UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CDS IN INFORMATICA E COMUNICAZIONE DIGITALE

Anno Accademico 2015-2016

Corso di

"Reti di Calcolatori e Comunicazione Digitale"

Modulo 8: Cenni sulla sicurezza

Prof. Sebastiano Pizzutilo
Dipartimento di Informatica

LA SICUREZZA

Con il termine "sicurezza" si intende l'insieme delle misure tese ad assicurare a ciascun utente autorizzato (e a nessun altro) tutti e soli i servizi previsti per l'utente, nei tempi e nelle modalità previste.

In generale, secondo la definizione OSI X.800, la sicurezza è l'insieme delle misure atte a garantire :

- ***Disponibilità controllata delle informazioni: il sistema deve rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.***
- ***Integrità delle informazioni: il sistema deve impedire la alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali.***
- ***Riservatezza delle informazioni: il sistema deve impedire a chiunque di ottenere o dedurre, direttamente o indirettamente, informazioni che non è autorizzato a conoscere..***

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

LA SICUREZZA

- **Aspetti economico-legali e privacy** - La **legislazione sulla privacy** in Italia è attualmente contenuta nella Costituzione (articoli 15 e 21), nel Codice penale (Capo III - Sezione IV) e nel Decreto legislativo 30 giugno 2003, **n. 196**, intitolato **Codice in materia di protezione dei dati personali.**
- **Aspetti tecnici – conoscenza dell'hardware e del software (gestione dell'hardware, gestione multiutenza del S.O. / politiche di salvataggio /backup dati/ disk image/ RAID/ …reti,….).**
- **Aspetti software :**
  - ***Prerequisiti:***
    - ✓ Conoscenza dei potenziali nemici e tipologia di attacchi **(virus, worm,…);**
  - ***Contromisure:***
    - ✓ I software **antivirus** , che consentono di rilevare e rimuovere i **virus .**
    - ✓ I **firewall** , ovvero sistemi di filtraggio delle informazioni utilizzati per creare una barriera difensiva perimetrale, ovvero per rendere più difficili gli attacchi ai sistemi di una LAN prevenendo gli accessi non autorizzati.
    - ✓ La **crittografia** , che consente di far transitare sulla rete messaggi cifrati nascondendone il contenuto e inoltre offre supporto di base alla certificazione e alla firma digitale.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

La SICUREZZA in rete

In un contesto di sistemi collegati in rete si parla di sicurezza per indicare l'insieme di procedure, pratiche e tecnologie per proteggere le risorse, gli utenti e le organizzazioni che operano in rete.

Quindi un approccio sistematico alla sicurezza di rete deve prevedere la considerazione di tre elementi fondamentali:

- ✓ **Evento Indesiderato (attacco alla sicurezza).** ***Ogni evento che compromette la sicurezza del sistema di calcolo (hardware, software, dati) (virus, hacking, …).***
- ✓ **Servizio di sicurezza. *Ogni servizio che migliora la sicurezza del sistema e delle informazioni in transito (antivirus, directory service..).***
- ✓ **Meccanismo di sicurezza. Ogni soluzione progettata per scoprire, prevenire e recuperare un attacco alla sicurezza (*crittografia, backup*,…).**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Attacchi alla sicurezza

- **malicious software (malware)**
  programmi caratterizzati dal fatto che si diffondono da un computer all'altro con lo scopo di produrre danni ai sistemi.
  Caratteristiche dei malware più recenti :
  - ***sono più difficili da individuare,***
  - ***più efficaci nel diffondere l'infezione,***
  - ***spesso sono virus (meccanismo riproduttivo) e worm (utilizzano la rete per propagarsi).***

- **Il termine virus in informatica indica una porzione di codice che ha la caratteristica di autoreplicarsi e inserire se stesso in file eseguibili preesistenti sul sistema.** ***Il virus si autoinstalla su altri computers che in diversa maniera entrano in contatto con la "vittima" attraverso scambio di floppy disk, invio di posta elettronica, navigazione in Internet, download di files, etc….***

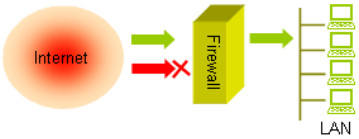
- **Un attacco di tipo DOS (Denial of Services) consiste nell' inondare di richieste casuali un host (un server) vittima, in modo tale che questi non riesca più a sopportare il carico di richieste e quindi smetta di funzionare.**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Firewall

Un Firewall (muro tagliafuoco**) è un sistema (** hardware e/o software**) che controlla il flusso di pacchetti che entra o esce da una LAN. Implementa specifiche politiche di filtraggio del traffico, confrontando i dati in transito sul sistema con profili di sicurezza predefiniti, per impedire accessi non autorizzati.**

Puo' essere realizzato sia come infrastruttura hardware dedicata sia utilizzando un computer e un opportuno insieme di software.



