Crittografia e sicurezza delle reti

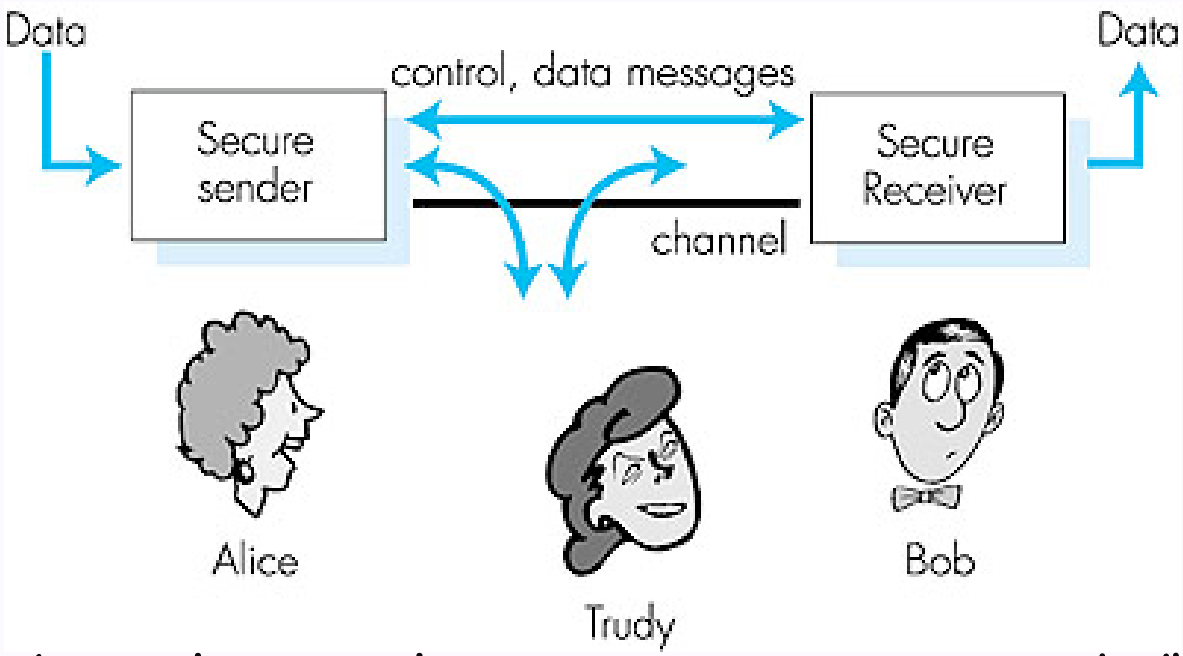
Alberto Marchetti Spaccamela

Crittografia e sicurezza

Sicurezza e crittografia sono due concetti diversi

- Crittografia tratta il problema della segretezza delle informazioni
- La sicurezza utilizza strumenti crittografici per realizzare applicazioni robuste in presenza di attacchi condotti da avversari
- I sistemi di sicurezza usati in pratica devono risolvere problemi di frodi:
    - Modifiche di messaggi
    - Autenticazione utenti

Amici e nemici: Alice, Bob,



- Bob e Alice vogliono comunicare in modo "sicuro"
- Trudy ("intruso/intrusa") può intercettare, rimuovere o aggiungere messaggi
- Trudy vuole modificare, conoscere o impedire la comunicazione

Requisiti di Sicurezza

Il sistema deve soddisfare i seguenti requisiti di sicurezza

- Disponibilita'
- Riservatezza
- Integrità
- Autenticazione
- Non ripudiazione

Requisiti di disponibilitá

Rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.

Nei sistemi informatici, i requisiti di disponibilità includono prestazioni e robustezza.

Requisiti di integrità

Impedire la **alterazione** diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali.

Se i dati vengono alterati e' necessario fornire strumenti per poterlo verificare facilmente.

Requisiti di riservatezza

Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere.

Se una informazione e' protetta, o se esiste una comunicazione in atto fra due utenti o processi in un certo contesto, non deve permettere di dedurre altre informazioni riservate.

Requisiti di autenticazione

Ciascun utente deve poter verificare l'autenticita' delle informazioni.

