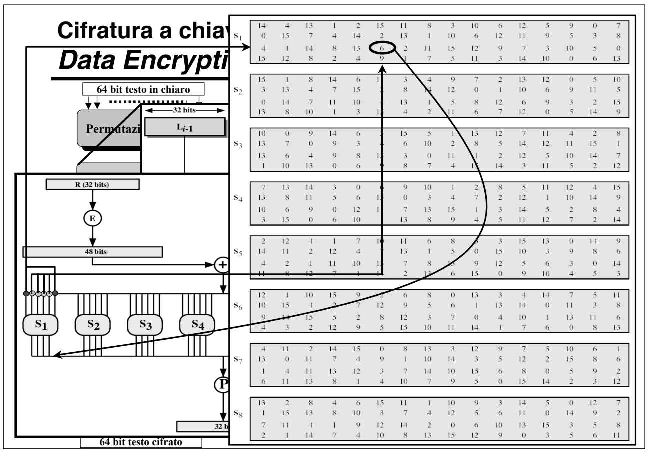


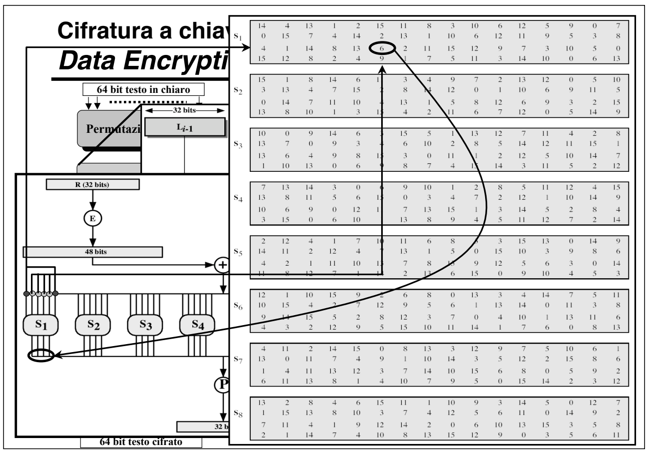


s_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
s_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
s_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
s_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
s_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
s_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
s_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
s_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

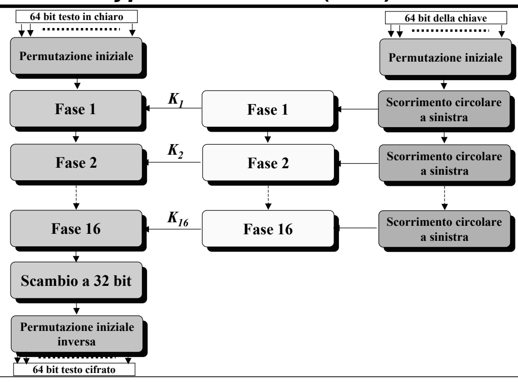




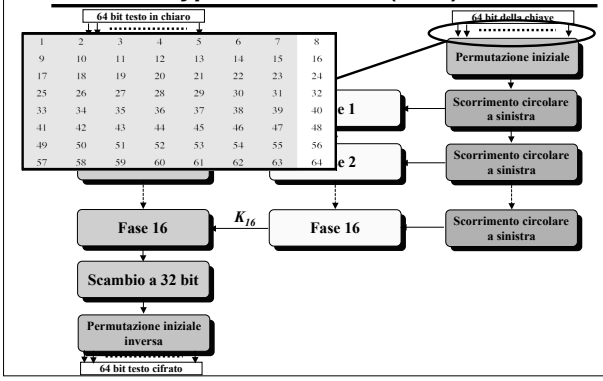




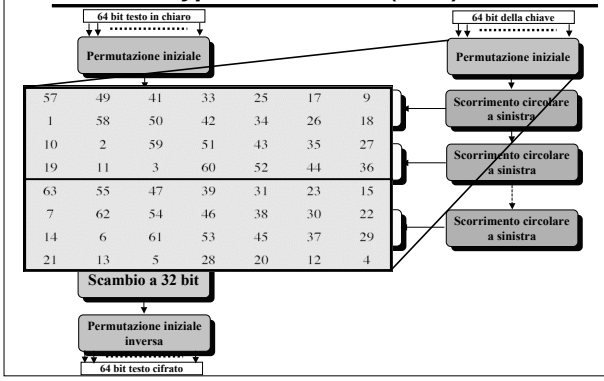
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



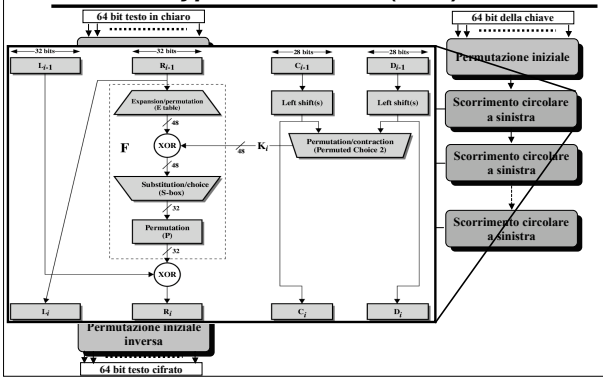
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



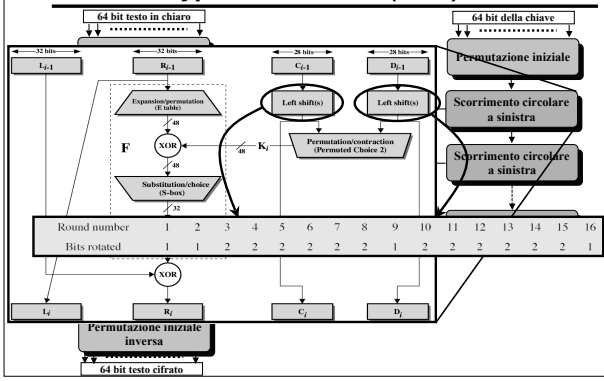
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



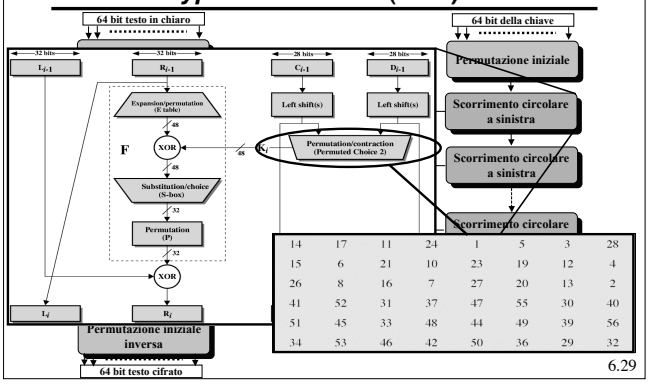
Cifratura a chiave simmetrica
Data Encryption Standard (DES)



Cifratura a chiave simmetrica
Data Encryption Standard (DES)



Cifratura a chiave simmetrica
Data Encryption Standard (DES)



Cifratura a chiave simmetrica
Data Encryption Standard (DES)

- In genere viene usato in unione con un concatenamento (CBC).
- La decifratura avviene con lo stesso meccanismo ma usando le chiavi in ordine inverso.
- La complessità dell'algoritmo risiede nella funzione F(.).

Cifratura a chiave simmetrica
Data Encryption Standard (DES)

- Il DEA utilizza uno schema di Feistel che permette l'uso dello stesso algoritmo in cifratura e decifratura.
- Gli elementi caratterizzanti sono la struttura della funzione f(.) e lo schema di espansione della chiave.
- La funzione f(.) è stata realizzata in modo da rispondere a certi specifici criteri:
  - » SAC (Strict Avanche Criterion) cambiando un bit in ingresso in media ne devono cambiare la metà in uscita.
  - » BIC (Bit Indipendent Criterion) non deve esserci un legame tra la variazione dei bit di ingresso e di quelli in uscita.
  - » Non linearità: deve essere altamente non lineare in modo da non poter essere efficacemente approssimata tramite un sistema lineare che si presta ad una procedura di risoluzione.

Cifratura a chiave simmetrica
Data Encryption Standard (DES)

- Per quanto concerne la robustezza, sono stati indetti tre concorsi (*challenger*) per violarlo:
  - *Challenger* I (1997): Scardinato in 4 mesi;
  - *Challenger* II (1998): Scardinato in 56 ore
  - *Challenger* II (1999) scardinato in 22 ore e 15 min. (testate 245×10^9 chiavi al sec.)
- Ad oggi, (nella sua forma con chiave a 56 bit) non è considerato sicuro.

Cifratura a chiave simmetrica
Triplo-DEA (T-DEA)

- Standardizzato dall'ANSI (1985) come X 9.17 e parte del DES dal 1999
- Usa 3 chiavi da 56 bit: $\mathbf{K_1}$, $\mathbf{K_2}$, $\mathbf{K_3}$.
- Opera come segue:

$$\mathbf{C = E_{K3}(D_{K2}(E_{K1}(P))}$$

- Questo significa che ha una chiave di lunghezza complessiva pari a 168 bit
- Si può cifrare e decifrare il DEA ponendo tutte le chiavi uguali (pensato per avere compatibilità con il DEA originale).
- Si può usare una chiave da 112 bit ponendo $\mathbf{K_1 = K_3}$.

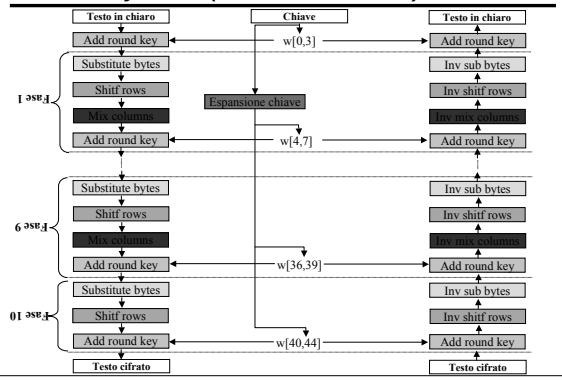
Cifratura a chiave simmetrica
AES

- Il *National Institute of Standards and Technology (NITS)*, ente governativo americano, nel 1997 ha lanciato un concorso pubblico per individuare un nuovo standard di crittografia, per uso generico del governo americano
  - il nome dello standard sarebbe stato AES (*Advanced Encryption Standard*);
  - lo scopo del concorso pubblico era quello di evitare ogni possibile sospetto sul nuovo standard.
- I requisiti richiesti erano:
  - utilizzo di crittografia a chiave simmetrica;
  - progetto completamente pubblico;
  - chiavi di lunghezza 128, 192 e 256 bit;
  - implementazione hw e sw;
  - algoritmo doveva essere liberamente utilizzato o non avere restrizioni particolari.

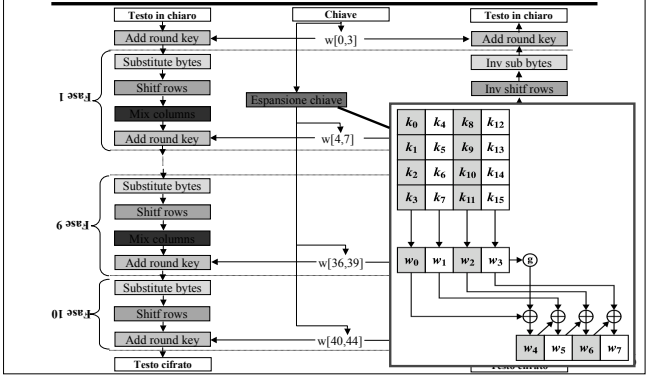
Cifratura a chiave simmetrica
AES - Rijndael

- L'algoritmo prescelto è stato il Rijndael (Rijmen e Daemen)
  - la selezione si è basata su criteri di sicurezza, efficienza, semplicità, flessibilità e requisiti di memoria (per sistemi embedded).
- Supporto chiavi e blocchi di cifratura da 128 a 256 bit, a passi di 32 bit
  - blocchi e chiavi possono avere diversa lunghezza.
- L'utilizzo più frequente prevede chiavi di 128 o 256 bit e blocchi di 128 bit.