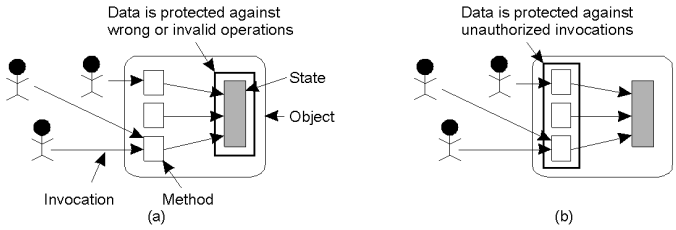
Il firewall agisce sui pacchetti in transito *da e per* una LAN, eseguendo su di essi operazioni di:

- ***Controllo***
- ***Modifica***
- ***Monitoraggio***

Un firewall ha la capacità di "aprire" il *pacchetto IP* per leggere le informazioni presenti sul suo *header*, e in alcuni casi anche di effettuare verifiche sul contenuto del pacchetto.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

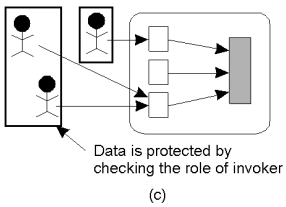
La protezione



a) *Protezione contro operazioni errate (necessario il **backup**)*

b) *Protezione contro operazioni non autorizzate (necessaria la "**autorizzazione**")*

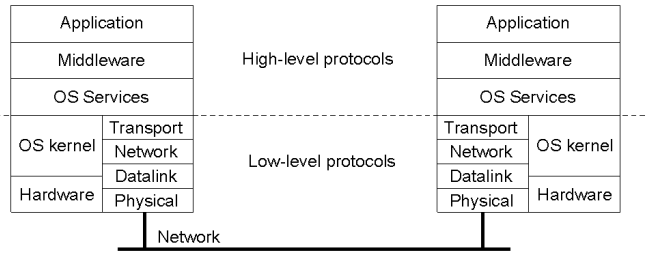
c) *Protezione contro utenti non autorizzati (necessaria la "**autenticazione**")*



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Stratificazione dei meccanismi di sicurezza

- ***Segretezza, riservatezza e integrità :*** ogni agente della comunicazione deve essere sicuro che nessun processo "ostile" o "non autorizzato" possa *modificare o distruggere* le informazioni trasmesse. ***(Cifratura)***
- ***Mutua autenticazione***: ciascun agente deve essere identificato (o autenticato), in modo da offrire sufficienti garanzie sull'identità del partner nelle comunicazioni. ***(firma digitale)***.
- ***Autorizzazione :*** protezione delle risorse in modo tale che solo gli agenti che abbiano i corretti privilegi d'accesso possano accedere e utilizzare le risorse . In letteratura la verifica dei privilegi d'accesso rientra nella categoria più ampia del controllo degli accessi, mentre l'autorizzazione si riferisce al processo di concessione dei privilegi d'accesso . ***(ACL, ticket)***.



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

I sistemi di Autenticazione

Active Directory è un insieme di servizi di rete adottati dai sistemi operativi della Microsoft ed utilizza vari protocolli (principalmente ***LDAP, DNS, DHCP, Kerberos***...)**.**

LDAP ad esempio viene usato come base dati centralizzata di tutti gli oggetti del dominio di rete: risorse (es. stampanti), servizi (es. email) e utenti (account utenti e gruppi).

L'insieme dei servizi di rete di Active Directory, ed in particolare il servizio di autenticazione ***Kerberos***, **realizzano il Single Sign-On (SSO)** per autenticare l'accesso ai servizi di una rete. Tramite tale meccanismo un utente, una volta entrato nel dominio ed effettuato quindi il ***logon*** da una qualsiasi delle macchine di dominio, può accedere a risorse disponibili in rete (condivisioni, mailbox, intranet ecc.) senza dover rieffettuare l'autenticazione.

- **I servizi Active Directory integrano il concetto Internet dello spazio dei nomi, utilizzando il servizio DNS (Domain Name System), e sono in grado di scambiare informazioni con le applicazioni che utilizzano il protocollo LDAP.**

- Active Directory è un Data Base System che in ambiente Microsoft Windows fornisce servizi di autenticazione, directory, gestione di security policy,….
- LDAP è un protocollo applicativo per effettuare query e modificare item in sistemi di directory service *(come Active Directory).*

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

ATTACCHI SOFTWARE

- ***ATTACCO PASSIVO (CONFIDENZIALITÀ' violata)***

Con uno *sniffer* Il nemico "origlia", tentando di ricavare informazioni

- ***ATTACCO ATTIVO (INTEGRITÀ' minacciata)***

Modifica dei messaggi :
Pagate 1000€ a Bob → **Pagate 100€ a Bob**
Cancellazione dei messaggi:
Pagate 1000€ a Bob → ✂ .....
Replicazione dei messaggi:
Pagate 1000€ a Bob → **Pagate 1000€ a Bob**
Pagate 1000€ a Bob
.....

AUTENTICAZIONE:
Sono Alice, accredita
1000 € a Mr. Lou Cipher → **Provami che sei Alice!**

AUTENTICAZIONE MUTUA:
Sono Bob → **Ciao Bob**
Sei la banca? → **Certo!**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Sniffing

attacco passivo: mira a compromettere riservatezza e autenticazione effettuando intercettazioni delle comunicazioni.

