La sicurezza informatica: aspetti multidisciplinari

Appuntamenti con la cultura

Università del Molise
28 aprile 2004

Vincenzo Acciaro

Viviamo nella società dell'informazione

- l'informazione costituisce un bene strategico per ogni organizzazione
- un bene prezioso che come tale deve essere custodito e protetto!

Dato di fatto

Le transazioni di moneta in forma elettronica costituiscono la prassi per istituti di credito, piccole, medie e grandi aziende

L’e-commerce stenta a decollare

- Causa principale:

  sfiducia dei possibili utenti

- Frodi e clonazioni:

  uno dei principali ostacoli alla diffusione dei pagamenti con le carte di credito

Rimedi?

- il sistema bancario italiano sta promovendo il passaggio a carte di credito dotate di microprocessore, basate su una tecnologia sicura

- L'adeguamento del sistema richiede notevoli sforzi in termini di tempo e risorse economiche da parte di tutti gli operatori del settore

L’appuntamento di oggi

affrontare insieme alcuni problemi legati alla custodia ed allo scambio della informazione

I relatori

Vincenzo Acciaro

Prof. Francesco Pappalardi
Università di Roma Tre

Il crittosistema RSA:
un sistema che ha 25 anni, ma che da 2000 anni proviamo ad attaccare

Vincenzo Acciaro

Prof. Francesco Di Ciommo
Università di Roma Tor Vergata

Sicurezza nelle comunicazioni elettroniche e responsabilità on-line: ovvero, Internet come luogo di *non diritto*

Vincenzo Acciaro

Prof. Mario Massimo Petrone
Università degli Studi del Molise

Il futuro dell'e-security:
quali garanzie?

Conclusioni

Prof.ssa Stefania Giova
Università degli Studi del Molise

Nuovi target all'orizzonte

AL Digital, azienda britannica specializzata in questioni di sicurezza, lancia un nuovo allarme riguardo la scarsa sicurezza garantita da molti cellulari Bluetooth

Bluesnarfing

In una dimostrazione per le vie di Londra, gli esperti di AL Digital hanno ottenuto in pochi minuti nominativi, appuntamenti e fotografie da ignari passanti dotati di cellulare Bluetooth tramite un normalissimo computer portatile ed un apposito programma

Alcuni dati

- Negli USA nel 2003 i modelli di auto che offrono l'istallazione di un kit Bluetooth veicolare sono aumentati del 40%

- nel 2008 nel mondo ci sarà un parco circolante di 22 miliorni di auto dotate di connessione wireless

Prof. Mario Massimo Petrone
Università degli Studi del Molise

Il futuro dell'e-security:
quali garanzie?

Vincenzo Acciaro

L’insicurezza delle tecnologie ICT è spesso riconducibile al software

- Gran parte dei problemi di sicurezza sono determinati da:
  - errori presenti (bugs)
  - cattivo uso

- Occorre capire come un errore presente in un programma possa essere utilizzato per compromettere la sicurezza del sistema

Prof. Francesco Pappalardi
Università di Roma Tre

Il crittosistema RSA:
un sistema che ha 25 anni, ma che da 2000 anni proviamo ad attaccare

Vincenzo Acciaro

Crittografia

definizioni

Vincenzo Acciaro

Gli elementi di un crittosistema

- un insieme M di messaggi in chiaro
- un insieme C di messaggi cifrati
- un insieme K di chiavi
- per ogni chiave k una funzione di codifica $E_k : M \rightarrow C$
- per ogni chiave k una funzione di decodifica $D_k : C \rightarrow M$

Le funzioni di codifica e decodifica sono algoritmi!

Possiamo immaginare E_k
(rispettivamente D_k)
come un singolo algoritmo, parametrico
nella chiave k

Relazione Fondamentale

per ogni chiave *k* e
per ogni messaggio in chiaro *m*:

$$D_k\ (\ E_k\ (m)) = m$$

Prerequisiti

- gli algoritmi *E* e *D* devono essere efficienti
- la sicurezza del sistema deve dipendere dalla segretezza della chiave *k*, e non dalla segretezza degli algoritmi *E* e *D* di codifica e decodifica.