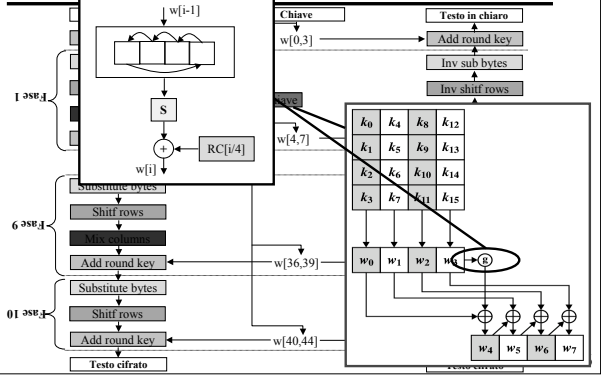
Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



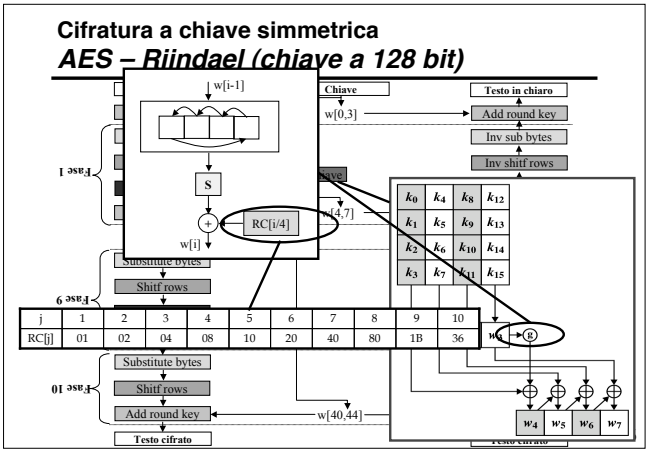
Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



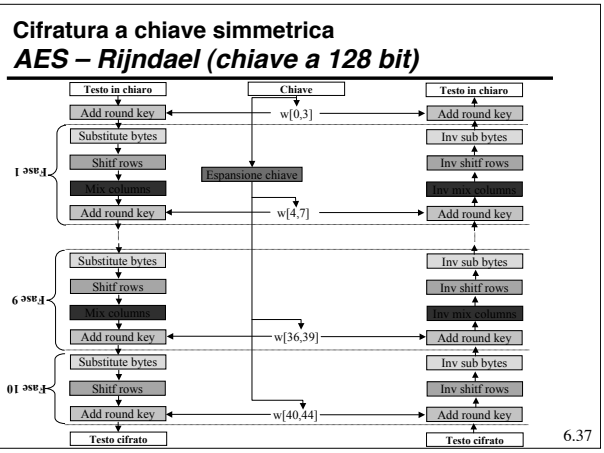
Cifratura a chiave simmetrica
AES – Riindael (chiave a 128 bit)



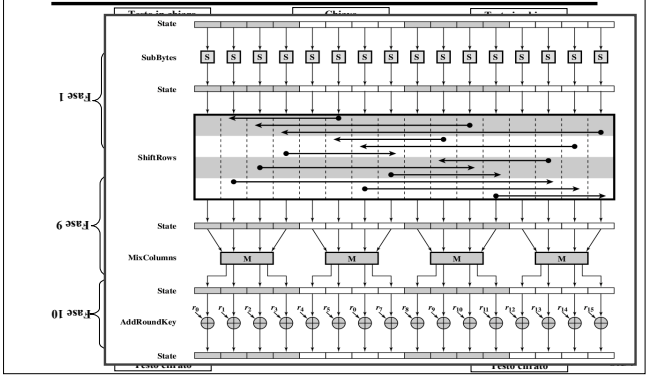
Cifratura a chiave simmetrica
AES – Riindael (chiave a 128 bit)



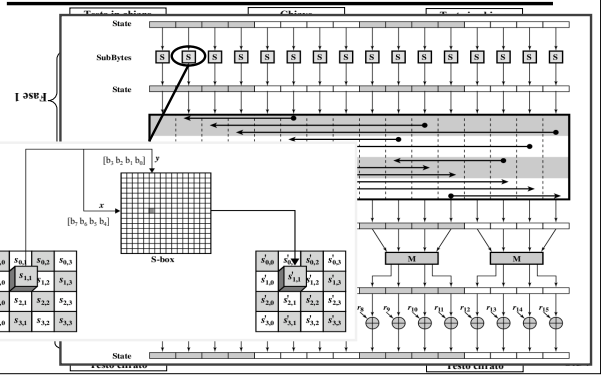
Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



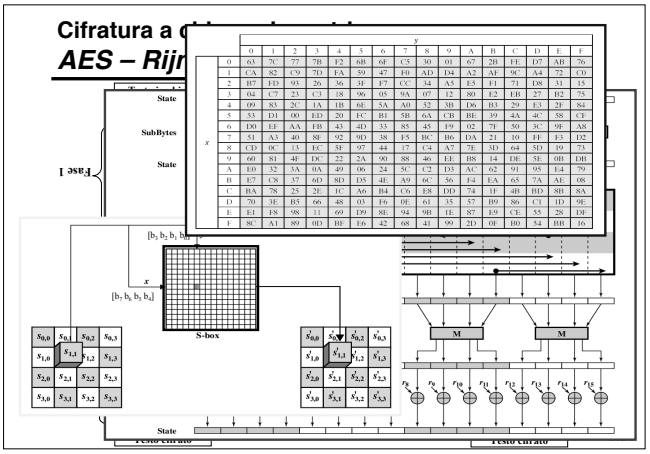
Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



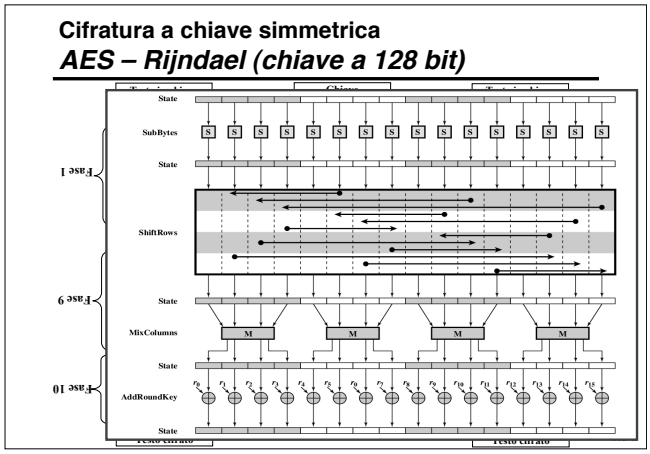
Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



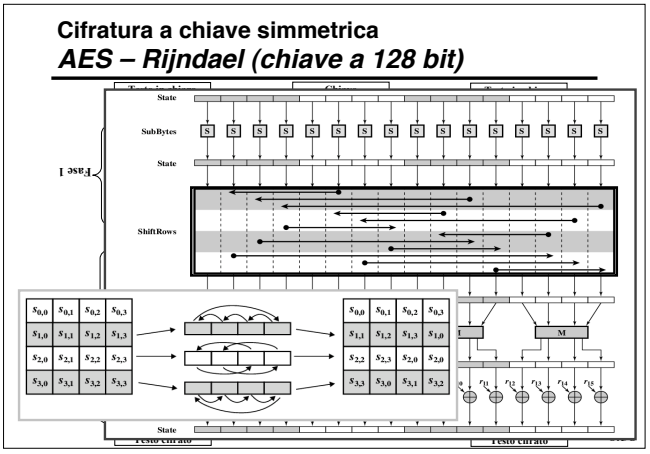
Cifratura a c
AES – Rijn



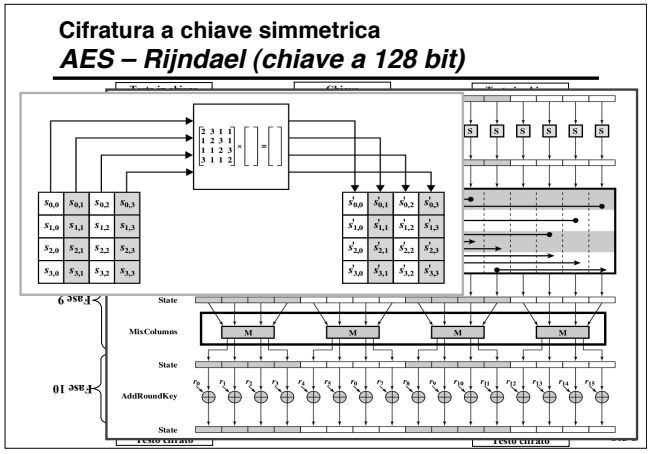
Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



Cifratura a chiave simmetrica
AES – Rijndael (chiave a 128 bit)



Cifratura a chiave simmetrica
Modalità di funzionamento

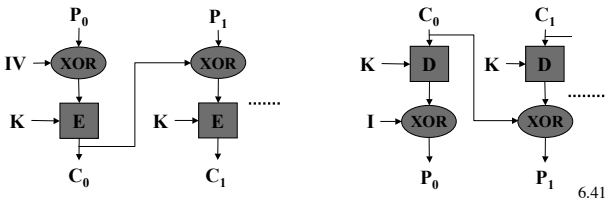
- Nonostante la complessità, il DES e l'AES sono una sostituzione monoalfabetica (ECB, *Electronic Code Block*)
  - lo stesso testo in ingresso genera sempre gli stessi blocchi in uscita;
  - ci sono problemi di sicurezza simili a quelli già visti per gli algoritmi di sostituzione più semplici;
  - funziona bene per piccoli blocchi di dati (es. trasmissione di una chiave di sessione).
- Per i messaggi lunghi l'analisi crittografica può essere in grado di individuare strutture regolari all'interno del messaggio
  - varie metodologie sono presenti per concatenare blocchi successivi tra di loro.

Cifratura a chiave simmetrica
Modalità di funzionamento

- Sono previste cinque modalità di funzionamento:
  - ***Electronic Code Book*** (ECB): cifratura di singoli valori o piccoli blocchi di dati (scambio di chiavi)
  - ***Cipher Block Chaining*** (CBC): trasmissioni di dati orientate ai blocchi.
  - ***Cipher FeedBack*** (CFB): Trasmissione di dati orientata al flusso.
  - ***Output FeedBack*** (OFB): Trasmissione di dati orientata al flusso per canali rumorosi.
  - ***Counter*** (CTR): trasmissioni di dati orientate ai blocchi.

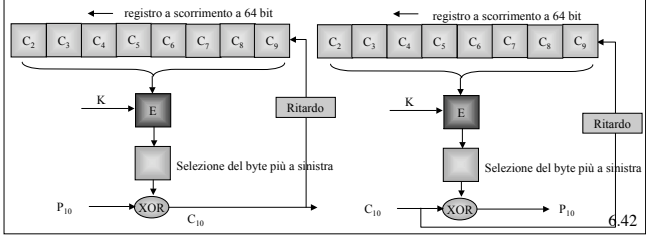
Cipher Block Chaining

- Ogni blocco di testo in chiaro è posto in XOR con il blocco cifrato precedente prima di essere codificato.
- Il primo blocco è posto in XOR con un vettore di inizializzazione IV (*Initial Vector*).



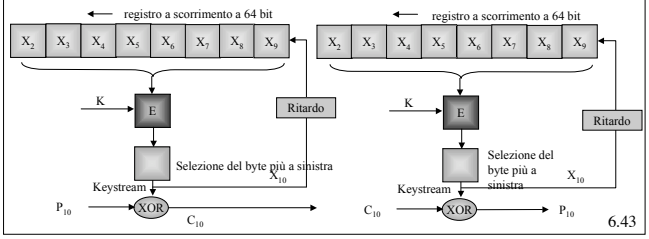
Cipher Feedback (CFB)

- Con questo algoritmo è possibile codificare un byte alla volta
  - in generale si possono codificare *s* bit alla volta.
- Un errore su un byte sulla linea condiziona un intero blocco.



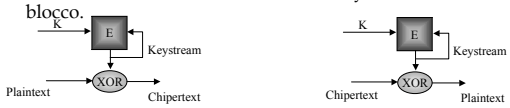
Output Feedback (OFB)

- La struttura è la stessa del CFB.
- L'algoritmo va inizializzato con un *Initial Vector.*



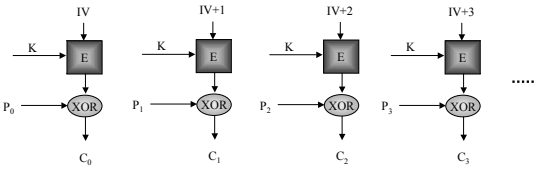
Output Feedback (OFB)

- Il *Keystream* non dipende dal messaggio in chiaro
  - In questo modo si realizza una cifratura a flusso.
  - errori sui singoli byte non si propagano a tutto il blocco (1 bit modificato nella stringa cifrata genere 1 solo bit di errore nel messaggio originale).
- Soggetto al *keystream reuse attack* se non si cambia K o IV:
  - XOR di 2 chipertext genera l'XOR dei due *plain text;*
  - è possibile ricavare il testo originale con una analisi statistica.
- Esiste una variante più efficiente detta ***Stream Cipher*** in cui la retroazione non avviene su un solo byte ma sull'intero blocco.



Counter (CTR)

- Utilizzato per poter decifrare singoli blocchi di un *ciphertext* senza dover decifrare tutti i blocchi precedenti.
- Se non si cambiano K e IV ad ogni codifica presenta le stesse debolezze dell'algoritmo precedente.



Cifratura a flussi

- Una cifratura a flussi è in grado di eseguire la crittografia del testo in chiaro un bit alla volta
  - tipicamente opera su almeno un byte alla volta.
- Il meccanismo consiste nel
  - generare una sequenza (*keystream*) pseudocasuale a partire da una chiave;
  - eseguire un OR esclusivo (XOR) tra il *keystream* ed il testo in chiaro.
- La cifratura a flussi è simile alla tecnica *One-Time Pad*
  - la tecnica one-time pad usa sequenze veramente casuali.

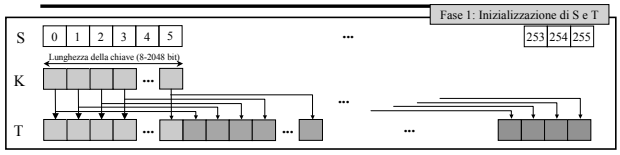
Cifratura a flussi

- Proprietà di un codificatore a flussi
  - il *keystream* deve avere un periodo molto elevato
    - » rende difficile l'analisi crittografica;
  - il *keystream* deve approssimare le proprietà di un numero casuale
    - » rende minima l'informazione contenuta nel testo cifrato;
  - la chiave deve essere sufficientemente lunga
    - » impedisce gli attacchi a forza bruta;
    - » almeno 128 bit.
- La cifratura a flussi può essere sicura quanto la cifratura a blocchi
  - il generatore pseudocasuale deve essere progettato in modo accurato;
  - è in genere più veloce e semplice
  - non permette di riutilizzare la stessa chiave
    - » lo XOR di due testi crittografati elimina la cifratura;
  - rappresenta la soluzione preferita per flussi di dati
    - » canali di comunicazioni sicuri (SSL, browser-Web).

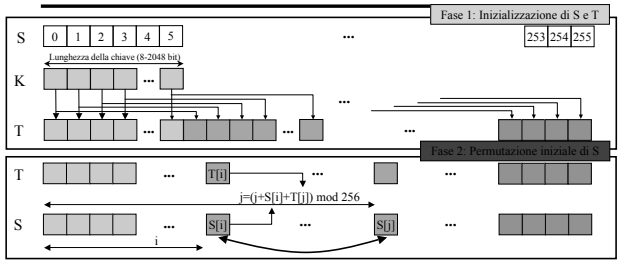
Cifratura a flussi – RC4

- Progettato nel 1987 da Ron Rivest per RSA Security.
- Chiave di dimensione variabile e operazioni orientate al byte.
- Il periodo della cifratura è enorme (>10^{100}).
- RC4 è attualmente la cifratura di flussi più diffusa
  - è molto veloce anche nelle implementazioni software;
  - è utilizzata dagli standard TLS/SSL e nel protocollo WEP.
- L'algoritmo RC4 è stato inizialmente tenuto segreto da RSA Security
  - nel 1994 la comunità degli hacker lo ha diffuso in rete.