Se i dati viaggiano non criptati su una rete è possibile, da un qualsiasi punto della rete, intercettare i pacchetti in transito destinati ad altri host. *È critica la fase in cui il client invia, in chiaro, a un server le informazioni relative all'autenticazione dell'utente.*

Sniffer:

- **conversione dei pacchetti in una forma leggibile e filtraggio in base a criteri definibili dall'utente.**
- **Monitoraggio della rete, sia in termini di performance, che di traffico e di errori, anche attraverso log.**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Spoofing

diversi tipi di attacchi che hanno come meccanica comune quella della sostituzione. In particolare:

- **se ci si sostituisce a un utente senza averne diritto, si sta facendo user account spoofing.**
- **Se si prende il controllo di un canale di comunicazione e su questo si modifica il contenuto dei pacchetti, si sta facendo data spoofing.**
- **Se si manipola l'indirizzo IP da cui parte una certa connessione in modo da far credere di essere un sistema sorgente differente, si sta facendo IP spoofing (o IP address spoofing).**

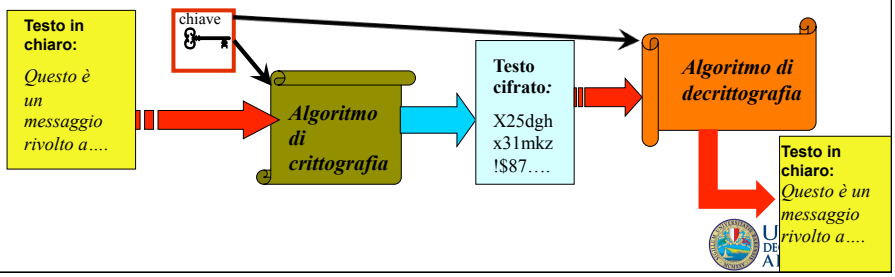
l'IP spoofing è il più noto e diffuso, e ha come obiettivo quello di aggirare i principali controlli attivi che sono basati sul monitoraggio degli indirizzi IP

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Crittografia: un po' di terminologia

Cifratura =crittografia da kryptòs (nascosto)

- ***Testo in chiaro*** : il messaggio originale da fornire in input all'algoritmo di cifratura;
- ***Algoritmo di crittografia (o cifratura)*** : algoritmo che esegue varie sostituzioni e trasformazioni del testo in chiaro;
- ***Chiave :*** è un dato in input all'algoritmo di cifratura, indipendente rispetto al testo ed in base al quale l'algoritmo produce un output differente;
- ***Testo cifrato*** : messaggio cifrato che risulta in output dall'algoritmo di cifratura;
- ***Algoritmo di decrittografia*** : algoritmo di crittografia eseguito al contrario, che accetta cioè in input il testo cifrato e la chiave e produce in output il testo in chiaro



Sistemi di CIFRATURA

I sistemi crittografici sono caratterizzati da **tre elementi indipendenti:**

- **Le operazioni per trasformare il testo in chiaro in testo cifrato** (*algoritmi per sostituzione, per scorrimento, per trasposizione o misti*).
- **Il numero di chiavi utilizzate (** *simmetrico o asimmetrico* **).**
- **Il modo in cui viene elaborato il testo in chiaro** (*a blocchi o a flusso*).

Un esempio: Algoritmo di Cifratura di Cesare

Dato un testo, ***si sostituisce ciascuna lettera dell'alfabeto del testo in chiaro con la lettera dell'alfabeto*** *che si trova* ***a tre*** *posizioni di distanza .*

Dato un alfabeto di 26 lettere ed assegnando un equivalente numerico a ciascuna lettera partendo da 0 : ogni lettera p del testo in chiaro si sostituisce con la lettera c (= p+3) del testo cifrato :

$$C = E(p) = (p + 3) \bmod(26)$$

L'algoritmo di decrittografia sarà semplicemente $P = D(C) = (C - 3) \bmod(26)$

Es: "ci vediamo alle 20 in piazza Umberto" Testo in chiaro

"fl yhgkdpr dooh 53 lq sldccd xpehuwr… Testo cifrato

La CIFRATURA tradizionale

Code-talkers navajo
1942

Tipi di cifratura tradizionale:

- **a sostituzione**, monoalfabetico o polialfabetico, le lettere del testo in chiaro viene sostituito da uno (*crittografia araba del X secolo, cifratura di Cesare*) o più caratteri dello stesso alfabeto o di una nuova nomenclatura (*Babington 1586 Maria Stuarda*).

- **a scorrimento**, ogni lettera del testo originario viene sostituita da numeri che corrispondono alla posizione della lettera nell'alfabeto. Tali numeri vengono sommati ad un numero prefissato (chiave) e nel testo cifrato viene inserita la lettera corrispondente al nuovo numero ottenuto dalla somma.(*crittogramma di Beale 1885 con book-cipher la dichiarazione di indipendenza americana*)

- **a trasposizione**, le lettere del testo vengono cambiate di posizione secondo il valore di una chiave che specifica la posizione di ogni lettera del testo in chiaro dove va spostata nel testo cifrato (*tavole di Vigener 1586*).