Infatti tali algoritmi sono noti
– almeno –
a chi abbia progettato il sistema!

Requisiti minimi di sicurezza

Un sistema crittografico dovrebbe essere sicuro rispetto ai seguenti tre livelli di attacco:

- attacco al codice cifrato. Quando il nemico conosce il solo messaggio codificato
- attacco tramite coppie note (*messaggio in chiaro, messaggio cifrato)*
- attacco tramite *conoscenza della funzione di codifica*. Quando il nemico può ottenere il testo cifrato per il testo in chiaro da lui scelto

Obiettivo

Scopo di un sistema crittografico e' l'ottenimento di

- segretezza e/o
- autenticità

Segretezza

- Dovrebbe essere impossibile per il nemico inferire il testo in chiaro dal testo cifrato
- Noti il messaggio in chiaro ed il messaggio cifrato, dovrebbe essere impossibile inferire la funzione di decodifica

Autenticità

- Dovrebbe essere impossibile al nemico trovare un messaggio cifrato corrispondente al messaggio in chiaro da lui scelto.
- Noti il messaggio in chiaro ed il messaggio cifrato, dovrebbe essere impossibile al nemico ricavare la funzione di codifica.

Si noti la simmetria tra segretezza ed autenticità!

Segretezza

- Non importa se E_k e' nota

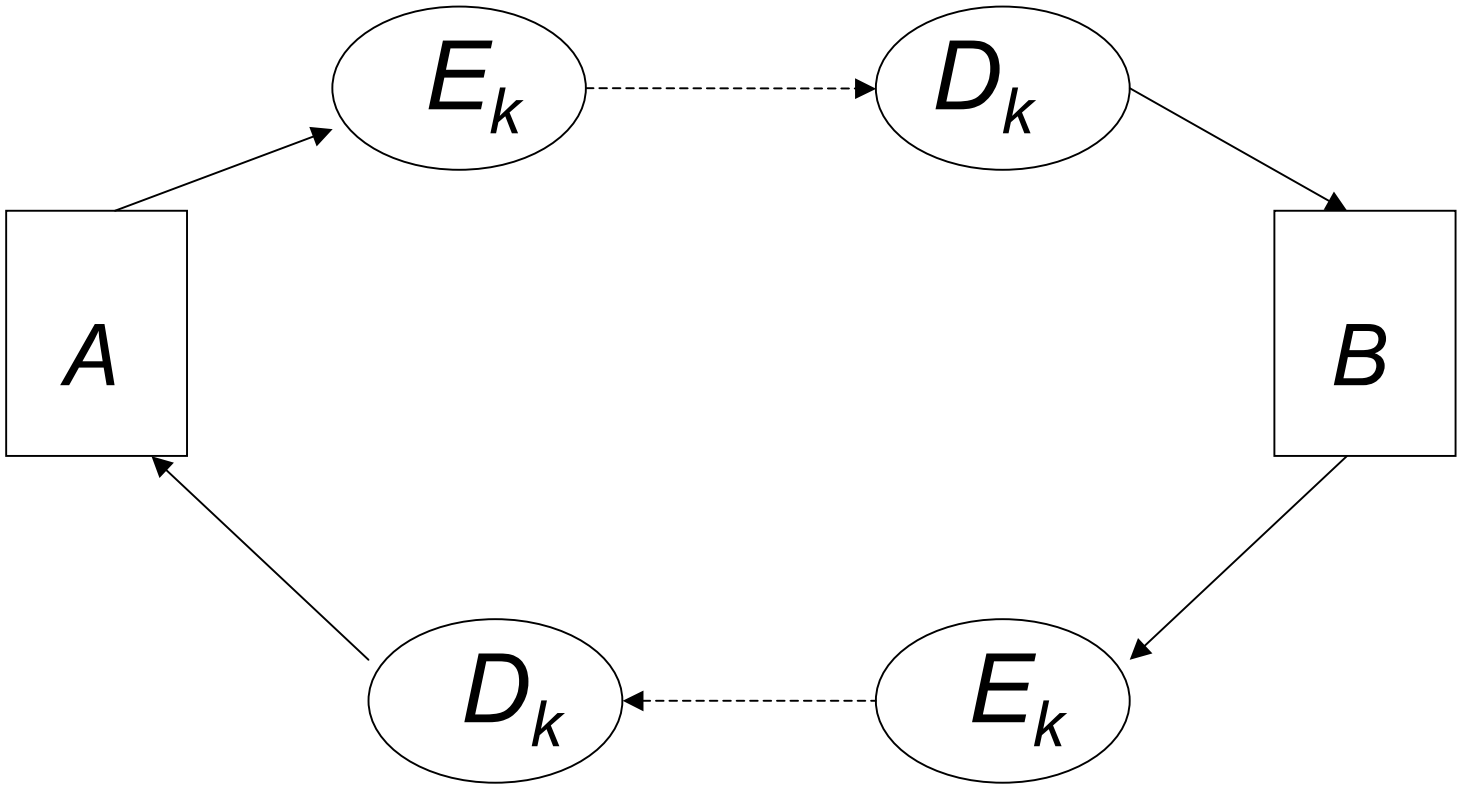
Autenticità

- Non importa se D_k e' nota

Per molti anni segretezza = autenticità

E_k e D_k erano le stesse per le due parti comunicanti

Sistema convenzionale



Problema

Se n parti vogliono comunicare occorre distribuire

$n(n-1)/2$ chiavi

una per ciascuna coppia di utenti del sistema!

Sistemi a chiave pubblica

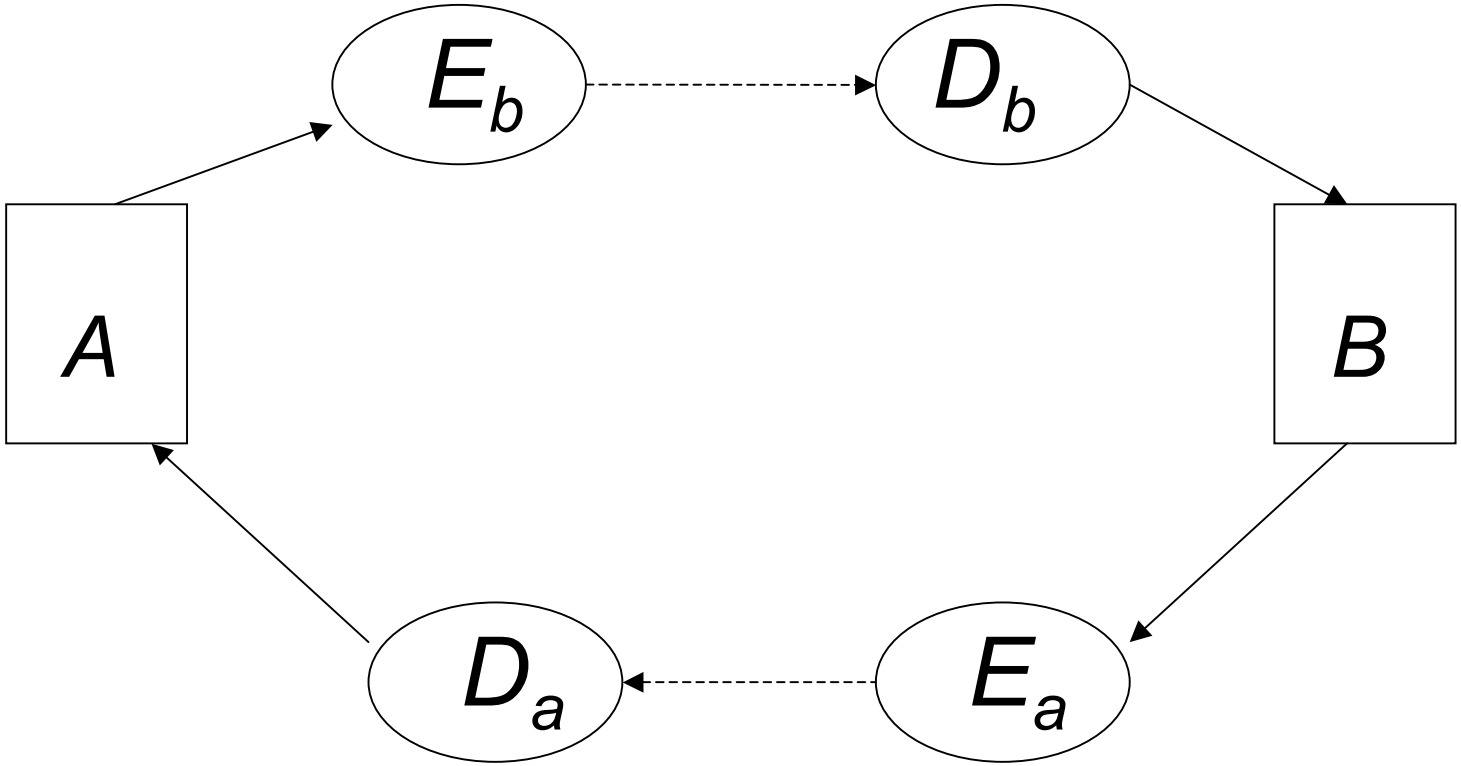
- Sono asimmetrici, ovvero gli algoritmi di codifica e decodifica utilizzati dalle due parti sono diversi.
- E’ possibile ottenere segretezza, autenticità o entrambe.