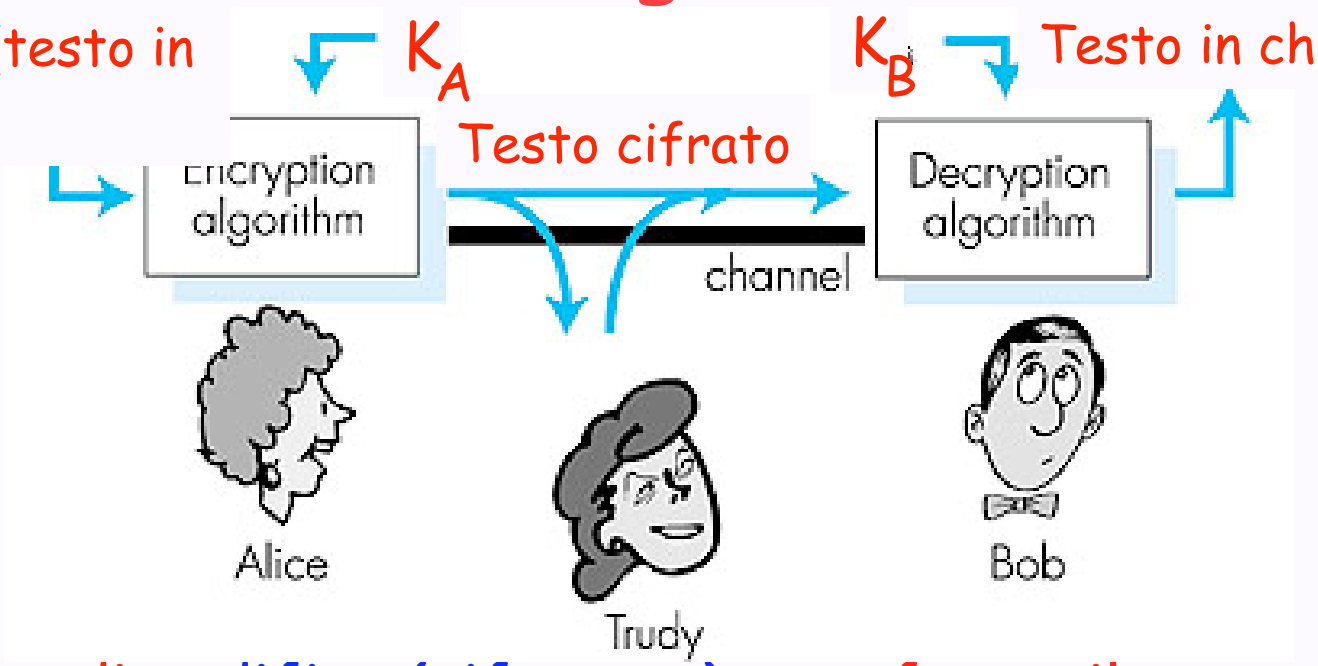
Si richiede di poter verificare se una informazione - non necessariamente riservata - e' stata manipolata.

Requisiti di non ripudiazione

Nessun utente deve poter ripudiare o negare messaggi da lui spediti o firmati.

Evitare che le informazioni e i messaggi siano negati dal firmatario in tempi successivi (es. firma di un contratto)

Crittografia



Algoritmo di codifica (cifratura): trasforma il testo in chiaro per renderlo incomprensibile

Algoritmo di decodifica (decifratura): trasforma il testo cifrato nel testo originale

la codifica e la decodifica sono funzione di una **chiave**

Codifica e decodifica crittografica

Algoritmo di codifica (cifratura): trasforma il testo in chiaro per renderlo incomprensibile

- la codifica è funzione di una **chiave (segreta)**

Algoritmo di decodifica (decifratura): trasforma il testo cifrato nel testo originale

- l' operazione di **decifratura** e' relativamente semplice nel caso in cui si conosca la chiave

Definizioni

- Messaggio m : stringa binaria (spesso considerato come numero intero senza segno)
- Chiave di codifica k_1 (si usa anche e)
- Chiave di decodifica k_2 (si usa anche d)
- Funzione (& algoritmo) di codifica: $E(m)$ (o $E_{k1}(m)$)
- Funzione (& algoritmo) di decodifica di testo cifrato c : $D(c)$ (o $E_{k2}(c)$)
- Per ogni messaggio m: $D_{k2}(E_{k1}(m)) = m$

Definizioni

Se non si conosce la chiave

- risulta molto laborioso ottenere informazioni - anche limitate - sul messaggio
- dedurre la chiave con cui è stato cifrato un documento anche conoscendo il testo in chiaro