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

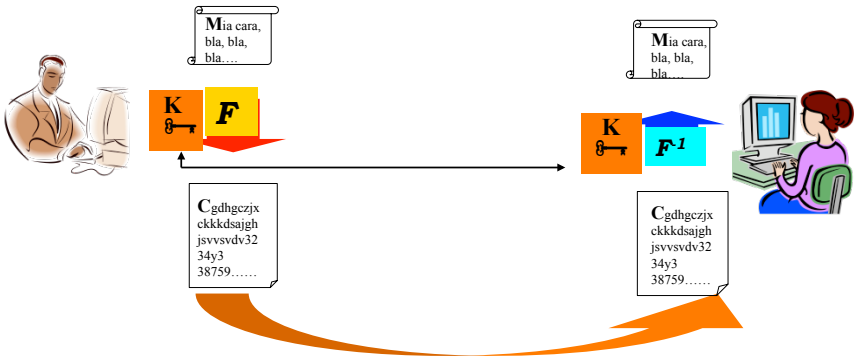
La CIFRATURA moderna

Cifrari moderni (sui computer) che operano a livello di bit:

- **XOR** consiste nell'effettuare una operazione XOR tra blocchi di bit del testo in chiaro con i bit di una chiave della stessa lunghezza.
- **a rotazione,** gli n bit della stringa originaria vengono spostati a destra o a sinistra in maniera circolare.
- **a sostituzione (S-Box),** sostituzione di stringhe di n bit con m bit (con n = < m).
- **a trasposizione (P-Box),** trasposizione dei bit in input con eventuale compressione o espansione dei bit.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

La cifratura SIMMETRICA



METAFORA: CASSAFORTE

Chiunque vuole aprirla, per mettere o togliere valori, deve conoscerne la combinazione

- ***A e B concordano* F( ) *e* F'( )**
- ***La chiave K è un segreto condiviso tra A e B***
- **La chiave *K* definisce un canale sicuro tra A e B**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

La cifratura SIMMETRICA

I metodi utilizzati per la crittografia **classica** sono metodi a chiave **simmetrica**, basati sull'ipotesi che gli alleati condividano una chiave nota solo a loro (e per questo detta segreta o anche **privata**).

Algoritmo di cifratura → **F( )** *Il messaggio cifrato* **C = F(K, M)**

Algoritmo di decifratura → **F'( )** *Il messaggio in chiaro* **M'= F'(K, C) = F'(K, F(K, M))** con M=M'

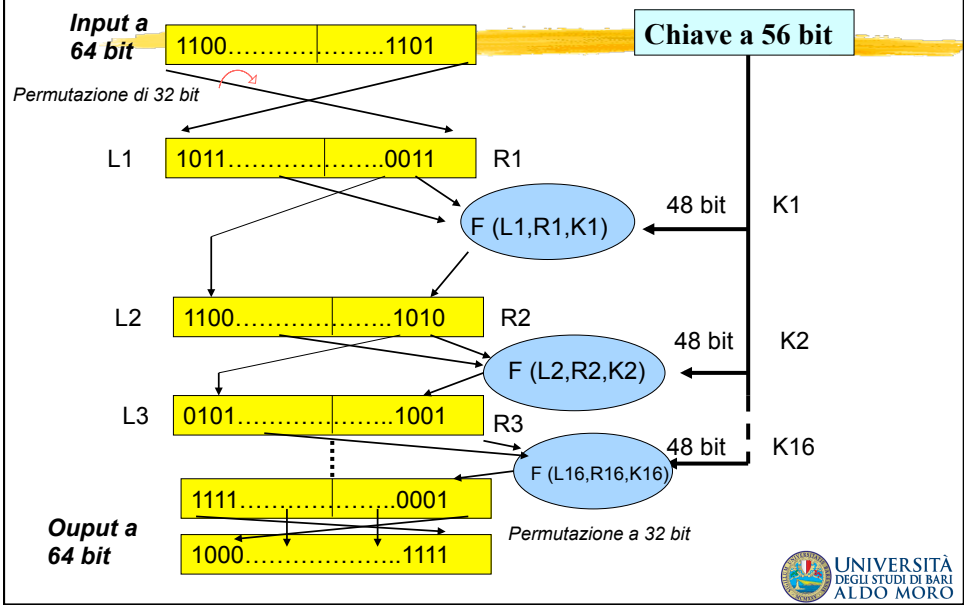
➔ **PROPRIETÀ di F( ) e F'( )**

I. Dato *C* , deve essere *difficile* ricavare *M* se non si conosce *K* e viceversa…

II. Dati *M* e *C*, deve essere *difficile* ricavare *K*, a meno che *K* non sia utilizzata una sola volta.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Esempio: **DES**



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

La cifratura SIMMETRICA

PRINCIPALI ALGORITMI

ALGORITMO	*CHIAVE (bit)*
CAST	**128**
Blowfish	**128**
IDEA	**128**
Triple-DES	**112**
DES (1977)	**56**

(K=testo in blocchi di 64 bit permutato più volte, con scambio di bit ed infine permutazione inversa per produrre un blocco di testo cifrato a 64 bit)

La chiave K non può essere trasmessa in chiaro via rete perché la rete è insicura.

Possibili soluzioni:

– A e B si accordano sulla chiave in un incontro faccia a faccia,

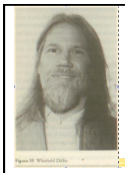
– A spedisce la chiave a B tramite un corriere,

– A suddivide la chiave in tanti pezzetti ed invia ciascun pezzetto a B attraverso un diverso canale di comunicazione (telefono, email, piccione viaggiatore,…).