Come funzionano

Se *A* e' un utente del sistema:

- Sceglie una chiave *a*
- Ottiene E_a e D_a
- Rende pubblica E_a

Obiettivo segretezza



Ricapitolando

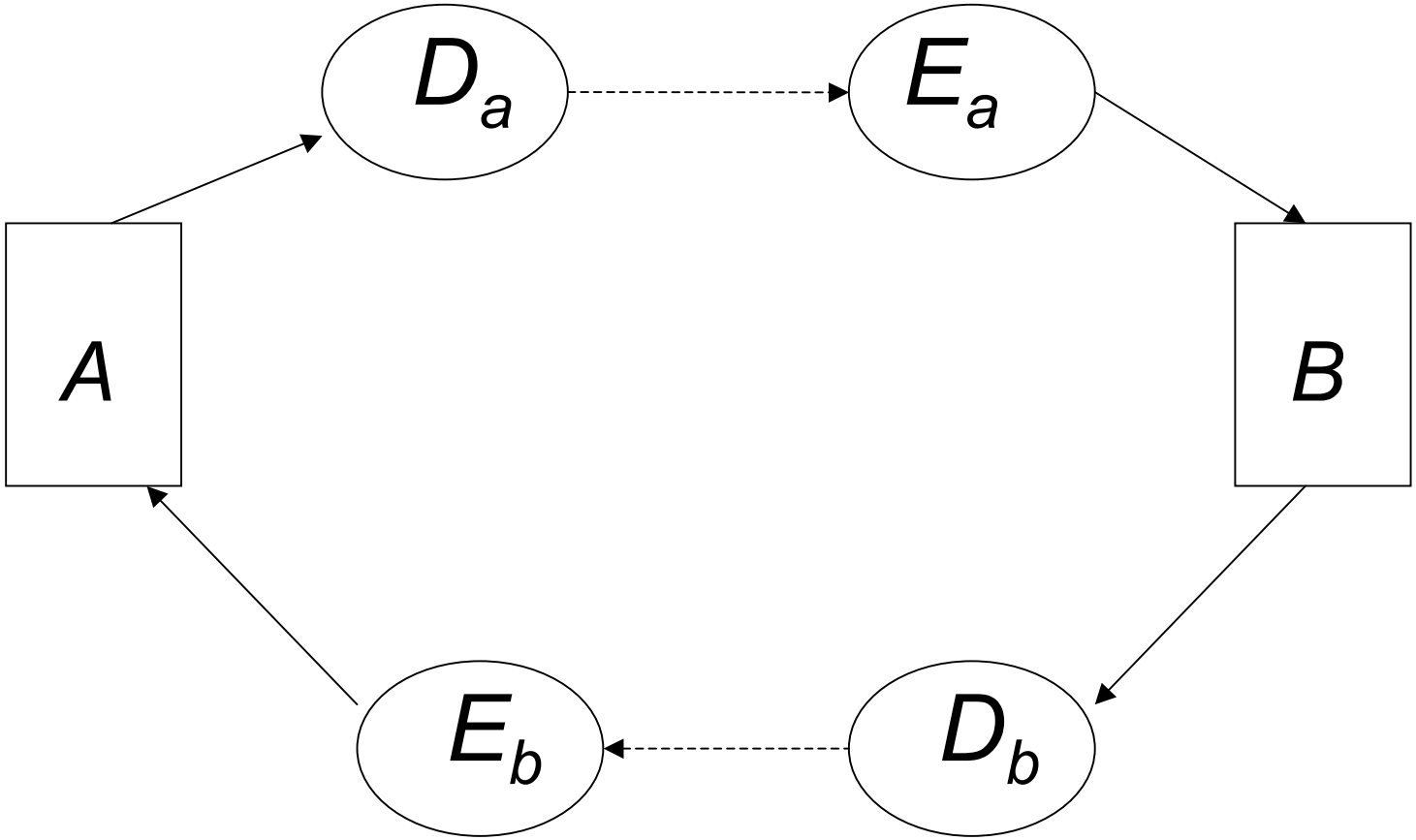
- *A* usa E_b per codificare i propri messaggi
- *B* usa E_a