Crittografia

- a chiave segreta $k_1 = k_2$
- a chiave pubblica k_1 e k_2 diversi

Minacce alla sicurezza

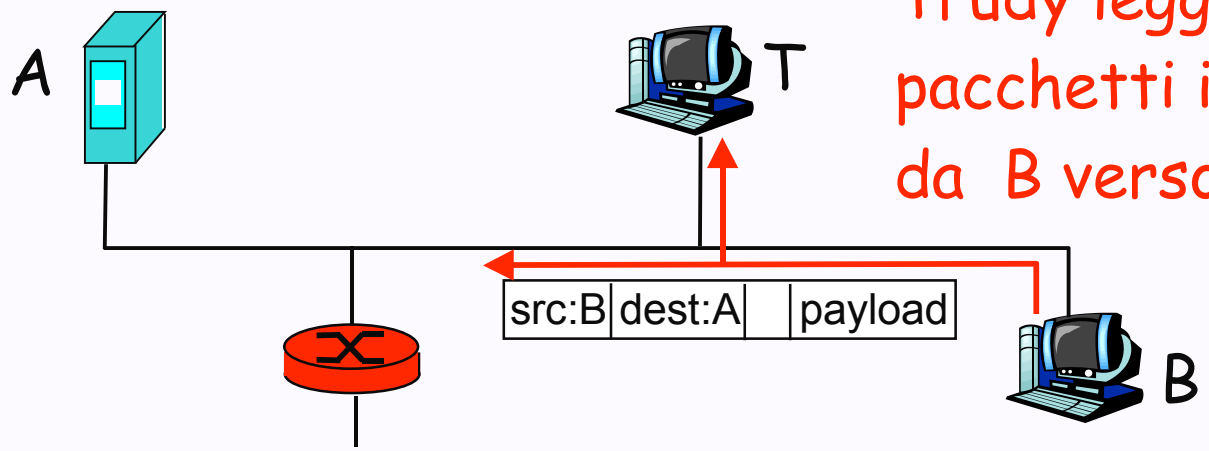
Tipi di intruso (o avversario)

- Intruso passivo: legge il messaggio senza alterarlo (es. password)
- Intruso attivo:
  - Può alterare il messaggio
  - Può inviare messaggi falsi spacciandosi presso il ricevente per il mittente autentico

Minacce alla sicurezza in Internet

Packet sniffing (to sniff = "odorare"):

- Evidente in mezzi condivisi
- Un adattatore di rete programmato ad hoc (NIC) legge tutti i pacchetti in transito
- Tutti i dati non cifrati (es.: password) possono essere letti

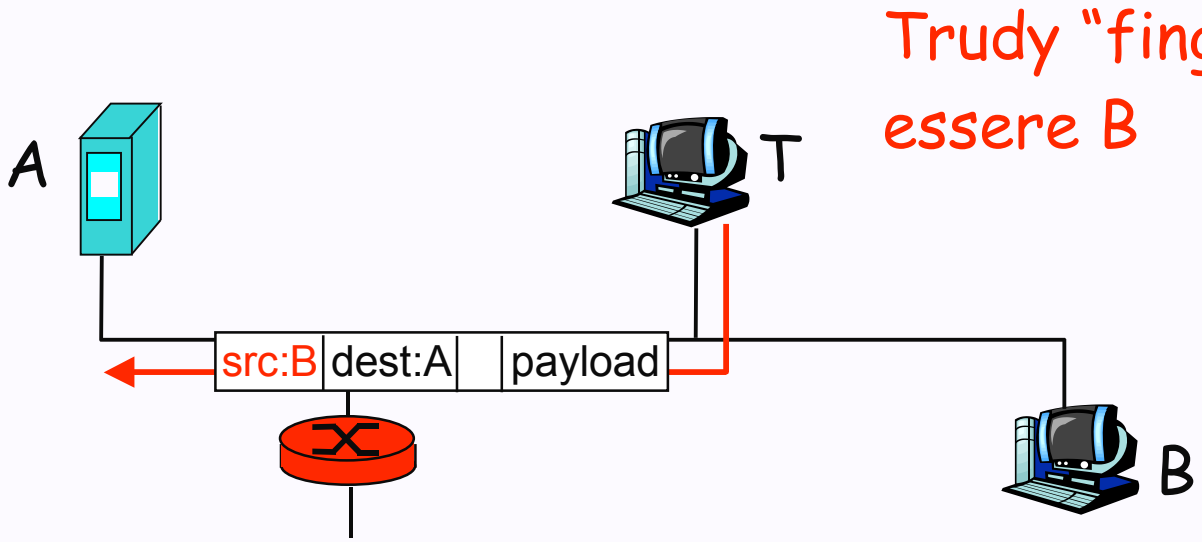


Trudy legge tutti i pacchetti inviati da B verso A

Minacce alla sicurezza

IP Spoofing:

- Un host genera pacchetti IP con indirizzi di sorgente falsi
- Il ricevente non è in grado di stabilire se l'origine dei pacchetti sia quella autentica



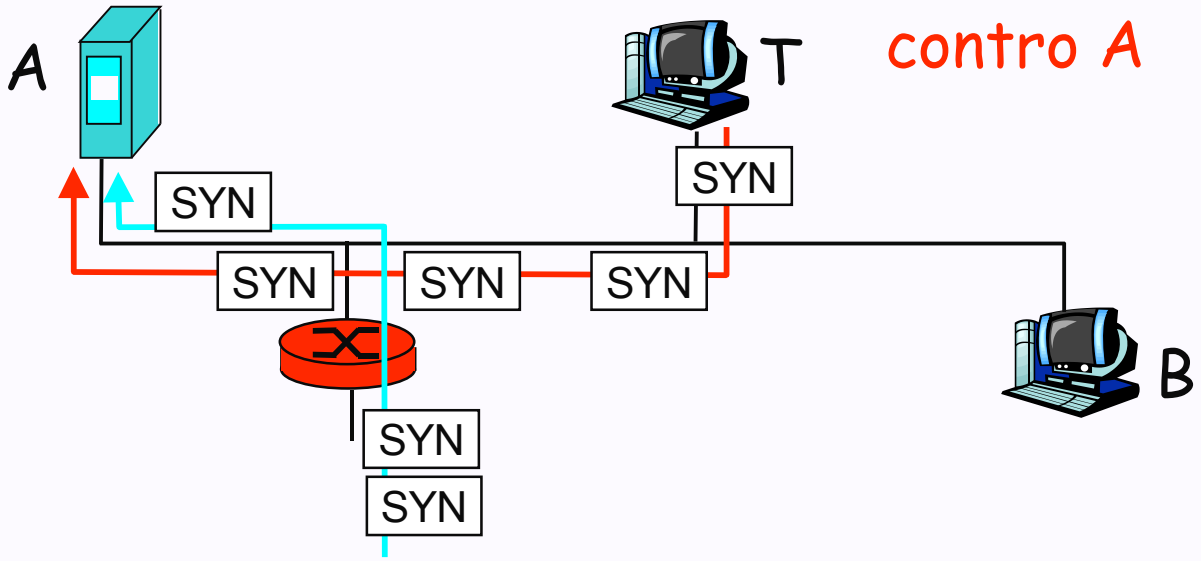
Trudy "finge" di essere B

Minacce alla sicurezza

Denial of service (DoS):

- Flusso di pacchetti "maligni" che sommerge il ricevente
- Distributed DoS (DDoS): attacco coordinato multiplo

Attacco SYN contro A



Crittografia: Modello Avversario

Trudy conosce

- lo spazio dei messaggi e ha qualche informazione parziale su m e $E_{k1}(m)$
- gli algoritmi *E,D*

Trudy non conosce le chiavi k_1, k_2

Trudy cerca di conoscere altre informazioni su m

Crittografia: Modello Avversario

Obiettivi di Trudy:

- Trudy può ottenere *m* ***NON Suffic.***
- Trudy può ottenere una particolare informazione su m ***NON Suffic.***
- Trudy può ottenere una qualunque significativa informazione su m ***Suffic.***

  Anche in modo probabilistico! (es. con prob. pari a 0.50000001 riesce a indovinare un dato bitdi un messaggio)

Sicurezza di un protocollo

La Crittoanalisi studia le modalità di attacco dei protocolli crittografici

Diversi tipi di attacco basati su

- ***Conoscenza*** *di testo cifrato*
- ***Conoscenza*** *testo in chiaro e corrispondente testo cifrato*
- ***Scelta*** *di testo in chiaro e conoscenza del corrispondente testo cifrato*
- ***Scelta*** *di testo crittato e conoscenza del corrispondente testo in chiaro*

Codici attaccabili

- Codice di Cesare (basato su traslazione)
- Codici basati su permutazioni dei caratteri

Conclusione : il numero delle chiavi deve essere grande ma questo non basta

Cifratura perfetta

- Spazio dei messaggi – $\{0,1\}^n$
- Dato un testo cifrato C la probabilità che $D_{k2}(C)=P$ per ogni P sia uguale alla probabilità a priori che P sia il testo in chiaro.