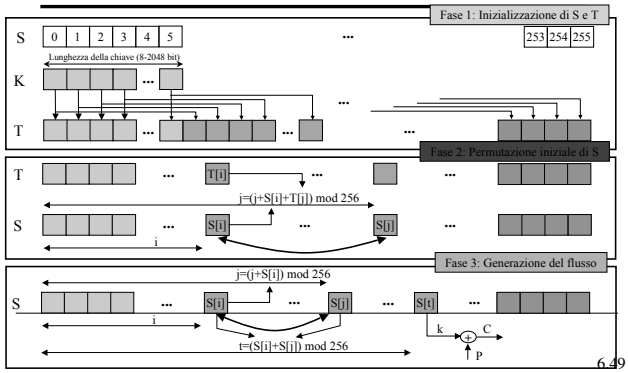
L'algoritmo RC4



L'algoritmo RC4



L'algoritmo RC4



Resistenza di RC4

- Diversi lavori su metodi di attacco all'algoritmo RC4 sono stati pubblicati
  - nessun approccio è realistico utilizzando una chiave di almeno 128 bit.
- Il protocollo WEP tuttavia è altamente insicuro
  - la vulnerabilità deriva dal modo in cui vengono generate le chiavi dell'algoritmo e non dall'algoritmo stesso;
  - il problema sembra non estendersi ad altre applicazioni basate su RC4.

Cifratura a chiave simmetrica

- Collocazione dei dispositivi di cifratura, due possibilità:
  - Sulle linee (il pacchetto rimane vulnerabile nei commutatori)
  - Sui dispositivi terminali (non è possibile cifrare anche le intestazioni ma solo i dati)
- L'ottimo e utilizzare ambedue i metodi.

Cifratura a chiave pubblica

- Utilizza due chiavi:
  - Una chiave $\mathbf{K_A}$ usata per la cifratura che viene resa pubblica (chiave pubblica).
  - Una chiave $\mathbf{K_B}$ usata per la decifratura che viene mantenuta segreta (chiave privata).
- Si evita (ma solo parzialmente!) il problema della distribuzione della chiave.
- Deve avere tre requisiti
  - $\mathbf{D_{KB}(E_{KA}(P)) = P}$
  - Non deve essere possibile dedurre $\mathbf{K_B}$ da $\mathbf{K_A}$.
  - K_B non deve poter essere dedotta tramite cifratura di testi noti

Cifratura a chiave pubblica
Rivest, Shamir, Adleman (RSA)

Scelta delle chiavi

- Si scelga due numeri primi grandi (ad esempio da 1024 bit): **p** e **q**.
- Si calcoli **n = p · q**, **z = (p -1)(q -1)**.
- Si scelga **e** (con **e < n**) tale che non abbia fattori comuni con **z** (**e** e **z** sono "primi relativi") **.**
- Si scelga **d** tale che **ed-1** sia esattamente divisibile per z (in altre parole **e · d mod z = 1.**
- La chiave pubblica $\mathbf{K_A = (n, e)}$ e la chiave privata $\mathbf{K_B = (n, d).}$

Cifratura a chiave pubblica
Rivest, Shamir, Adleman (RSA)

- Dati (**n**, **e**) e (**n**, **d**):
  - Per cifrare una sequenza di bit **m**, si calcola:
    $\mathbf{c = m^e \bmod n}$ (ossia il resto di $\mathbf{m^e}$ diviso **n**)
  - Per decifrare una sequenza di bit **c** ricevuta, si calcola:
    $\mathbf{m = c^d \bmod n}$ (ossia il resto di $\mathbf{c^d}$ diviso **n**)
- Ciò che accade è che

$$\mathbf{m = (m^e \bmod n)^d \bmod n}$$

Cifratura a chiave pubblica
Rivest, Shamir, Adleman (RSA)

Bob sceglie **p** = 5, **q** = 7.
Quindi **n** = 35, **z** = 24.
e = 5 (così **e**, **z** sono primi relativi).
d = 29 (così **ed-1** è divisibile esattamente per **z**).

	Lettera	m	m^e	$c = m^e \bmod n$
Cifra:	l	12	248832	17

	c	c^d	$m = c^d \bmod n$	Lettera
Decifra:	17	48196857210675091509141182522307200	12	l

Cifratura a chiave pubblica
Rivest, Shamir, Adleman (RSA)

- Perché vale $\mathbf{m = (m^e \bmod n)^d \bmod n}$ **?**
- La base è un risultato della teoria dei numeri, ossia se p e q sono primi e n = p q allora:

$$\mathbf{x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n}$$

- $\mathbf{(m^e \bmod n)^d \bmod n} = \mathbf{m^{ed} \bmod n} =$
  $= \mathbf{m^{ed \bmod (p-1)(q-1)} \bmod n} =$
  (grazie al risultato della teoria dei numeri di cui sopra)
  $= \mathbf{m^1 \bmod n} =$
  (dato che si è scelto **ed** divisibile per **(p-1)(q-1)** con resto 1)
  $= \mathbf{m}$

Cifratura a chiave pubblica
Rivest, Shamir, Adleman (RSA)

- Si osservi che l'algoritmo funziona anche a chiavi invertite.
- Il meccanismo è sicuro perché, al momento, non sono noti algoritmi veloci per la fattorizzazione dei numeri (altrimenti basterebbe fattorizzare n)
- Il problema della cifratura a chiave pubblica è il tempo di elaborazione, rispetto alla chiave simmetrica:
  - In software è 100 volte più lenta
  - In hardware è da 1000 a 10.000 volte più lenta
- Allora viene usato, in genere, solo per lo scambio di una chiave simmetrica di sessione.

Integrità e firma elettronica

- La firma elettronica è la forma più completa di verifica di integrità. Tale tipo di firma dovrebbe far sì che:
  - L'integrità del messaggio originale sia assicurata.
  - La firma sia legata indissolubilmente al messaggio.
  - La firma sia verificabile (permette di identificare chi ha firmato).
  - La firma sia non falsificabile e non rifiutabile (solo quell'individuo deve poter fare quella firma e non deve poterla disconoscere).

Firma elettronica

- Un modo per firmare il proprio documento è quello di codificarlo con la propria chiave privata.
- Dato che solo il proprietario ha la chiave privata, questo assicura che solo lui può averlo codificato, e chiunque può verificare che è stato lui a codificarlo usando la sua chiave pubblica e ritrovando il messaggio.
- Questo procedimento ha un limite:
  - La cifratura di un messaggio (con chiave pubblica) è una operazione onerosa se fatta su grandi quantità di dati. È lo stesso vale per la decifratura, obbligatoria per poter leggere il messaggio

Firma elettronica

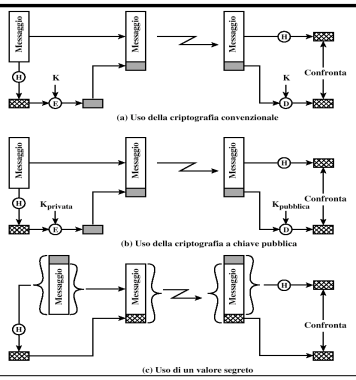
- Un meccanismo alternativo che impone un minor onere computazionale è quello del ***message digest*** (sunto del messaggio).
- Il principio è simile a quello dei codici a rivelazione d'errore, si applica ad un messaggio p una funzione H( ) il cui risultato è un blocco di dati d_p (il ***digest***) con dimensioni molto minori di p. Tale *digest* deve essere legato in modo univoco la messaggio originale
- Tale funzione H() viene chiamata funzione di **hash** .

Integrità e Firma elettronica
Digest

- La funzione di ***hash*** H() deve avere le seguenti proprietà:
  - Deve poter essere applicata a messaggi di qualunque dimensione.
  - Deve produrre un risultato di lunghezza fissa.
  - Deve essere relativamente semplice e veloce da calcolare.
  - Per ogni *digest* d dato, deve essere computazionalmente impossibile trovare x tale che H(x) = d (non invertibilità).
  - Per ogni messaggio x deve essere computazionalmente impossibile trovare y ≠ x tale che H(y) = H(x) (impedisce falsificazioni).
  - Deve essere computazionalmente impossibile trovare una qualsiasi coppia (x, y) tale H(x) = H(y).

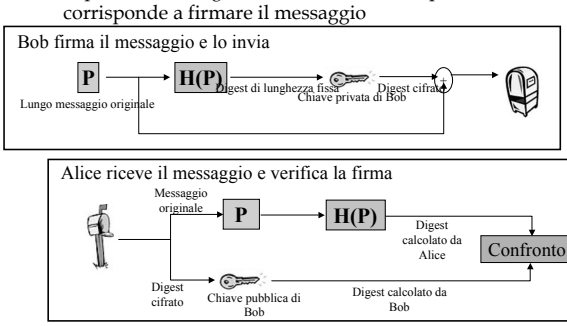
Integrità e Firma elettronica
Digest

Possibili usi del *digest* per la verifica dell'integrità



Integrità e Firma elettronica
Digest

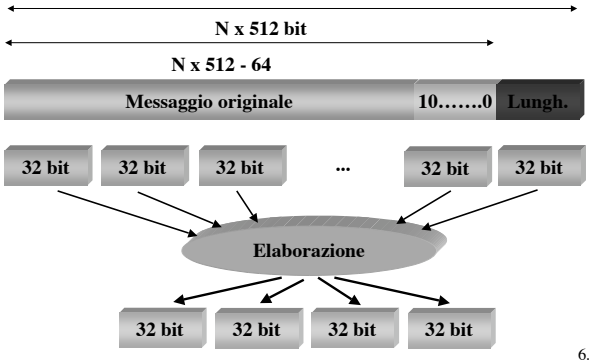
- Si può usare il *digest* cifrato con la chiave privata; corrisponde a firmare il messaggio



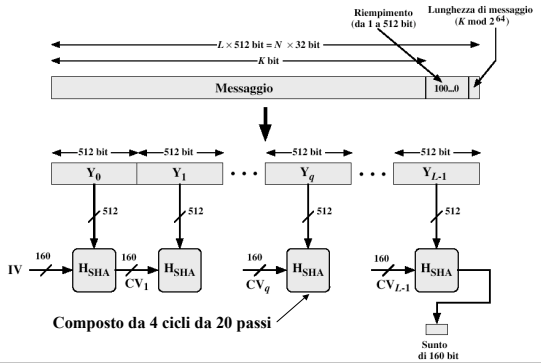
Integrità e Firma elettronica
Digest

- Gli standard più usati per il *digest* attualmente sono sostanzialmente due:
  - ***Secure Hash Algorithm*** (**SHA**): sviluppato dal NIST e rivisto successivamente e standardizzato come FIPS PUB 180-1 noto come **SHA-1**, e usa *digest* da 160 bit.
  - MD5 definito da Ron Rivest [RFC 1321] che usa un *digest* di 128 bit.

Integrità e Firma elettronica
Digest - MD5



Integrità e Firma elettronica
Digest - SHA-1



Integrità e Firma elettronica
Digest – The Birthday Attack

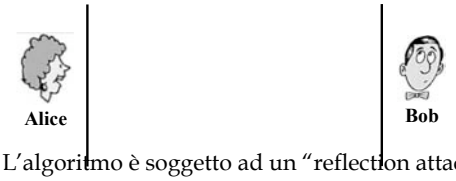
- *Quanti studenti sono necessari in una classe affinché la probabilità che almeno due di essi siano nati lo stesso giorno sia superiore a 1/2?*
  - Dalla teoria della probabilità la risposta è 23.
- In generale, se esiste una qualche relazione tra *n* ingressi (studenti, messaggi, ecc.) e *k* uscite (compleanni, digest):
  - ci sono $n(n-1)/2$ coppie di ingressi possibili;
  - se $n(n-1)/2 > k$, la probabilità di avere due ingressi che diano luogo alla stessa uscita è abbastanza elevata;
  - in pratica tale probabilità e significativa per
- Se *m* è la lunghezza del digest, tra $2^{m/2}$ diversi messaggi è abbastanza probabile trovarne due che diano luogo allo stesso digest
  - più il digest è lungo più è difficile trovare tale coppia di messaggi.

Autenticazione

- Obiettivo: Bob vuole che Alice provi la sua identità
- Una prima serie di *Autentication Protocol* (AP) semplici potrebbero essere:
  - **AP1:** Alice invia un pacchetto dicendo "Sono Alice".
  - **AP2:** Alice invia un pacchetto dicendo "Sono Alice" ed allega il suo indirizzo IP.
  - **AP3:** Alice invia un pacchetto dicendo "Sono Alice" ed allega una password.
  - **AP3.1:** Alice invia un pacchetto dicendo "Sono Alice" ed allega una password cifrata.

Autenticazione

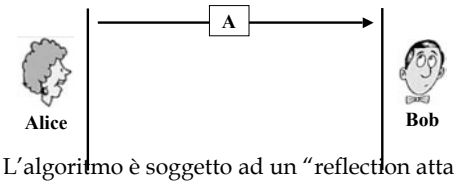
- **AP4** Per evitare un "*playback attack*", si usa un *nonce* (*only once*) R, ossia un numero usato una volta sola generato a caso da Bob).



- L'algoritmo è soggetto ad un "reflection attack".