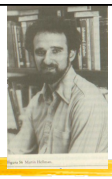
Non sempre queste soluzioni sono possibili e/o economiche…inoltre è necessaria una chiave diversa per ogni coppia di utenti.

Con n utenti sono necessarie circa n(n-1)/2 chiavi . ⇒ Scarsa scalabilità

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

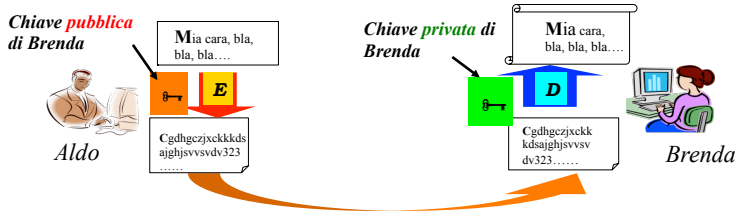


LA CIFRATURA ASIMMETRICA



Diffie ed Helmann nel '75 idearono la cifratura ***asimmetrica*** per risolvere il problema della diffusione della chiave tra due utenti.

METAFORA: L'utente A chiude il suo messaggio in una cassetta con un proprio lucchetto e spedisce la cassetta a B conservando la sua chiave. B riceve la cassetta ed appone un secondo lucchetto conservando la sua chiave. B trasmette la cassetta con due lucchetti ad A. A toglie il suo lucchetto e rispedisce a B la cassetta con il solo lucchetto di B. B finalmente può aprire con la sua chiave il lucchetto e leggere il messaggio.



La crittografia asimmetrica è un metodo di cifratura basato sull'esistenza di due diverse chiavi, una chiave pubblica utilizzata per criptare ed una chiave privata utilizzata per decriptare. La metafora che la descrive è quella della cassetta postale: *Chiunque può inserire un messaggio nella cassetta ma solo chi ha la chiave (privata) può aprire la cassetta e prelevare il messaggio.*

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CIFRATURA ASIMMETRICA

K1 = chiave pubblica destinatario
K2 = chiave privata del destinatario
M= messaggio in chiaro, D= messaggio cifrato
Alg. cifratura = E( ) Alg. Decifratura = D( )

ad esempio: A** vuole inviare un messaggio segreto M a **B

1. **A si procura K1, la chiave pubblica di B**
2. **A calcola *C* = E(*K1*, *M*)**
3. **A invia *C* a B**
4. **B decripta il messaggio con la sua chiave privata K2**, cioè **calcola *M* = D(K2 , *C*)**

PROPRIETÀ di E( ) e D( )

I. Dato *C*, deve essere difficile ricavare *M* se non si conosce *K2*.
II. Dati *M* e *C*, deve essere difficile ricavare *K1*, a meno che *K1* non sia utilizzata una sola volta.
III. Anche se si conosce *K1* deve essere difficile ricavare *K2* e viceversa.

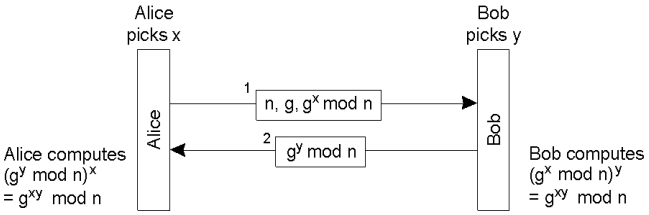
UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Il principio di Diffie-Hellman per lo scambio della chiave pubblica

Consente a due entità di stabilire una chiave condivisa e segreta utilizzando un canale di comunicazione insicuro (pubblico) senza la necessità che le due parti si siano scambiate informazioni o si siano incontrate in precedenza.

Nell'implementazione originale del 1976 del protocollo si considera inizialmente un numero ***g***, generatore del gruppo moltiplicativo degli **interi modulo *n***, dove ***n*** è un numero primo.

- Uno dei due interlocutori **A** sceglie un numero casuale ***x*** e calcola il valore $A = g^x \bmod n$ e lo invia attraverso il canale pubblico a **B**, assieme ai valori ***g*** e ***n***.
- **B** da parte sua sceglie un numero casuale ***y***, calcola $B = g^y \bmod n$ e lo invia ad **A**.
- **A** calcola $K_A = B^x \bmod n$, mentre **B** calcola $K_B = A^y \bmod p$.



Questo metodo non risolve completamente il problema di un potenziale eavesdropper che intercetta le comunicazioni tra A e B e si interpone tra i due spacciandosi per A o per B

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CIFRATURA ASIMMETRICA per assicurare l' autenticità

AUTENTICITÀ

***A** vuole inviare un messaggio non segreto **M** a **B** ma vuole fornirgli una prova di autenticità*

1. **A calcola $C = E(PRIV_A, M)$**
2. **A invia (M, C) a B**
3. **B calcola $M' = D(PUB_A, C)$ e verifica che $M \equiv M'$**

METAFORA: LA FIRMA

Solo chi ha la chiave privata può firmare un documento. Tutti gli altri possono verificare la firma con la chiave pubblica.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CIFRATURA ASIMMETRICA

SEGRETEZZA + AUTENTICITÀ

A vuole inviare un messaggio segreto M a B, fornendogli anche una prova di autenticità

1. **A calcola $Z = E(PRIV_A, M)$**
2. **A si procura PUB_B, la chiave pubblica di B**
3. **A calcola $C = E(PUB_B, Z)$**
4. **A invia *C* a B**
5. **B calcola $Z = D(PRIV_B, C)$**
6. **B si procura PUB_A, la chiave pubblica di A**
7. **B calcola $M' = D(PUB_A, C)$ e verifica che $M \equiv M'$**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CIFRATURA ASIMMETRICA

ALGORITMI PIÙ DIFFUSI

- **RSA(1978)** – probabilmente il più diffuso; basato sulla scomposizione in fattori primi di un numero intero, (RSA dal nome dei suoi creatori **R**ivest, **S**hamir e **A**dleman dell'MIT) . La sua sicurezza non è stata provata.