  In altre parole:

  $Pr[\text{plaintext}=P \mid C] = Pr[\text{plaintext}=P]$
- Le probabilità sono definite sullo spazio delle chiavi e sullo spazio dei possibili testi in chiaro

Esempio – One Time Pad

- Spazio del Testo in chiaro - $\{0,1\}^n$
- Spazio della Chiave - $\{0,1\}^n$
- Lo schema è simmetrico, la chiave k è scelta a caso
- $E_k(P) = C = P \oplus K$
- $D_k(C) = C \oplus K = P$

I codici perfetti sono possibili?

Teorema: one time pad è un metodo di cifratura perfetto. (Dimostr.: esercizio)

Problema: dimensione dello spazio delle chiavi.

Teorema (Shannon): Un metodo di cifratura A non può essere perfetto se lo spazio delle chiavi è più piccolo dello spazio dei possibili messaggi (Dimostr.: esercizio)

Sicurezza in pratica

La sicurezza in crittografia è valutata in base alle risorse di tempo e di calcolo necessarie per dedurre informazioni

- *ogni protocollo crittografico puo' essere "rotto" con sufficienti risorse di tempo e calcolo*
- *se un algoritmo puo' essere "rotto" usando per 30 anni un sistema di calcolo del valore di 10 miliardi di Euro allora puo' essere sicuro.*

La sicurezza di un algoritmo dipende dal campo di applicazione.

Sicurezza in pratica

La sicurezza di un protocollo dipende anche dal numero di possibili chiavi:

se ci sono molte possibili chiavi allora ci vuole molto tempo (o molta fortuna) per trovare la chiave segreta:

- *20 bit (circa 1 milione di diverse chiavi) allora non e' affatto sicuro*
- *56 bit (circa 66 milioni di miliardi diverse chiavi) andava bene dieci anni fa ma oggi e' "poco" sicuro*
- *512 bit (piu' di 40000000….0000000000 - 4 seguito da 153 zeri - diverse chiavi) oggi e' sicuro; domani?*

Sicurezza in pratica

Grandi Numeri

- Colonne Enalotto 622.614.630=1.15 2^{29}
- Secondi dalla creazione del sistema solare 1.38 2^{57}
- Cicli in un secolo di una macchina a 3 GHz 4.05 2^{61}
- Cicli in un secolo di 1000000 di macchine a 2 GHz 4.05 2^{81}
- Numeri primi di 249 bit 1.8 2^{244}
- Elettroni nell'universo 1.8 2^{258}

Sicurezza in pratica

Avversario: Potere computazionale

- Tempo
- Hardware
- Memoria

Teoria: avversario dispone di tempo e spazio polinomiali nella dimensione del problema

- In pratica – 2^{64} è ammissibile, 2^{80} no

Sicurezza dei protocolli

Tipi di Attacco

- Ascolto (Eavesdropping)
- Testo codificato e testo in chiaro (Known plaintext)
- Scelta testo in chiaro (Chosen plaintext)
- Scelta testo cifrato (Chosen ciphertext)
- Testi di attacco scelti in dipendenza di risultati parziali
- Accesso fisico
- Modifiche di messaggi

Programma schematico

- Crittografia a chiave segreta e a chiave pubblica
- Integrità dei dati e firma digitale
- Autenticazione utenti
- Teoria dei numeri, Casualità
- Standard (SSL,IPSEC, Kerberos,X.509)
- Firewall
- Aspetti seminariali (??): aspetti legali, applicazioni e-commerce, ecc.

Bibliografia

Libro di testo:

- *Network Security: private communication in a public world*, 2 ed. Kaufman,Perlman,Speciner, Prentice Hall

Libri raccomandati o utili e riferimenti:

- *Handbook of Applied Cryptography*
  Menezes, Van Oorschot, Vanstone, CRC Press
  scaricabile http://www.cacr.math.uwaterloo.ca/hac
- *Articoli, rapporti tecnici, RFC*
- *Cryptography and network security*, William Stallings, 3 ed., Prentice Hall (2 ed. in italiano: Crittografia e sicurezza delle reti)

Altri corsi sul Web

I siti di questi docenti contengono molto materiale di interesse

- Ron Rivest, MIT
- Dan Boneh, Stanford.
- Phil Rogaway, Davis.
- Doug Stinson, Waterloo.
- Amos Fiat, Tel Aviv

Esami e ricevimento

- Esame scritto (80%), progetto (20%).
- Progetti in gruppi di due o tre

- Ricevimento: Giovedì ore 11.30, via Salaria II p. oppure martedì dopo lezione
- E-mail: marchetti@dis.uniroma1.it