Autenticazione

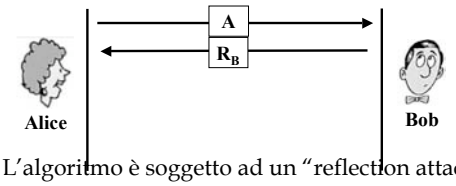
- **AP4** Per evitare un "*playback attack*", si usa un *nonce* (*only once*) R, ossia un numero usato una volta sola generato a caso da Bob).



- L'algoritmo è soggetto ad un "reflection attack".

Autenticazione

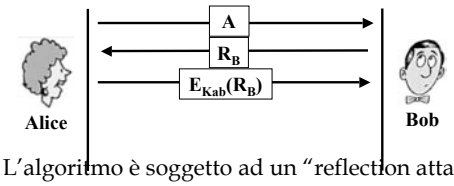
- **AP4** Per evitare un "*playback attack*", si usa un *nonce* (*only once*) R, ossia un numero usato una volta sola generato a caso da Bob).



- L'algoritmo è soggetto ad un "reflection attack".

Autenticazione

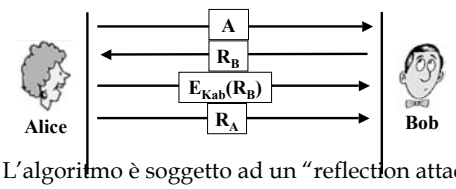
- **AP4** Per evitare un "*playback attack*", si usa un *nonce* (*only once*) R, ossia un numero usato una volta sola generato a caso da Bob).



- L'algoritmo è soggetto ad un "reflection attack".

Autenticazione

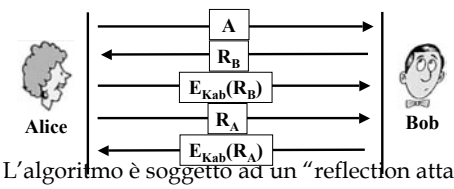
- **AP4** Per evitare un "*playback attack*", si usa un *nonce* (*only once*) R, ossia un numero usato una volta sola generato a caso da Bob).



- L'algoritmo è soggetto ad un "reflection attack".

Autenticazione

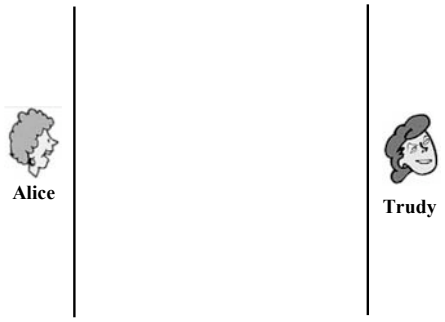
- **AP4** Per evitare un "*playback attack*", si usa un *nonce* (*only once*) R, ossia un numero usato una volta sola generato a caso da Bob).



- L'algoritmo è soggetto ad un "reflection attack".

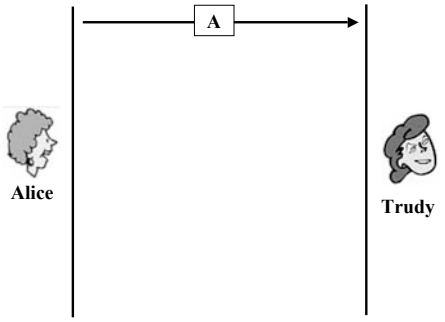
Autenticazione

Reflection Attack



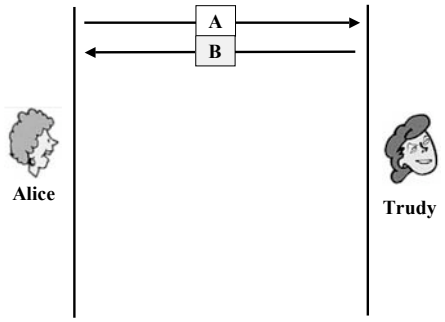
Autenticazione

Reflection Attack



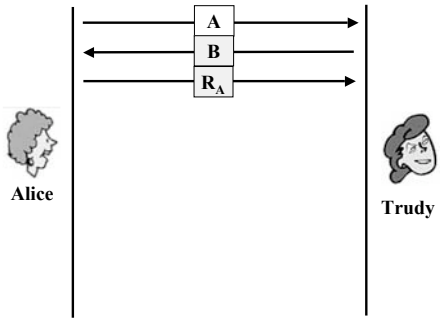
Autenticazione

Reflection Attack



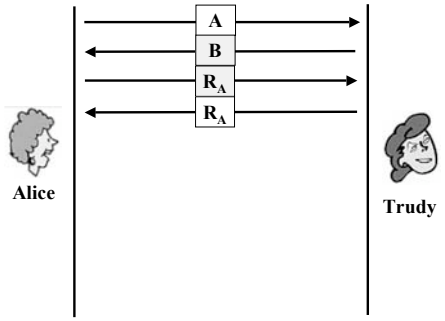
Autenticazione

Reflection Attack



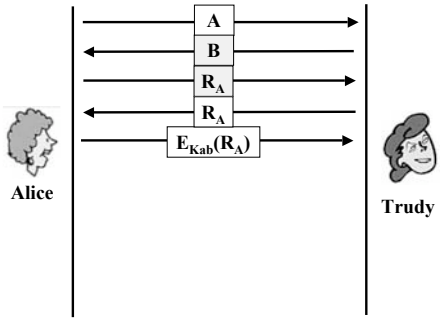
Autenticazione

Reflection Attack



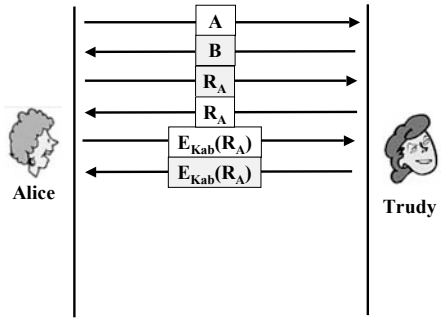
Autenticazione

Reflection Attack



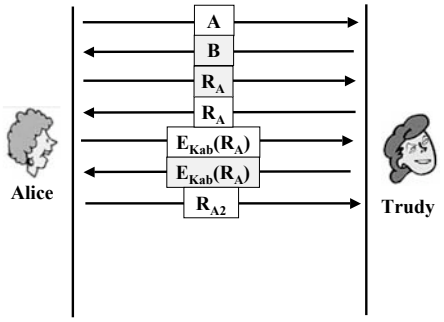
Autenticazione

Reflection Attack



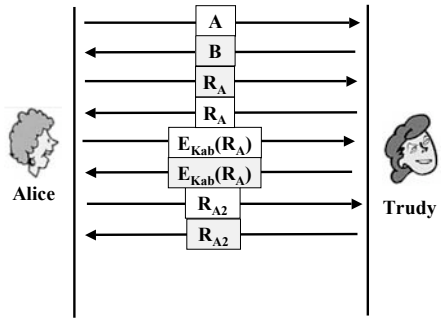
Autenticazione

Reflection Attack



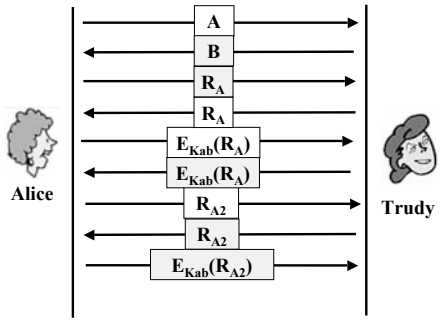
Autenticazione

Reflection Attack



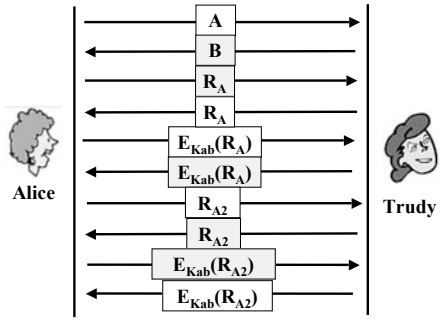
Autenticazione

Reflection Attack



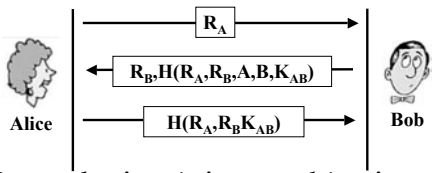
Autenticazione

Reflection Attack



Autenticazione

- **AP5 Uso di una funzione di hash H(.).**



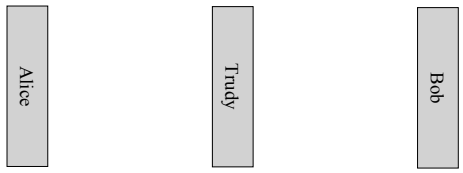
- **Questo algoritmo è sicuro perché un intruso non può ottenere da nessuna delle due parti il digest di un messaggio desiderato**
  - **Entrambi i digest contengono valori scelti dal mittente, che l'intruso non può controllare.**

Autenticazione

- Come si scambiano la chiave segreta?
- Una elegante soluzione consiste nell'algoritmo di Diffie-Hellman:
  - Alice genera due numeri primi molto grandi, *n* e *g* (in modo che rispettino determinate proprietà) e un qualunque numero *x*.
  - Alice trasmette a Bob (n, g, g^x mod n).
  - Bob genera un numero casuale *y*.
  - Bob invia ad Alice (g^y mod n) e calcola [(g^x mod n)^y mod n].
  - Alice calcola [(g^y mod n)^x mod n].
  - Per l'aritmetica dei moduli le due quantità sono uguali e pari a (g^{xy} mod n); questo valore rappresenta la chiave di sessione.

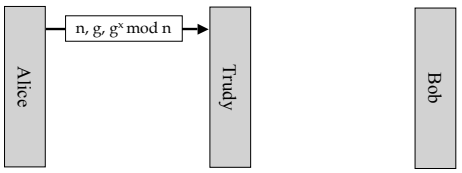
Autenticazione

- L'algoritmo di Diffie-Helman è soggetto all'attacco *man-in-the-middle*.



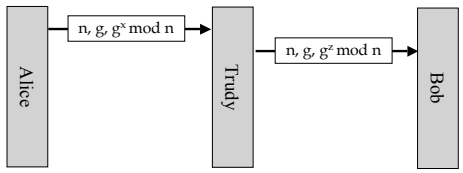
Autenticazione

- L'algoritmo di Diffie-Helman è soggetto all'attacco *man-in-the-middle*.



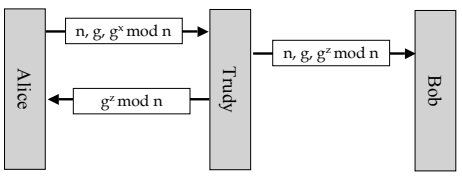
Autenticazione

- L'algoritmo di Diffie-Helman è soggetto all'attacco *man-in-the-middle*.



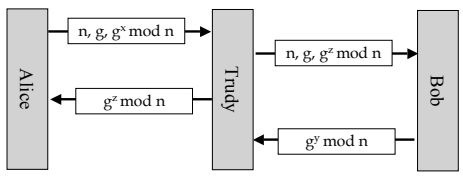
Autenticazione

- L'algoritmo di Diffie-Helman è soggetto all'attacco *man-in-the-middle*.



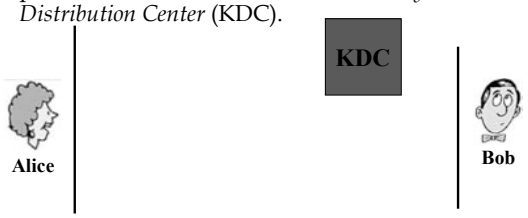
Autenticazione

- L'algoritmo di Diffie-Helman è soggetto all'attacco *man-in-the-middle*.



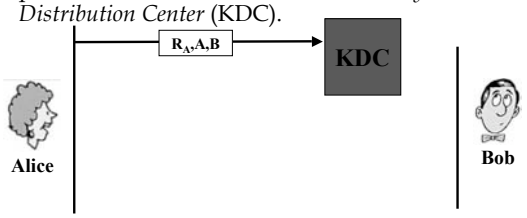
Autenticazione

- Mantenere chiavi segrete differenti per tutti i sistemi con cui si ci vuole autenticare può non essere realistico.
- **AP6** Un meccanismo per ovviare a questo problema consiste nell'utilizzare un *Key Distribution Center* (KDC).



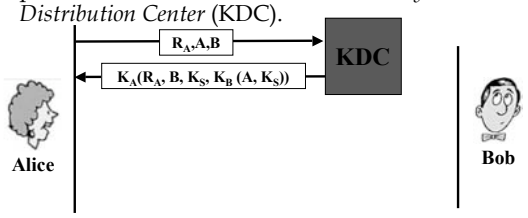
Autenticazione

- Mantenere chiavi segrete differenti per tutti i sistemi con cui si ci vuole autenticare può non essere realistico.
- **AP6** Un meccanismo per ovviare a questo problema consiste nell'utilizzare un *Key Distribution Center* (KDC).



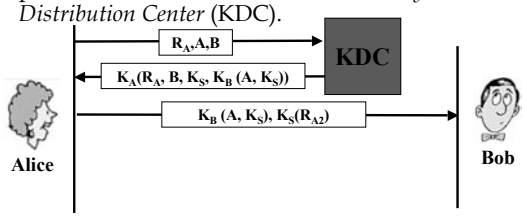
Autenticazione

- Mantenere chiavi segrete differenti per tutti i sistemi con cui si ci vuole autenticare può non essere realistico.
- **AP6** Un meccanismo per ovviare a questo problema consiste nell'utilizzare un *Key Distribution Center* (KDC).



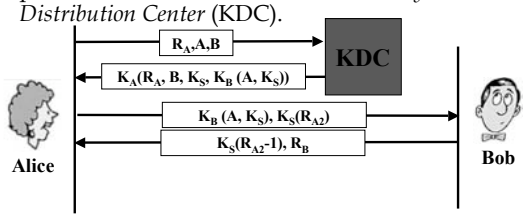
Autenticazione

- Mantenere chiavi segrete differenti per tutti i sistemi con cui si ci vuole autenticare può non essere realistico.
- **AP6** Un meccanismo per ovviare a questo problema consiste nell'utilizzare un *Key Distribution Center* (KDC).