- Knapsack (1978) – violato più volte, non è considerato sicuro
- Rabin(1979)
- ElGamal (1985)
- Schnorr(1991)

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Sistema di crittografia a chiave pubblica: RSA

Ad esempio **l'utente A vuole spedire un messaggio segreto a B**.

Semplificando i passaggi di RSA:

1. **B** sceglie due **numeri primi molto grandi** (per esempio da 300 cifre) e li moltiplica con il suo computer,
2. **B** invia il numero ottenuto (la sua chiave pubblica) **ad A**. Chiunque può vedere questo numero.
3. **A** usa questo numero per cifrare il messaggio.
4. **A** manda il messaggio cifrato **a B**, chiunque può vederlo ma non decifrarlo.
5. **B** riceve il messaggio e, utilizzando i due fattori primi che solo lui conosce, lo decifra.

A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire **i due fattori primi** con cui decifrare il messaggio.

Per trasmettere grandi quantità di dati occorre tanto tempo. La soluzione è che A e B si scambino con questo sistema solo la chiave segreta (che non occupa molto spazio), che poi useranno per comunicare tra loro usando un sistema a crittografia simmetrica, più semplice e veloce.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CENTRO DISTRIBUZIONE CHIAVI (CDC)
per l'AUTENTICAZIONE

L'ALGORITMO ASIMMETRICO NON RICHIEDE SEGRETI CONDIVISI; QUANDO NECESSARIO BASTA SOLO (!!) PROCURARSI LA CHIAVE PUBBLICA DEL PARTNER…

…MA DOVE SI VA A PRENDERLA?

IL CENTRO DISTRIBUZIONE CHIAVI (CDC) è una terza entità incaricata di generare le coppie di chiavi pubbliche e private di ciascun utente e provvede a spedirle agli utenti interessati ad una comunicazione sicura.

DISTRIBUZIONE DELLE CHIAVI

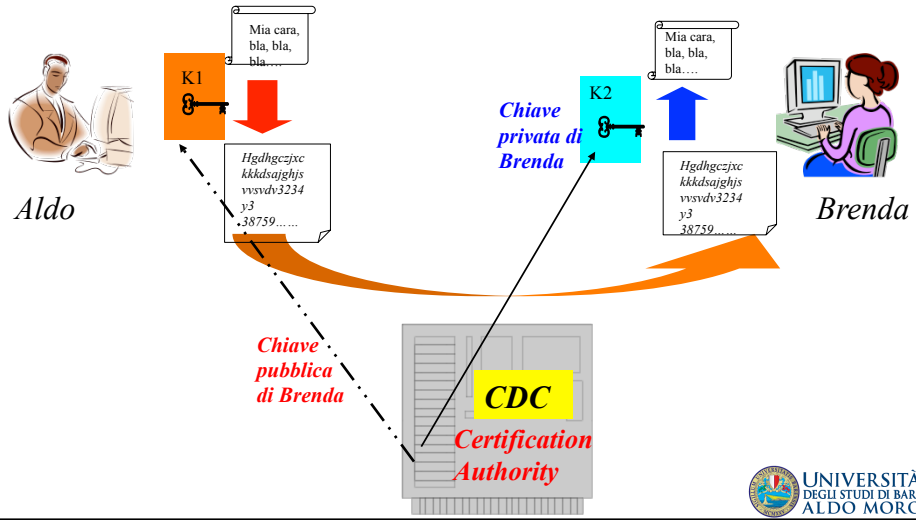
A vuole conoscere la chiave pubblica (PUB_B) di B:

1. **A -> CDC: PUB_B** *A chiede a CDC la chiave pubblica di B*
2. **CDC -> A: B, PUB_B** *CDC invia ad A la chiave pubblica di B*
   A ritiene che PUB_B sia la chiave pubblica di B.
3. **A -> B: E(PUB_B, M)** *A invia un messaggio crittografato a B*

Sembra tutto a posto ma…?

…. Chi mi garantisce che il messaggio ricevuto sia realmente del CDC ?

Centro Distribuzione Chiavi Certificate
per l'AUTENTICAZIONE



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

I CERTIFICATI
per l'AUTENTICAZIONE

Il problema nasce dal fatto che A ha attribuito il messaggio a CDC ma non c'è nessuna prova che quel messaggio sia effettivamente del CDC.