Obiettivo autenticità

Prerequisito fondamentale:

per ogni chiave k e
per ogni messaggio in chiaro m:

$$E_k\ (\ D_k\ (m)) = m$$



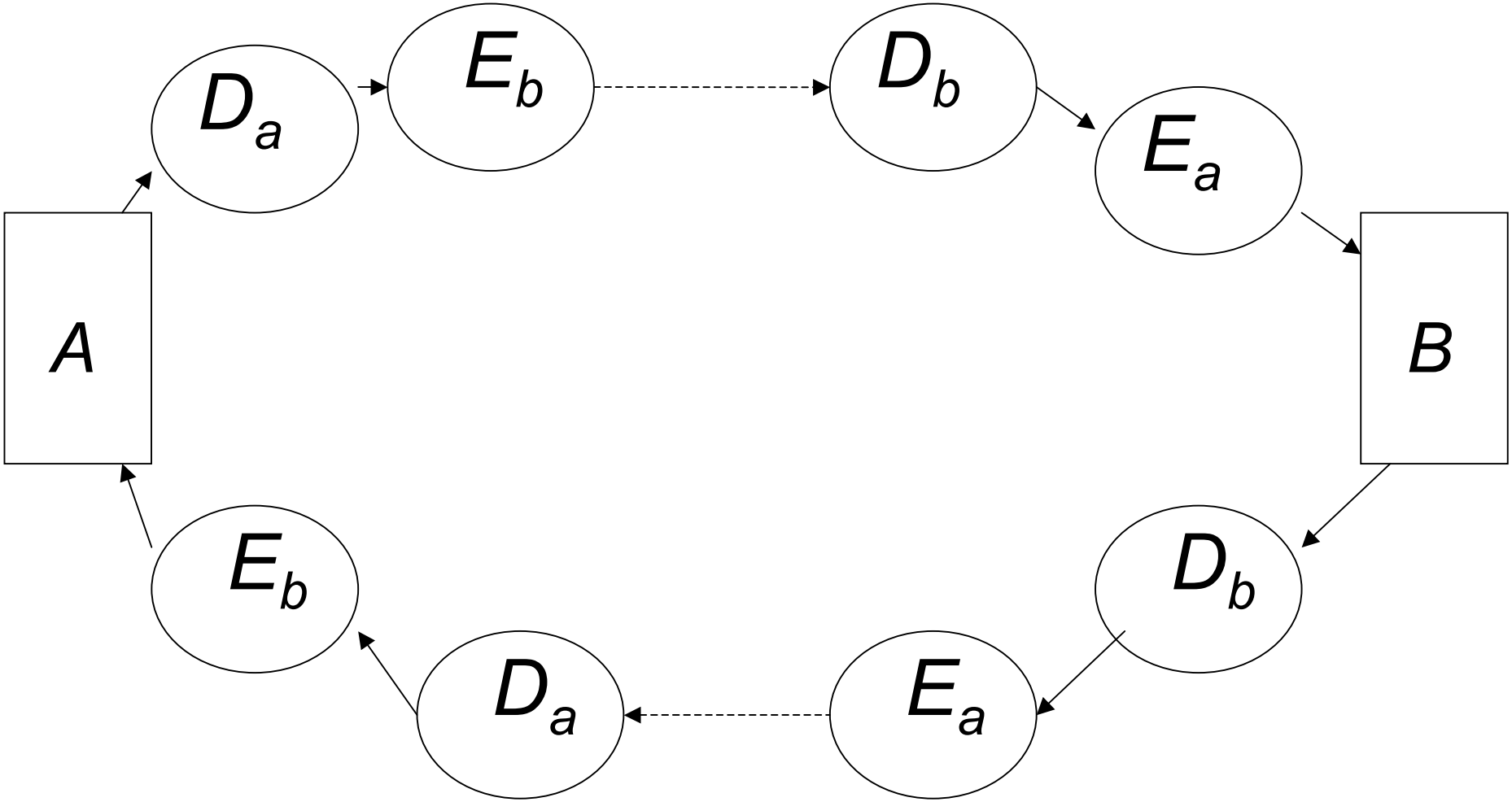
Vincenzo Acciaro

Obiettivo segretezza ed autenticità

Prerequisito fondamentale:

per ogni chiave k e
per ogni messaggio in chiaro m:

$$E_k\ (\ D_k\ (m)) = m$$



Vincenzo Acciaro

Firma elettronica

(collegata al problema autenticità)

Se *A* invia un messaggio a *B*, la firma di *A* deve soddisfare i seguenti requisiti:

- *B* deve riconoscere che si tratta della firma di *A*
- Nessuno, *B* incluso, deve poter imitare la firma di *A*
- Se *A* nega che la firma apposta su un documento possa essere la sua, una terza parte deve essere in grado di risolvere la disputa

Per ottenere gli obiettivi proposti, le funzioni di codifica e decodifica devono essere difficilmente invertibili

Distinguiamo due tipi di funzioni difficilmente invertibili:

- One way functions
- One way trap door functions

One way functions

Una funzione $f : X \rightarrow Y$ e' one way se:

- per ogni x in X e' semplice calcolare $f(x)$ (semplice = calcolabile in tempo polinomiale)
- per ogni y in Y e' difficile calcolare un x tale che $f(x)=y$

One way trap door functions

Una funzione $f : X \rightarrow Y$ e' one way trap door se:

- per ogni x in X e' semplice calcolare $f(x)$ (semplice = calcolabile in tempo polinomiale)
- per ogni y in Y e' semplice calcolare un x tale che $f(x)=y$
- la conoscenza di un algoritmo per calcolare la funzione f non implica la conoscenza di un algoritmo per calcolare f^{-1}

Quindi…

e’ possibile rendere noto un algoritmo per calcolare *f*

senza permettere - *ad alcuno* –
di ricavare un algoritmo per calcolare f^{-1}

Problema

Esistono tali funzioni *one way trap door* ?

Esempio canonico

$X = \{ (p,q) \mid S \leq pq \leq T,\ p,q \text{ primi} \}$

$S, T > 10^{100}$

$f: X \longrightarrow N$ definita come $f(p,q) = pq$

f e' una funzione del tipo cercato?

In centinaia di anni di ricerca
non e' stato trovato
un algoritmo efficiente
di fattorizzazione!