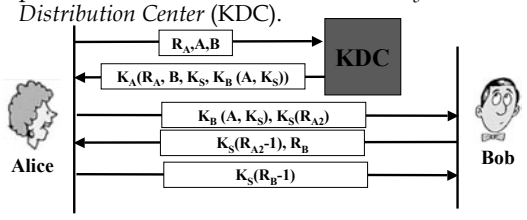
Autenticazione

- Mantenere chiavi segrete differenti per tutti i sistemi con cui si ci vuole autenticare può non essere realistico.
- **AP6** Un meccanismo per ovviare a questo problema consiste nell'utilizzare un *Key Distribution Center* (KDC).



Autenticazione

- Mantenere chiavi segrete differenti per tutti i sistemi con cui si ci vuole autenticare può non essere realistico.
- **AP6** Un meccanismo per ovviare a questo problema consiste nell'utilizzare un *Key Distribution Center* (KDC).



Autenticazione

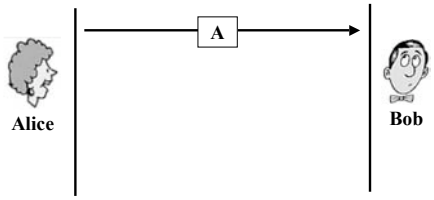
- L'algoritmo di autenticazione visto è il Needham-Schroeder.
- Sebbene sembri sicuro, in realtà presenta una falla, nel caso l'intruso sia venuto in possesso di una vecchia chiave di sessione K_s. Needham e Schroeder ne hanno proposto una variante che risolve il problema.
- Questa forma di autenticazione è utilizzata dal *Kerberos* (Windows 2000):
  - prevede la presenza di un client (utente), un server di autenticazione (AS), un server emettitore di *ticket* (TGS, *Ticket Grant Server*) e i server che forniscono i servizi;
  - l'AS autentica gli utenti tramite la password e fornisce una chiave per autenticarsi presso il TGS;
  - il TGS fornisce una chiave di sessione e permette di autenticare l'utente presso i diversi server presenti;
  - le repliche dei messaggi sono evitate utilizzando un timestamp nei messaggi scambiati.

Autenticazione

- **AP7**: utilizzo della chiave pubblica:

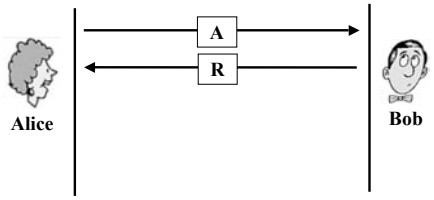
Autenticazione

- **AP7**: utilizzo della chiave pubblica:



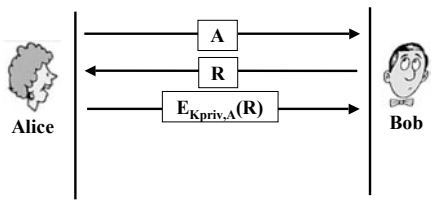
Autenticazione

- **AP7**: utilizzo della chiave pubblica:



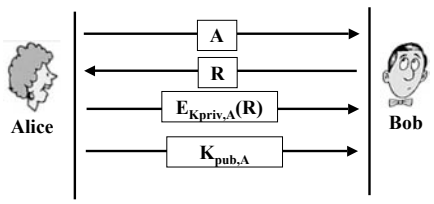
Autenticazione

- **AP7**: utilizzo della chiave pubblica:



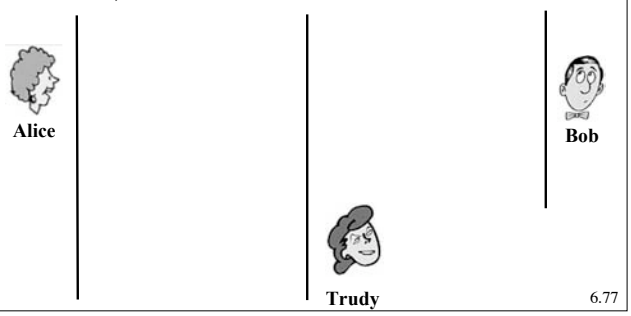
Autenticazione

- **AP7**: utilizzo della chiave pubblica:



Autenticazione

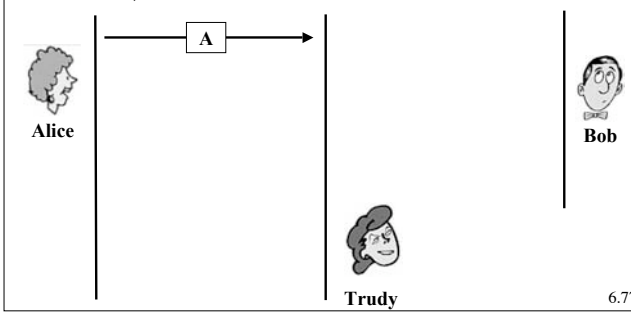
- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



6.77

Autenticazione

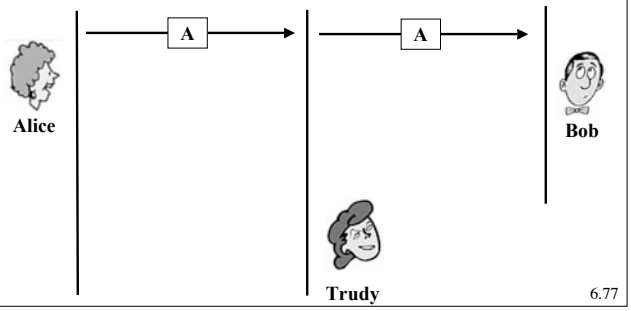
- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



6.77

Autenticazione

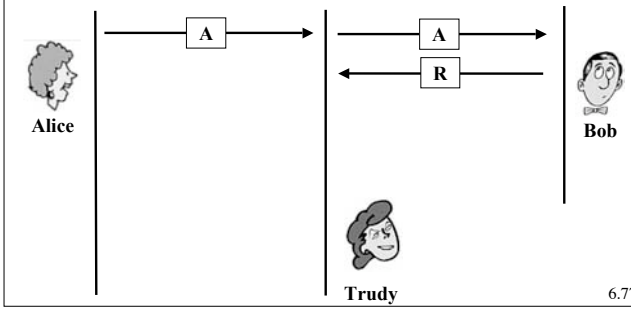
- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



6.77

Autenticazione

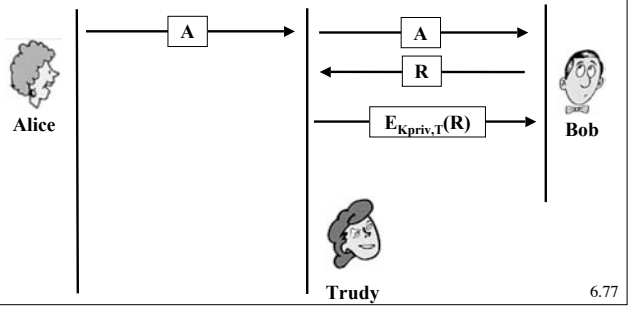
- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



6.77

Autenticazione

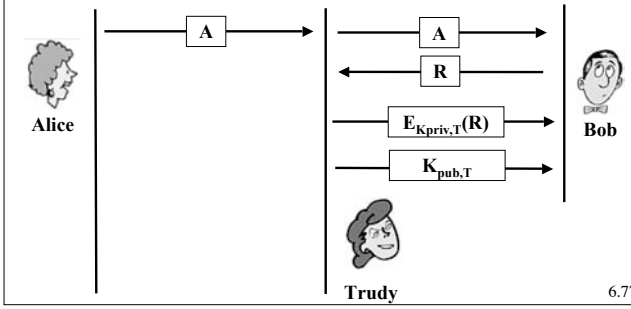
- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



6.77

Autenticazione

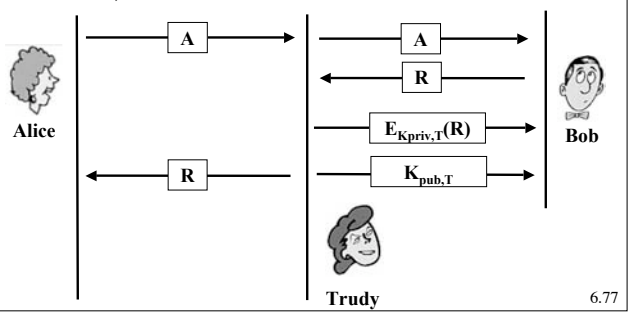
- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



6.77

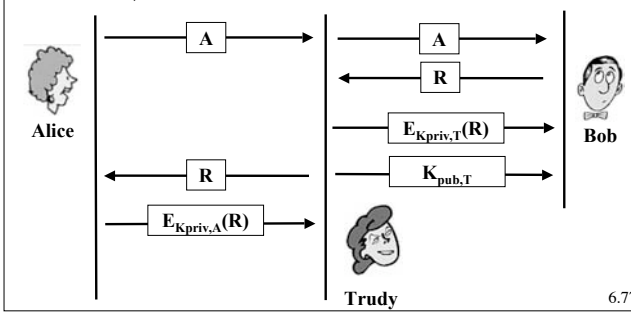
Autenticazione

- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



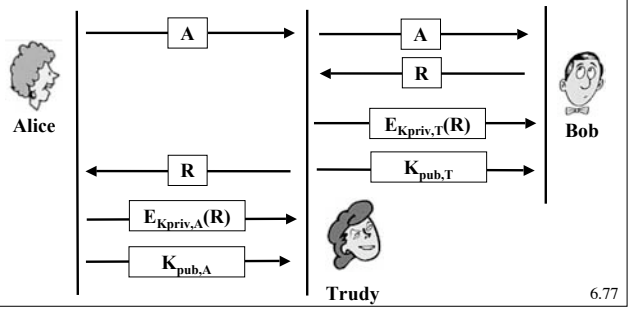
Autenticazione

- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)



Autenticazione

- AP7 è soggetto all'attacco nel mezzo (*in the middle attack*)

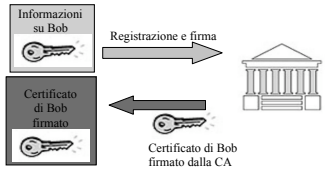


Autenticazione
Distribuzione delle chiavi

- Il problema dello scambio delle chiavi pubbliche in AP7 è risolto utilizzando i certificati.
- Un certificato è un documento elettronico in cui si trovano diversi dati dell'utente (nome, indirizzo, email, sito web) e la sua chiave pubblica.
- La validità del certificato (e quindi l'appartenenza della chiave pubblica al soggetto indicato) deve essere garantita da un'autorità riconosciuta da entrambe le parti.

Autenticazione
Distribuzione delle chiavi

- I certificati, per essere validi, devono essere "firmati" da una *Certification Authority* (CA), riconosciuta come fidata da tutti
  - le entità (persone, router, etc.) possono registrare le loro chiavi pubbliche alla CA;
  - l'entità che si iscrive deve fornire una "prova dell'identità" alla CA.



- Quando Alice vuole la chiave pubblica di Bob:
  - Prende il certificato di Bob (da Bob, dalle apposite *Directory*).
  - Applica la chiave pubblica della CA e ricava la chiave pubblica di Bob.

Autenticazione
Certificati X.509

- Uno degli standard più diffuso è X.509 (ITU).
- In sostanza, X.509 è una descrizione dei contenuti del certificato.
- I certificati X.509 sono codificati utilizzando ASN.1.

Version	Versione X.509
Serial Number	Identifica univocamente il certificato insieme al nome della CA
Signature Algorithm	L'algoritmo utilizzato per la firma
Issuer	Nome della CA
Validity period	Periodo di tempo in cui è valido
Subject name	Entità a cui appartiene il certificato
Public key	Chiave pubblica e algoritmo che la utilizza
Issuer ID	Un identificativo opzionale del soggetto che ha emesso il certificato
Subject ID	Un identificativo opzionale del soggeto del certificato
Extensions	Molte estensioni definite
Signature	Firma del certificato

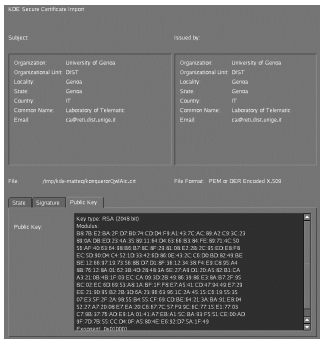
Autenticazione

Certification Authority

- Avere una sola certification authority non è possibile
  - carico di lavoro elevato;
  - punto critico in caso di guasti;
  - difficoltà di individuazione su scala mondiale.
- Si è pensato di utilizzare un diverso approccio, denominato PKI (*Public Key Infrastructure*):
  - certificati;
  - molteplici CA, organizzate gerarchicamente;
  - directory, per la conservazione dei certificati in locazioni pubbliche.
- L'organizzazione attuale prevede diverse CA all'apice della gerarchia
  - le loro chiavi pubbliche si trovano nei browser.
- I certificati possono essere revocati
  - aggiornamento delle *Certificate Revocation List* da parte delle CA;
  - in caso di abusi o compromissione della segretezza.