***È un problema di autenticità e non di segretezza*: il messaggio non trasporta alcuna informazione segreta**

Un problema analogo può nascere quando A vuole la chiave pubblica di B per verificare una firma digitale che si presume di B

SOLUZIONE:

Il CDC deve rilasciare un CERTIFICATO: cioè un documento firmato dal CDC che stabilisce il collegamento utente-chiave.

CDC viene detto CERTIFICATION AUTHORITY (Autorità di Certificazione)

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

DISTRIBUZIONE CHIAVI CON CERTIFICATO per l'AUTENTICAZIONE

DISTRIBUZIONE CHIAVI CON CERTIFICATO

A vuole sapere la chiave pubblica PUB_B di B

1. **A -> CDC :** ***A*** *chiede a* ***CA*** *la chiave pubblica di* ***B***
2. **CDC ->A: E(*$PRIV_{CA}$*, *PUB_B*)** ***CA*** *trasmette ad* ***A*** *la chiave* PUB_B, ***certificata con la sua firma privata***. ***A*** *conosce la chiave pubblica di CA e riconosce la sua firma convincendosi che* PUB_B *è la chiave pubblica di* ***B.***
3. **A -> B: E(*PUB_B*, *M*)** ***A*** *invia un messaggio segreto a* ***B*** *utilizzando la chiave pubblica di B.*

PROBLEMA : CHI CERTIFICA UNA CA?

Dopo il *msg* 2**, A** deve verificare la firma **di CA.**
Ma come fa **A** ad essere sicura che ***PUB_{CA}*** è proprio la chiave pubblica di **CA ?**

SOLUZIONE:

- **CA** pubblica ***PUB_{CA}*** sui quotidiani più importanti;
- La chiave di **CA** è certificata da un'altra **CA ,** un'altra chiave pubblica, un altro certificato e così via…_ **(CERTIFICATION HIERARCHY).**

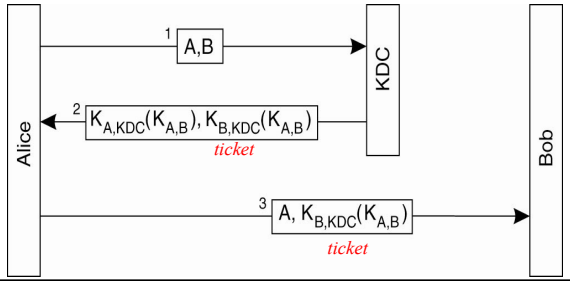
ESEMPI: X.509, AIPA

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Protocollo di autenticazione di Needham-Schroder per l'AUTENTICAZIONE

Se il mittente *A* vuole instaurare un canale sicuro con il ricevente *B* può farlo attraverso l'utilizzo di un **Key Distribution Center.**

1. ***A*** **invia un messaggio al KDC, comunicandogli di voler parlare con** ***B.***
2. **Il KDC restituisce ad A un messaggio contenente la chiave condivisa con B ($K_{A,B}$) crittografata con la chiave segreta che *A* condivide con il KDC ($K_{A,KDC}$).**
3. **il KDC delega *A* a contattare il ricevente *B*, inviandoli la chiave condivisa con B ($K_{A,B}$) crittografata con la chiave pubblica di B ($K_{B,KDC}$) = *ticket*.**
4. **A contatta B inviandogli il ticket .**
5. **Il ricevente B sarà l'unico che può fare uso del ticket, dato che è l'unico, oltre al KDC, che sa come decodificare l'informazione che contiene.**



Fingerprint *per l'integrità e la confidenzialità*

Per rendere più efficiente il meccanismo di trasmissione con firma dei messaggi si utilizza una funzione hash attraverso la quale si calcola una stringa identificativa del messaggio, detta fingerprint (impronta digitale) composta da un numero limitato di caratteri (solitamente 128 bit).

"Hash" è una funzione operante in un solo senso (che *non può essere invertita*), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di *"impronta digitale"* del testo in chiaro, e viene detta *valore di hash*, *checksum crittografico* o *message digest*.

La funzione hash deve inoltre essere molto veloce da calcolare, in modo da rendere significativamente vantaggioso creare il fingerprint del messaggio e criptare quello, piuttosto che criptare tutto il messaggio.

A questo punto è possibile assicurare l'integrità del messaggio limitando l'uso dell'algoritmo di crittografia a chiave pubblica al solo fingerprint.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Funzione hash

Le funzioni (algoritmi) "Hash" elaborano qualunque insieme di bit e possiedono i seguenti requisiti:

1) L'algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto Digest.

2) La stringa di output è univoca per ogni documento e ne è un identificatore. Perciò, l'algoritmo è utilizzabile per la firma digitale.

3) L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output.

- Quando due testi producono lo stesso ***hash***, si parla di ***collisione***, e la qualità di una funzione di hash è misurata direttamente in base alla difficoltà nell'individuare due testi che generino una collisione.
- La lunghezza dei valori di hash più comunemente adottata è di 128 bit. Tuttavia va registrata la possibilità d'uso di hash di dimensione maggiore (SHA, ad esempio, può anche fornire stringhe di 224, 256, 384 e 512 bit).

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Firme Digitali *per l'integrità e la confidenzialità*

- **Le funzioni hash possono essere anche utilizzate per la creazione di *firme digitali*, in quanto permettono la rapida creazione della firma anche per file di grosse dimensioni, senza richiedere calcoli lunghi e complessi**:

è infatti computazionalmente più conveniente eseguire con rapidità un hashing del testo da firmare, e poi autenticare solo quello, evitando così l'esecuzione dei complessi algoritmi di crittografia asimmetrica su grosse quantità di dati.