Autenticazione

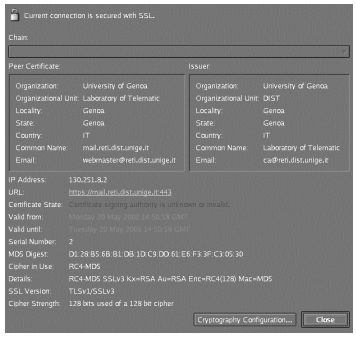
Certificati



Certificato di una CA autofirmato

Autenticazione

Certificati



Certificato di un server web firmato da una CA non riconosciuta dal browser

Autenticazione

Certificati

Certificato di un server web firmato da una CA riconosciuta dal browser

Autenticazione e segretezza

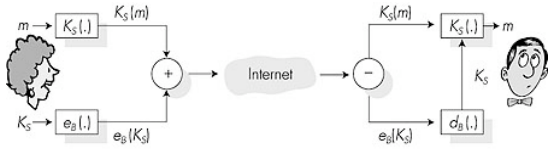
- Si osservi che la pratica usuale è quella di:
  - Usare chiave simmetriche per la cifratura dei dati (più veloci).
  - Cambiare spesso (ogni sessione o più) la chiave simmetrica.
  - Scambiarsi la chiave simmetrica tramite una cifratura a chiave pubblica.
  - Autenticare l'identità della chiave pubblica usando una CA.

Sicurezza - Protocolli

- Oltre che dal punto di vista della locazione fisica dei meccanismi di sicurezza, riveste una notevole importanza la scelta del loro posizionamento nella pila protocollare.
- I dispositivi di sicurezza possono essere implementati:
  - A livello di applicazione (ad es. email, DNS)
  - A livello di trasporto (ad es. SSL, SET)
  - A livello di rete (IPsec)
  - A livello di linea (WEP)

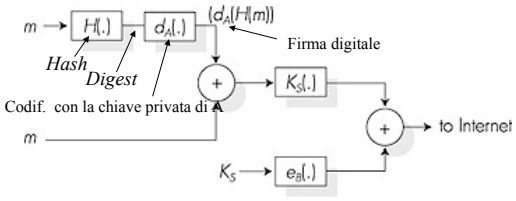
E-mail sicure - Segretezza dei dati

- Alice vuole inviare un messaggio m segreto a Bob



- Genera una chiave simmetrica casuale , K_S
- Cifra il messaggio con K_S, $K_S(m)$.
- Cifra anche K_S con la chiave pubblica di Bob, $e_B(K_S)$.
- Invia sia $K_S(m)$ che $e_B(K_S)$ a Bob

E-mail sicura - Segretezza, autenticazione ed integrità



- Il digest del messaggio viene cifrato con la chiave privata del mittente (firma e integrità)
- Il messaggio viene cifrato con una chiave simmetrica insieme alla firma; il tutto viene cifrato con la chiave pubblica del destinatario (segretezza)

E-mail sicura: standard

- PGP, *Pretty Good Privacy*
  - prevede autenticazione, segretezza, firma digitale e compressione;
  - gli utenti si scambiano le chiavi;
  - ad oggi è lo standard più diffuso.
- PEM, *Privacy Enhanced Mail*
  - standard IETF, RFC 1421-1424;
  - non è mai stato utilizzato (richiede una unica root per certificare).
- S/MIME, *Secure MIME*
  - si integra perfettamente con le codifiche MIME;
  - prevede una gerarchia di CA per la distribuzione di certificati con le chiavi pubbliche degli utenti.

E-mail sicura - PGP

Pretty Good Privacy (PGP)

- E' uno schema di di cifratura per e-mail, uno standard de facto.
- Usa la cifratura simmetrica (Triple-DES o IDEA) e a chiave pubblica (RSA), le funzioni di *Hash* (MD5 o SHA) e la firma digitale come descritto prima
- Quindi fornisce riservatezza, autenticazione del mittente e verifica dell'integrità del messaggio
- Inventato da Phil Zimmermann, oggetto per tre anni di indagini da parte federale (USA).

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3m
   qJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```


Sicurezza nei DNS - DNSSec

- DNS spoofing: un intruso può inserire risoluzioni errate nelle cache dei *Name Server*.
- DNSSec è un progetto per rendere sicura la risoluzione dei nomi in Internet (RFC 2535).
- I suoi obiettivi principali sono:
  - autenticare le transazioni;
  - distribuire le chiavi pubbliche appartenenti ai domini registrati;
  - distribuzione dei certificati degli utenti.

Secure Socket Layer (SSL)

- SSL opera a livello di trasporto e fornisce funzioni per la sicurezza ad ogni applicazione basata su TCP
- E' utilizzato da varie applicazioni fra cui www *server* e *browser* per servizi di *e-commerce* (shttp)
- I servizi per la sicurezza di SSL sono:
  - Autenticazione del server (tramite certificato firmato da CA fidate)
  - Cifratura dei dati
  - Autenticazione dei client (opzionale)
- E' la base della ***Transport Layer Security (TSL)*** dell'IETF

Secure Socket Layer (SSL)

- La comunicazione si compone di due protocolli:
  - instaurazione della connessione, permette di autenticare il server e di stabilire una chiave di sessione;
  - trasporto dell'informazione cifrata.
- SSL supporta diversi algoritmi di cifratura:
  - DES con 3 chiavi + SHA-1 a 168 bit è la combinazione più sicura, anche se molto lenta;
  - RC4 a 128 bit + MD5 è la combinazione più usata per il commercio elettronico, è più veloce ma anche più facile da violare.

Secure Socket Layer (SSL)

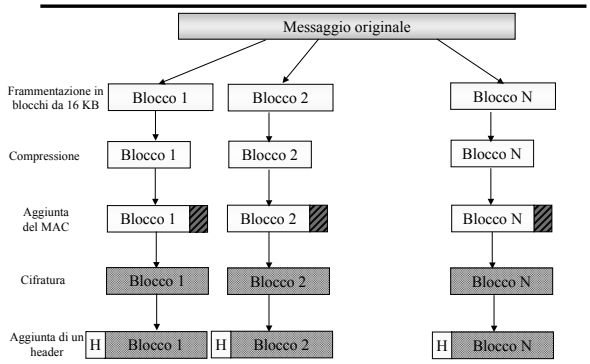
Autenticazione del server

- Un *browser* con SSL deve possedere la chiave pubblica di una o più CA.
- Il *browser* richiede il certificato del Server secondo uno dei CA che conosce.
- Il *browser* usa la chiave pubblica del CA per estrarre la chiave pubblica del Server.

Sessioni SSL

- Per effettuare lo scambio sicuro, SSL crea delle sessioni che possono essere usate anche da più connessioni TCP contemporaneamente
- La sessione prevede:
  - la generazione di una chiave simmetrica da parte del *browser*, cifrata con la chiave pubblica del server e ad esso inviata;
  - La decifratura della chiave simmetrica da parte del server
  - Uno scambio per definire se e come i messaggi verranno cifrati

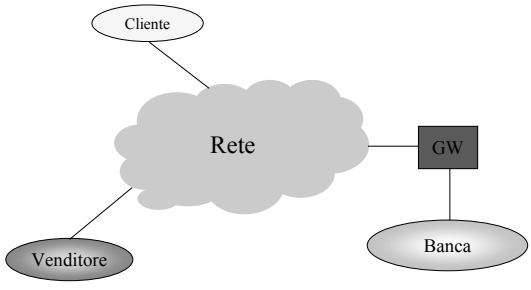
Secure Socket Layer (SSL)



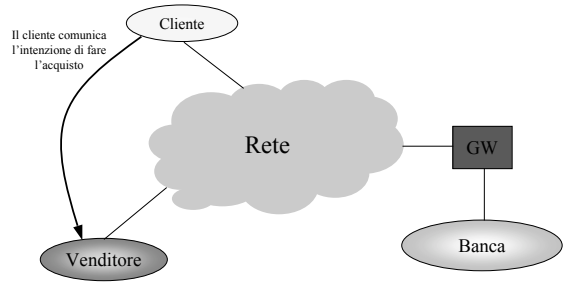
Secure Electronic Transaction (SET)

- E' stato progettato per realizzare i pagamenti via carta di credito e le transazioni via Internet (VISA e Mastercard);
- Prevede la presenza di tre attori che devono essere tutti certificati:
  - Cliente (certificato dalla propria banca)
  - Venditore (certificato dalla propria banca)
  - Banca (del venditore)
- Dà significato legale ai certificati;
- Il numero di carta di credito del cliente passa alla banca del venditore senza che quest'ultimo lo possa vedere.
- Tre componenti software:
  - *Browser wallet* (portafoglio)
  - *Merchant server*
  - *Acquirer Gateway*

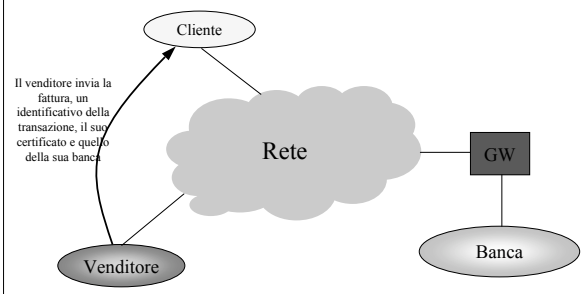
Secure Electronic Transaction (SET)



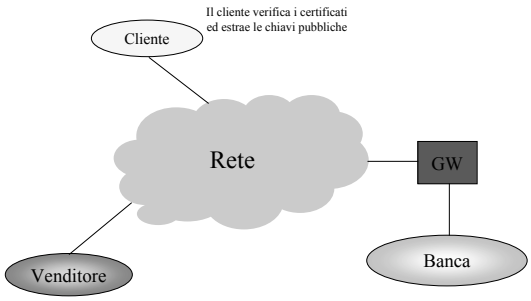
Secure Electronic Transaction (SET)



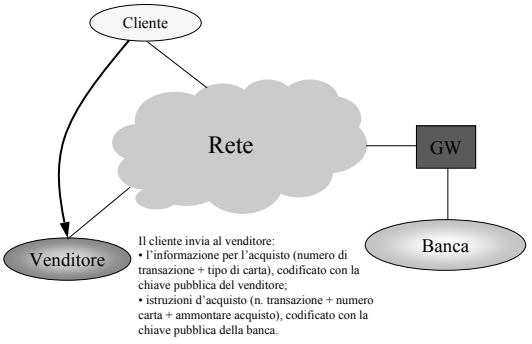
Secure Electronic Transaction (SET)



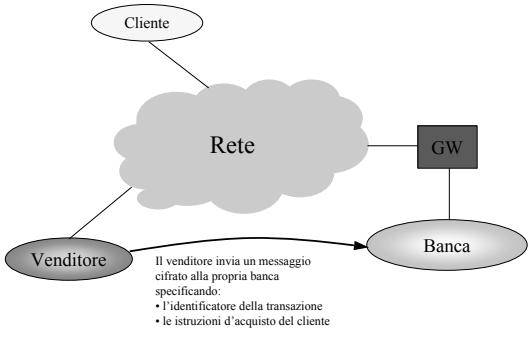
Secure Electronic Transaction (SET)



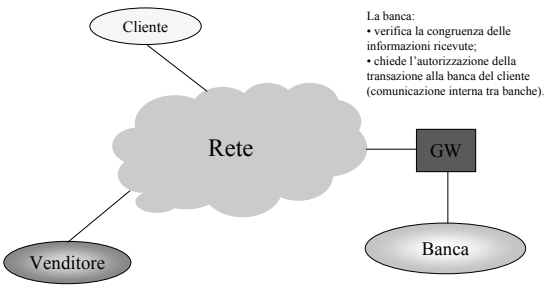
Secure Electronic Transaction (SET)



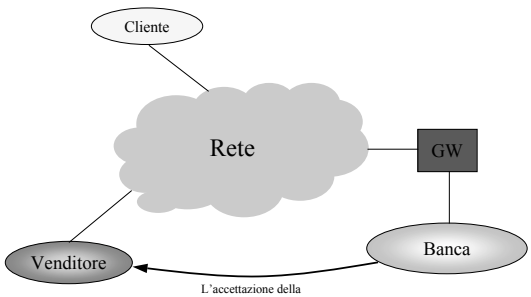
Secure Electronic Transaction (SET)



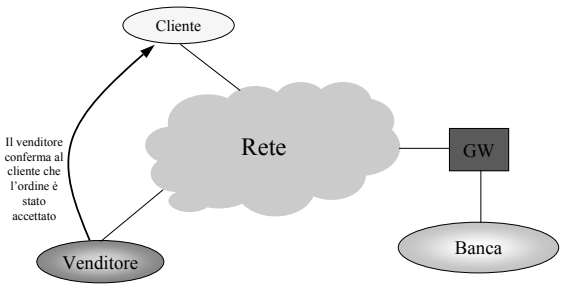
Secure Electronic Transaction (SET)



Secure Electronic Transaction (SET)



Secure Electronic Transaction (SET)



IPsec (IP security)

- La cifratura continua ad essere *end-to-end* ma viene effettuata nel livello di rete sui pacchetti IP e quindi diventa disponibile a tutti i protocolli che usano IP (oltre TCP, UDP, ICMP, SNMP,…).
- Per quanto concerne l'autenticazione, in questo caso questa può avvenire anche nei confronti di indirizzi IP.
- IPsec si compone di due protocolli:
  - ***Authentication Header* (AH) *protocol***
  - ***Encapsulation Security Payload* (ESP) *protocol***

IPsec (IP security)

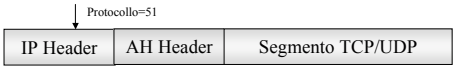
- Alcuni esempi di utilizzo di IPsec sono:
  - Interconnessione sicura di reti aziendali tramite Internet (in sostanza permette la realizzazione di ***Virtual Private Network*** (VPN)).
  - Accesso remoto sicuro in Internet.
  - Interconnessione sicura fra organizzazioni diverse via Internet.
  - Migliore sicurezza nel commercio elettronico.

IPsec (IP security)

- Ambedue i protocolli di IPsec (ESP e AH) operano tramite una canale logico a livello di rete chiamato ***Security Association*** (**SA**), creato tra sorgente e destinazione con un *handshake*.
- L'SA è
  - Unidirezionale
  - Univocamente determinato da:
    - » Protocollo di sicurezza usato (ESP o AH).
    - » Indirizzo IP della sorgente.
    - » ID a 32 bit della connessione (SPI, *Security Parameter Index*).

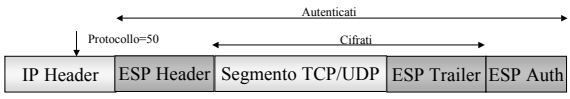
IPsec - AH

- Fornisce l'autenticazione dell'*host* e l'integrità dei dati ma non la riservatezza.
- L'intestazione AH viene inserita fra quella IP ed i dati
- Il numero di protocollo è il 51
- I *router* intermedi elaborano il *datagram* in modo usuale.
- L'intestazione dell'AH comprende:
  - un identificatore di connessione;
  - un campo che specifica il tipo di dati trasportati (UDP, TCP, ICMP…);
  - un numero di sequenza;
  - Un *digest* "firmato"e calcolato sul *datagram* originale.
- La firma di solito viene effettuata con la chiave simmetrica negoziata.



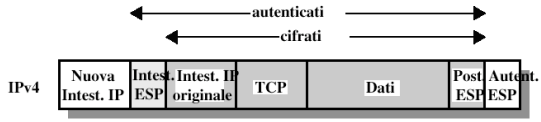
IPsec - ESP

- Fornisce la riservatezza, l'autenticazione dell'host e l'integrità dei dati
- I dati e il postambolo dell'ESP sono cifrati
- L'indicazione della successiva intestazione è nel postambolo ESP.
- L'header ESP contiene un numero di sequenza e il SPI.
- Il campo di autenticazione del ESP è simile ha quello dell'AH.
- Il numero di protocollo contenuto nell'intestazione IP quando si usa ESP è 50.



IPsec - Modalità di trasporto

- Due sono le modalità di funzionamento:
  - Modalità di trasporto
  - Modalità Tunnel
    - » applicabile se le due entità sono apparati intermedi come *router* o *firewall*.
    - » permette comunicazioni sicure a terminali che non usano IPsec.
    - » Permette la cifratura dell'intero pacchetto IP.



IPsec - SA

- L'architettura IPSec prevede due modalità per lo scambio delle chiavi:
  - manuale, configurata dagli amministratori sugli apparati;
  - automatica, nel qual caso è necessario un meccanismo automatico per lo scambio e la gestione delle chiavi
    - » *Internet Key Exchange* (IKE, RFC 2409) è il protocollo di default per lo scambio delle chiavi dell'IPSec;
    - » *Internet Security Association and Key Management Protocol* (ISAKMP, RFC 2047 e 2048) definisce le procedure per stabilire ed interrompere gli SA. L'associazione per la sicurezza ISAKMP definisce permette di utilizzare diversi algoritmi per lo scambio delle chiavi, tra i quali IKE.

WEP

- Le reti wireless sono per loro stessa natura particolarmente sensibili alle problematiche di sicurezza.
- L'802.11 nella sua versione originale prevede l'utilizzo della cosiddetta *Wired Equivalent Privacy* (WEP), un meccanismo che dovrebbe garantire lo stesso livello di sicurezza di una rete cablata.
- Ogni stazione condivide una chiave segreta con l'AP
  - il meccanismo di distribuzione di queste chiavi non è definito nello standard.

WEP

- L'algoritmo utilizzato è il RC4 (Rivest, 1994).
  - al messaggio viene aggiunto un CRC;
  - il risultato viene posto in XOR con un *keystream* generato dall'algoritmo RC4 a partire dalla chiave segreta e da un vettore iniziale IV;
  - il pacchetto risultante (IV + messaggio cifrato) viene inviato sul canale.
- La chiave in genere è la stessa per tutti gli utenti
  - tutti possono vedere il traffico della rete, come in una rete Ethernet.

WEP

- L'algoritmo non è molto sicuro:
  - è possibile riuscire a violare il codice osservando un numero di pacchetti non molto alto;
  - è perfino possibile ricavare una coppia IV-*keystream* per inteferire con la comunicazione.
- L'IEEE non prevede di migliorare questo meccanismo
  - ritiene il livello di protezione sia congruente con quanto definito inizialmente;
  - per il supporto di un maggior livello di sicurezza rimanda alla definizione dello standard 802.11i.

Bluetooth

- Il range trasmissimo di Bluetooth è più limitato di 802.11
  - minori problemi di sicurezza.
- Prevede 3 livelli di sicurezza, da nessuna protezione ad una completa cifratura e controllo di integrità.
- Due device Bluetooth per comunicare devono condividere una chiave (*passkey*)
  - i dispositivi scelgono il livello di sicurezza;
  - selezionano una chiave di sessione a 128 bit;
  - la cifratura avviene con un algoritmo denominato E_0 e il controllo di integrità con l'algoritmo SAFER+.
- Il livello di protezione non è molto elevato.
- Si possono autenticare solo i terminali e non gli utenti.

Sicurezza nelle reti di telecomunicazioni

Parte II

Sicurezza dei sistemi informativi

Sicurezza dei sistemi informativi

- Intrusioni:
  - rilevamento delle intrusioni;
  - gestione delle password.
- Software pericoloso:
  - Virus, trojan, worm;
  - protezione dei sistemi informatici.
- Firewall:
  - tecniche di implementazione dei firewall;
  - sistemi fidati.

Intrusioni

- La violazione di un sistema informativo può avvenire principalmente tramite due diverse tecniche:
  - intrusione (*hacker*);
  - introduzione di codice "ostile" (*virus, trojan*).
- L'intrusione consiste:
  - nel login da parte di utenti non autorizzati;
  - nell'acquisizione di privilegi senza autorizzazione da parte di utenti del sistema.
- La difficoltà della difesa di un sistema deriva dal dover sventare tutti gli attacchi possibili, mentre l'hacker si concentra su un solo anello debole della catena.

Intrusioni

- Classi di intrusioni:
  - *hacker*, attacco ai controlli di accesso per sfruttare l'account di un utente legittimo;
  - *utente legittimo*, acquisizione di privilegi superiori a quelli consentiti (dati, programmi o risorse).
- Tipologie di hacker:
  - esperti dalle sofisticate conoscenze tecniche
    - » hanno la capacità di individuare i punti deboli dei sistemi e mettere a punto gli attacchi;
  - "soldati semplici", senza particolare preparazione
    - » passano ore ad utilizzare gli strumenti preparati dagli esperti.
- Tipologie di attacchi:
  - benigni, dimostrazioni della abilità di un hacker;
    - » non causano danni ma consumano risorse;
  - maligni, volti ad azioni dannose o criminali.
- Non è possibile stabilire a priori la pericolosità di un attacco.

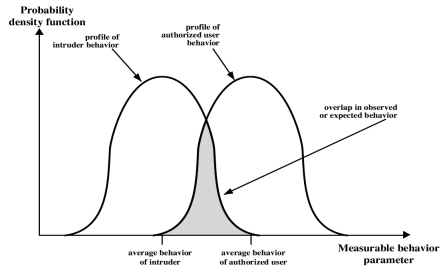
Tecniche di intrusione

- Obiettivo dell'hacker è quello di accedere ad un sistema o ampliare i propri privilegi.
- Tali operazioni possono avvenire conoscendo la password di altri utenti
  - le password devono essere protette:
    - » crittografia monodirezionale (per es. funzioni di hash);
    - » controllo degli accessi sul file delle password.
  - tecniche di violazione delle password:
    - » tentare le password di default dei sistemi;
    - » ricerca esaustiva di tutte le passwork brevi (es. 3 caratteri);
    - » parole di un dizionario e elenco di password probabili;
    - » informazioni personali riguardanti l'utente (nome, cognome, indirizzo, numero di telefono, targa, codice fiscale);
    - » cavallo di Troia;
    - » intercettazione della linea.

Rilevamento delle intrusioni

- La rilevazione di una intrusione assume una importanza fondamentale:
  - l'hacker può essere identificato ed espulso dal sistema prima di provocare danni;
  - rappresenta un deterrente verso i tentativi di accesso non autorizzato;
  - consente di raccogliere informazioni sulle tecniche di intrusione utilizzate.
- La rilevazione di una intrusione si basa sulla supposizione che il comportamento di un hacker differisca da quello di un utente autorizzato
  - purtroppo esiste sempre un'area di sovrapposizione:
    - » falsi allarmi;
    - » mancata identificazione degli intrusi.

Profili di comportamento



Gli schemi di comportamento degli utenti legittimi possono essere definiti osservando il passato. La stessa considerazione vale per i comportamenti degli hacker.

Rilevamento delle intrusioni

- Rilevamento statistico delle anomalie:
  - rilevamento a soglie;
  - sistema a profilo.
- Rilevamento a regole:
  - rilevamento delle anomalie;
  - identificazione delle anomalie.
- Lo strumento fondamentale è rappresentato dai record di auditing:
  - registrazioni native
    - » sono incluse in praticamente tutti i sistemi multiutente;
    - » potrebbero non contenere tutte le informazioni necessarie;
    - » variano da sistema a sistema;
  - registrazioni specifiche per il rilevamento
    - » contengono esclusivamente le informazioni necessarie per il rilevamento;
    - » possono essere utilizzate su diversi sistemi;
    - » sovraccaricano il sistema con registrazioni aggiuntive a quelle native;
  - i campi delle registrazioni determinano l'utilità dell'auditing
    - » soggetto, azione, oggetto, eccezzioni, uso delle risorse, time-stamp;
    - » le operazioni spesso sono decomposte in azioni elementari e registrate in questa forma.

Rilevamento delle intrusioni

- Un sistema di rilevamento delle intrusioni deve:
  - rilevare una grande percentuale di attacchi
    - » in caso contrario fornirebbe un falso senso di sicurezza;
  - evitare i falsi allarmi
    - » altrimenti gli amministratori tenderebbero ad ignorare gli allarmi o perderebbero troppo tempo nella loro analisi.

Rilevamento statistico delle anomalie

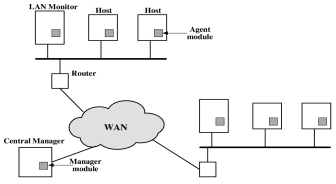
- Prevede la raccolta di dati relativi al comportamento degli utenti legittimi lungo un determinato arco di tempo.
- Rilevamento a soglia: conteggio degli eventi in un arco temporale e confronto con un valore "critico"
  - sistema abbastanza rozzo e poco attendibile;
  - utile se affiancato ad altri schemi.
- Rilevamento a profilo: definizione del profilo del comportamento di ogni utente e individuazione delle deviazioni significative
  - analisi dei record di auditing per definire il profilo e le deviazioni rispetto al comportamento medio;
  - definizione dei parametri rappresentativi del comportamento;
  - test per determinare la variazione:
    - » media e deviazione standard, multivariazione, processo di Markov, serie temporali, modello operativo.

Rilevamento a regole

- Si osservano gli eventi nel sistema e si applicano un insieme di regole per decidere se una determinata sequenza di attività è sospetta o meno.
- Rilevamento delle anomalie
  - simile al rilevamento statistico;
  - si basa sull'osservazione dei dati storici per identificare gli schemi d'uso e definire regole che descrivano tali schemi
    - » comportamenti passati, privilegi, sequenze temporali, ecc.
  - il comportamento corrente viene confrontato con le regole dedotte;
  - è necessario disporre di un database di regole consistente.
- Identificazione degli attacchi
  - usa regole per identificare gli attacchi noti
    - » sono specifiche della macchina e del sistema operativo;
    - » sono definite da esperti e non in modo automatico dall'analisi dei dati storici:
      - ✓ gli utenti non devono accedere a file di altri, gli utenti usano spesso gli stessi file, gli utenti non accedono direttamente ai dischi, gli utenti non copiano i programmi di sistema;
    - » sono condizionati all'abilità di coloro che identificano le regole.
  - manca di flessibilità: per la stessa situazione di attacco possono esserci diverse sequenze dei record di auditing. Per questo spesso si utilizzano meccanismi in grado di condensare diverse sequenze di eventi in una unica azione.

Sistemi di rilevamento distribuiti

- La difesa dei sistemi informatici è coordinata all'interno di una rete.
- È necessario garantire l'integrità e la sicurezza dei dati di auditing scambiati attraverso la rete.
- Il modulo d'agente raccoglie tutti i dati di auditing e li converte in un opportuno formato.
- Il LAN Monitor analizza il traffico della rete locale.
- Il Modulo Centrale raccoglie le informazioni dagli agenti ed effettua le elaborazioni per rilevare le intrusioni.



Honeypot

- Sono sistemi fittizi progettati per tenere lontano gli hacker dai sistemi critici.
- I compiti principali degli honeypot sono:
  - distrarre gli hacker;
  - raccogliere informazioni sulle attività degli hacker;
  - invogliare l'hacker a rimanere nel sistema un tempo sufficiente per essere rilevato.
- Gli honeypot non sono utilizzabili dagli utenti legittimi
  - ogni accesso è dunque sospetto.
- A volte si utilizzano vere e proprie reti di honeypot.
- Gli attacchi contro gli honeypot sembrano avere successo
  - gli amministratori hanno la possibilità di studiare il comportamento degli hacker.

L'autenticazione tramite password

- La password rappresenta il meccanismo utilizzato per verificare l'identità dell'utente.
- Nei sistemi Unix la password viene memorizzata crittografata
  - la procedura utilizzata consiste in 25 stadi basati su un algoritmo DES modificato:
    - » in questo modo non è possibile utilizzare hardware dedicato;
    - » l'algoritmo della forza bruta è troppo pesante;
  - la possibilità di disporre del file in cui sono memorizzate le password permette di utilizzare *password cracker* su macchine molto potenti;
  - l'incremento della potenza computazionale rende più debole il meccanismo, anche se ad oggi la forza bruta non è ancora utilizzabile per scardinare questo meccanismo.

L'autenticazione tramite password

- Uno dei principali problemi di sicurezza è rappresentato dagli utenti del sistema.
- Le password scelte spesso sono molto brevi.
- Es.: studio alla Purdue University
  - il 3% degli utenti ha password con meno di 4 caratteri.