- **La firma digitale è definita come il Digest di un documento crittografato con chiave privata** (e non con quella pubblica, come avviene di solito).

- **La firma digitale è l'unico caso in cui l'uso delle chiavi è invertito: *la chiave pubblica serve a decrittare la firma e trovare il Digest iniziale, mentre quella privata serve a crittografare una stringa anziché ad aprirla.***

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Fingerprint *per l'integrità e la confidenzialità*

Quando A vuole mandare a B un messaggio autenticato e integro, calcola il fingerprint, lo cripta con la sua chiave privata e lo aggancia in fondo al messaggio in chiaro.

Quando B riceve il messaggio può decriptare con la chiave pubblica di A il fingerprint e verificare che esso corrisponda applicando la funzione di hash al messaggio ricevuto. *Se non c'è conformità tra il fingerprint calcolato e quello autenticato, il messaggio non è integro.*

Un algoritmo di *hash* molto utilizzato in crittografia è MD5 (Message Digest 5, 1992) che produce *fingerprint* di 128 bit.

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

MD4

- L'**MD4** è una funzione crittografica di hashing scritta da Ronald Rivest del MIT nel 1990.
- L'**MD4** è utilizzato per la generazione di un *message digest* (o "impronta del messaggio", una stringa di lunghezza fissa) di 128 bit da un messaggio di lunghezza variabile. L'algoritmo ha influenzato successivi codici quali l'MD5 e l'SHA.
- L'algoritmo non è sicuro ed il suo uso è pertanto sconsigliato in applicazioni in cui si richiede un elevato grado di sicurezza.

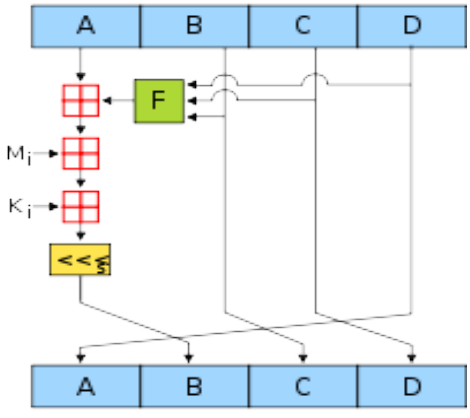
UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

MD4

L'MD4 consiste di 48 operazioni, raggruppate in tre blocchi da 16 operazioni ciascuno.

F ***è una funzione non lineare; una funzione F è usata in ogni passaggio.***
M_i ***indica un blocco da 32 bit del messaggio in input,***
K_i ***indica una costante a 32 bit, differente per ogni operazione.***

denota l'addizione modulo 2^{32}



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SHA

- La sigla SHA sta per **Secure Hash Algorithm** e indica una famiglia di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) degli USA.
- Come ogni algoritmo di hash, **l'SHA produce un *message digest* di lunghezza fissa partendo da un messaggio di lunghezza variabile.**
- La sicurezza di un algoritmo di hash risiede nel fatto che la funzione non sia reversibile (non sia cioè possibile risalire al messaggio originale conoscendo solo questo dato) e che 2 messaggi diversi non devono mai fornire lo stesso *digest*.
- Gli algoritmi della famiglia sono denominati **SHA-1**, **SHA-224**, **SHA-256**, **SHA-384** e **SHA-512**: le ultime 4 varianti sono spesso indicate genericamente come **SHA-2**, per distinguerle dal primo. Quest'ultimo produce un *digest* del messaggio di soli 160 bit,

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SSL (TLS)

- Netscape nel 1994 ha inventato il protocollo ***Secure Socket Layer*** **(SSL)** per promuovere l'applicazione e l'evoluzione del commercio elettronico sulla rete internet.
- *SSL* fornisce un canale crittografato del tipo *end-to-end* tra il client ed il server. Prima che venisse scoperto questo tipo di protocollo le transazioni avvenivano in chiaro e potevano tranquillamente essere intercettate (sniffate).
- La standardizzazione del protocollo *SSL* ha preso il nome di ***Transport Layer Security*** **(TLS)** e viene documentata nella RFC 2246
- **Il protocollo *TLS* non è legato al protocollo *HTTP* e può essere utilizzato con altre applicazioni, come ad esempio la posta elettronica**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SSL (TLS)

Il funzionamento del protocollo **TLS** può essere suddiviso in tre fasi principali:

* **Negoziazione** fra le parti dell'algoritmo da utilizzare
* **Scambio delle chiavi** e autenticazione
* **Cifratura simmetrica** e autenticazione dei messaggi

All'interno di una sessione tipicamente vengono utilizzati i seguenti protocolli:

* **Per lo scambio di chiavi**: RSA, Diffie-Hellman, …
* **Per l'autenticazione**: RSA, DSA, ….
* **Cifratura simmetrica**: RC4, Triple DES, AES, …..
* **Per le funzioni crittografiche di hash**: in **TLS** sono utilizzati *HMAC-MD5 o HMAC-SHA* mentre in **SSL** *MD5 e SHA*.