Lunghezza	Numero	Frazione del totale
1	55	0,4%
2	87	0,6%
3	212	2%
4	449	3%
5	1260	9%
6	3035	22%
7	2917	21%
8	5773	42%
Totale	13787	100%

Debolezza delle password

- Molte persone scelgono password banali
  - questo rappresenta il secondo punto di debolezza dell'utilizzo delle password.
- Pes es. sono state attaccate circa 14000 password Unix crittografate provenienti da diversi sistemi utilizzando:
  - il nome dell'utente, il nome dell'account, le iniziali e altre informazioni personali;
  - circa 60000 parole provenienti da un dizionario del sistema;
  - varie permutazioni delle precedenti parole
    - » introduzioni di maiuscole/minuscole, sostituzione o-0;
    - » circa 3000000 di tentativi;
  - **sono state individuate circa il 25% delle password!**
  - il tempo di calcolo può essere di una sola ora.

Strategie di scelta della password

- La soluzione ideale sarebbe utilizzare password di 8 caratteri generate casualmente
  - gli utenti difficilmente riuscirebbero a ricordarsele.
- Un compromesso consiste nello scartare quelle troppo banali:
  - istruzioni all'utente
    - » molti utenti hanno un concetto errato di password "resistente";
  - password generate dal computer
    - » i meccanismi di generazione automatica sono in genere male accettati dagli utenti;
  - controllo reattivo
    - » il sistema esegue un *password checker* per individuare le password deboli;
    - » il meccanismo richiede tempo e risorse;
  - controllo proattivo
    - » la password è sottoposta ad una verifica preventiva prima di essere accettata.

Verifica proattiva delle password

- I controlli proattivi sono una soluzione di compromesso:
  - se troppo complessi comporteranno lamentele da parte degli utenti;
  - se troppo semplici danno utili indicazioni ai cracker.
- Approcci possibili:
  - definizione di regole
    - » lunghezza delle password pari a 8 caratteri;
    - » presenza di una lettera maiuscola, una minuscola, un numero ed un segno di punteggiatura;
  - dizionario delle parole inaccettabili
    - » problemi di spazio di memorizzazione e tempo di verifica;
  - utilizzo di un modello di Markov per la generazione delle password "semplici";
  - utilizzo di un filtro di Bloom.

Software pericoloso

- Trap door
  - punto di accesso segreto in un programma, per aggirare le normali procedure di accesso;
  - sono inserite dai programmatori per eseguire il debug dei programmi;
  - le misure di sicurezza devono concentrarsi nello sviluppo del programma.
- Bombe logiche
  - codice incluso in un programma legittimo;
  - la bomba è programmata per "esplodere" al verificarsi di determinati eventi
    - » presenza/cancellazione di determinati file;
    - » date/orari.

Software pericoloso

- Trojan
  - è un programma apparentemente utile che nasconde del codice indesiderato;
  - possono essere utilizzati per compiere azioni che richiedano i privilegi di altri utenti;
  - il trojan può risiedere in un compilatore che modifica tutti i programmi al momento della compilazione;
  - i trojan sono spesso cammuffati da inocue applicazioni.
- Zombie
  - è un programma che assume segretamente il controllo di un computer connesso in rete e lo utilizza per sferrare attacchi anonimi;
  - vengono impiantati in centinaia di computer e utilizzati per sommergere i siti web con un'enorme quantità di traffico.

Virus

- Il virus consiste in un programma che può infettare a sua volta altri programmi.
- La presenza di una rete contribuisce a facilitare la diffusione dei virus.
- Un virus può trovarsi in un qualsiasi punto di un programma eseguibile
  - il codice del virus viene richiamato immediatamente all'avvio del programma;
  - il virus "marca" i file infetti;
  - il virus svolge le operazioni per le quali è stato programmato, in genere un danneggiamento del sistema.
- Esistono diverse categorie di virus
  - parassiti, residenti in memoria, per il settore di boot, invisibili, polimorfici.

Virus a macro

- I virus a macro costituiscono oggi i 2/3 dei virus presenti.
- Sono indipendenti dalla piattaforma.
- Attualmente infettano principalmente i documenti MS Word.
- Una macro è un eseguibile (in genere Visual Basic) contenuto in un documento Word o Excel
  - le macro possono essere eseguite automaticamente
    - » Autoexecute, all'avvio di Word;
    - » Automacro, per un determinato evento (all'apertura/chiusura di un file, all'avvio di una applicazione);
    - » Macro di comandi, all'esecuzione di determinati comandi di Word.
- Una volta che la macro è in esecuzione può replicarsi in altri documenti e danneggiare il sistema.
- L'evoluzione più pericolosa viene propagata tramite le email (Visual Basic) e si attiva non appena si apre il messaggio o l'allegato (es. Melissa, 1999)
  - il virus si propaga generando altri messaggi email;
  - la diffusione di questi virus è rapidissima (ore, giorni).

Worm

- Come i virus delle email si propagano da sistema a sistema.
- In questo caso però la propagazione avviene senza l'intervento umano:
  - i worm cercano nuove macchine da infettare, da cui continuare a moltiplicarsi;
  - una volta attivo in un sistema, un worm può comportarsi come un virus o un trojan;
  - un worm si propaga attraverso la rete:
    - » messaggi di posta elettronica;
    - » funzionalità di esecuzione remota;
    - » funzionalità di login remoto.
  - l'individuazione dei potenziali host da infettare avviene esaminando tabelle interne al sistema.

Tecniche antivirus

- Prima generazione:
  - identificazione della struttura del codice del virus.
- Seconda generazione:
  - utilizzo di regole euristiche
    - » individuazione delle parti crittografate del virus e della chiave;
    - » verifica di integrità su tutti i programmi.
- Terza generazione
  - individuazione delle azioni dei virus
    - » l'antivirus deve risiedere in memoria.
- Quarta generazione
  - integrazione delle tecniche precedenti.

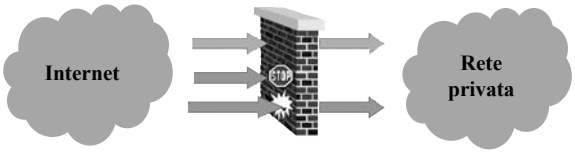
Tecniche antivirus avanzate

- Emulatori software
  - » emulano parti di un software prima della sua esecuzione.
- Sistema immunitario digitale
  - » integrazione e coordinamento dei diversi sistemi informativi al fine di individuare immediatamente il virus, rimuoverlo e aggiornare un database di conoscente condiviso.
- Software a bloccaggio del comportamento
  - si integra con il sistema operativo;
  - monitora una serie di operazioni potenzialmente pericolose:
    - » tentativi di accesso ai file, formattazioni, modifiche a file eseguibili o macro, modifiche a configurazioni critiche del sistema, eseguibili provenienti da siti web o allegati di posta, avvio di comunicazioni di rete;
  - blocca un programma nel caso rilevi comportamenti pericolosi;
  - per quanto ben cammuffato, un virus per creare danni ad un sistema deve per forza eseguire un determinato tipo di operazioni;
  - prima che il virus venga individuato devono essere state eseguite alcune operazioni dannose.

I firewall

- La connettività ad Internet rappresenta ormai una scelta quasi obbligata per la maggior parte delle aziende
  - sempre una maggior parte di applicazioni e servizi richiedono tale collegamento;
  - la connessione rappresenta un potenziale pericolo per l'azienda stessa.
- La protezione individuale di ciascuna workstation rappresenta un approccio poco pratico
  - difficoltà di gestione;
  - la rete locale necessita di alcuni servizi intrinsicamente poco sicuri (RPC, directory condivise, ecc.).
- La soluzione migliore consiste nell'utilizzo di un firewall.

I firewall



- Tutto il traffico scambiato tra la rete privata ed Internet deve attraversare il firewall.
- Solo il traffico autorizzato può attraversare il firewall.
- Il firewall è immune agli attacchi.

I firewall

- Un firewall
  - rappresenta l'unico punto di accesso alla rete
    - » offre la protezione da:
      - ✓ utenti non autorizzati;
      - ✓ servizi potenzialmente vulnerabili;
    - » semplifica la gestione della sicurezza
      - ✓ le funzionalità sono raggruppate in un unico sistema;
  - fornisce un sistema di monitoraggio degli eventi relativi alla sicurezza;
  - può fornire la piattaforma per il supporto di determinati servizi
    - » NAT, logging di accesso alla rete esterna;
  - può funzionare da piattaforma IPSec.

Funzionalità dei firewall

- Controllo dei servizi
  - determina quali servizi sono accessibili dall'esterno e dall'interno
    - » filtraggio indirizzo IP/porta TCP;
    - » proxy.
- Controllo della direzione
  - determina la direzione in cui possono essere attivate le richieste di servizi.
- Controllo degli utenti.
- Controllo del comportamento
  - relativamente all'utilizzo di determinati servizi:
    - » filtro antispam.

Limitazioni dei firewall

- I firewall non possono proteggere da attacchi in grado di oltrepassarli
  - sistemi informativi dotati di modem per l'accesso dall'esterno.
- Non proteggono nemmeno dalle minacce interne
  - dipendenti.
- Non impediscono il trasferimento di codice infettato da virus
  - sarebbe poco pratico eseguire tale scansione su tutto il traffico in ingresso.

Categorie di firewall

- Router a filtraggio dei pacchetti.
- Firewall di ispezione a stati.
- Gateway a livello delle applicazioni.
- Gateway a livello dei circuiti.

Router a filtraggio dei pacchetti

- Applicano un insieme di regole ad ogni pacchetto IP in ingresso
  - elimina o inoltra il pacchetto;
  - agisce in entrambe le direzioni.
- Le regole si basano su
  - indirizzo IP, di origine e di destinazione;
  - indirizzo di trasporto, di origine e destinazione
    - » definisce le applicazioni;
  - protocollo IP
    - » definisce il protocollo di trasporto;
  - interfaccia
    - » l'interfaccia da cui arriva/parte il pacchetto.
- Esiste sempre una politica di default
  - forward, rende più semplice l'utilizzo ma è molto pericolosa;
  - discard, i servizi vanno aggiunti singolarmente

Router a filtraggio dei pacchetti

- Vantaggi
  - semplicità di configurazione;
  - velocità di funzionamento.
- Svantaggi
  - non impedisce di sfruttare i bug di determinate applicazioni;
  - mancano di funzionalità di autenticazione degli utenti e di logging dettagliato;
  - sono sensibili alle configurazioni errate.

Attacchi ai router a filtraggio dei pacchetti

- Spoofing dell'indirizzo IP
  - ad esempio utilizzando indirizzi interni;
  - soluzione: non accettare pacchetti con indirizzi IP interni provenienti dall'esterno.
- Attacchi che utilizzino il *source routing*.
  - attualmente quasi tutti i sistemi escludono questo meccanismo;
  - soluzione: scartare questo tipo di pacchetti.
- Attacchi a frammentazione
  - l'intestazione TCP viene spezzata in diversi frammenti IP;
  - soluzione: scartare i pacchetti con "IP Fragment Offset" uguale a 1.

Firewall di ispezione a stati

- Le applicazioni di tipo client in genere utilizzano porte TCP nel range 1024-16383
  - l'apertura in ingresso di tutte queste porte rappresenta un punto debole del sistema.
- Un firewall a ispezione di stati tiene traccia di tutte le connessioni TCP attive
  - per ogni connessione si considerano
    - » indirizzo IP di sorgente e destinazione;
    - » porta TCP di sorgente e destinazione;
    - » stato della connessione;
  - il traffico in ingresso verso le porte appartenenti ad un certo intervallo (1024-16383) è accettato solo per le connessioni TCP attive.

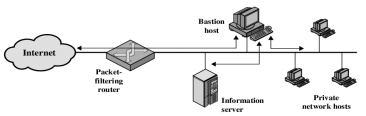
Gateway a livello delle applicazioni (proxy server)

- Si comporta come un ripetitore
  - l'utente contatta il gateway utilizzando l'applicazione di interesse (FTP, telnet, http);
  - il gateway richiede eventualmente l'autenticazione dell'utente;
  - il gateway contatta l'applicazione sull'host remoto e inoltra il traffico dell'utente;
  - il gateway può essere configurato per supportare solo alcune funzionalità dell'applicazione.
- Deve essere in grado di esaminare solo alcune applicazioni
  - risulta più sicuro rispetto ai filtri a pacchetto;
  - consente un maggior dettaglio di logging.
- Richiede un livello di elaborazione elevato per ogni connessione

Gateway a livello dei circuiti

- Configura due connessioni TCP
  - la prima tra l'utente interno ed il gateway;
  - la seconda tra il gateway e l'utente esterno.
- Il gateway inoltra i segmenti TCP tra le due connessioni senza esaminarne il contenuto
  - la funzione di sicurezza consiste nella scelta delle connessioni consentite.
- Il gateway può essere configurato per supportare anche il filtraggio a livello delle applicazioni
  - incorporare un proxy server per determinate applicazioni;
  - eseguire funzionalità proxy sul traffico in uscita.

Configurazione dei firewall



Single homed

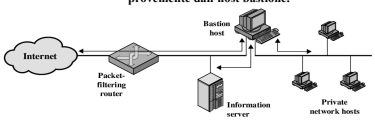
L'host bastione svolge le funzioni di autenticazione e proxy.

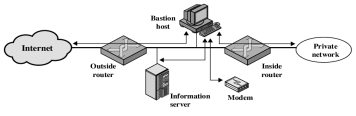
In ingresso è accettato solo il traffico verso l'host bastione.

L'uscita è consentita solo al traffico proveniente dall'host bastione.

Dual homed

Impedisce la comunicazione diretta fra gli host esterni e quelli interni in caso di violazione del firewall.





Sottorete schermata

Tre livelli di divesa contro gli hacker.

Il router esterno rende visibile solo la DMZ.

La rete privata ha la possibilità di accedere solo alla zona DMZ: gli host non possono creare percorsi diretti verso Internet