



Crittografia Moderna

A.A. 2021-22



Principi di base

Storicamente

- ▶ Schemi di cifratura progettati ad hoc
- ▶ Valutati basandosi sulla chiarezza, sull'ingegnosità del progetto e sulla difficoltà percepita di rottura
- ▶ Nessuna nozione condivisa di cosa significhi per uno schema essere “sicuro”
- ▶ Nessun modo per “produrre evidenza di ciò”



Crittografia moderna: pilastri

- ▶ Spostamento verso una “scienza”
- ▶ **Definizioni** rigorose di cosa significa “sicuro”
- ▶ **Assunzioni** circa la complessità di certi problemi matematici
- ▶ **Dimostrazioni/prove** che una costruzione è sicura



Principio 1: definizioni rigorose

- ▶ Essenziali per la progettazione accurata, lo studio, la valutazione e l'uso di primitive crittografiche

“Se non è chiaro cosa si vuole ottenere, come è possibile stabilire quando (e se) il risultato è stato ottenuto?”



Principio 1: definizioni rigorose

- ▶ Permettono di valutare ciò che è stato costruito
- ▶ Permettono di comparare schemi



Le definizioni non sono facili

- ▶ Definizioni: due componenti
 - ▶ garanzie di sicurezza (**security goal**): da quali tipi di azioni di un attaccante lo schema protegge
 - ▶ un modello delle minacce (**threat model**): che potere ha l'attaccante
- ▶ Cosa dovrebbe garantire uno schema di cifratura sicuro?
 - ▶ Dovrebbe essere impossibile per un attaccante recuperare la chiave di cifratura? Lo schema
$$\mathbf{Enc}_K(m) = m$$
non fornisce alcuna informazione su K ma è chiaramente insicuro.



Le definizioni non sono facili

- ▶ Dovrebbe essere impossibile per un attaccante recuperare l'intero testo in chiaro dal cifrato?
 - ▶ Si consideri uno schema di cifratura che protegge un database di dati sensibili e rivela il 90% del suo contenuto.
 - ▶ Siamo soddisfatti che il 10% è invece protetto?
- ▶ Dovrebbe essere impossibile per un attaccante recuperare qualsiasi carattere del messaggio in chiaro dal cifrato?
 - ▶ Sembra buona, ma ancora insufficiente.
 - ▶ In un database di dati finanziari potrebbe rivelare se alcune transazioni hanno valori maggiori o minori di una certa soglia
 - ▶ E poi, come formalizzare il “recupero di un carattere”?
 - ▶ Inoltre, provare ad indovinare è un attacco da considerare?



Le definizioni non sono facili

- ▶ La definizione giusta dovrebbe:
 - ▶ escludere il rilascio di informazioni utili da parte del cifrato
 - ▶ chiarire cosa debba essere considerato un attacco
- ▶ Ciò che richiediamo in fondo è che:

Indipendentemente da qualsiasi informazione l'attaccante possa già avere, un cifrato non dovrebbe rilasciare ***nessuna informazione aggiuntiva*** circa il sottostante messaggio in chiaro



Le definizioni non sono facili

- ▶ La definizione non cerca di definire quale tipo di informazione circa il messaggio in chiaro sia “significativa”
 - ▶ Nessuna informazione aggiuntiva deve essere rilasciata
 - ▶ Lo schema di cifratura è utile in tutte le potenziali applicazioni
- ▶ Cosa manca ancora? Una precisa formulazione di
 - ▶ conoscenza a-priori dell’attaccante sul messaggio in chiaro
 - ▶ cosa significa esattamente “rilasciare informazione”



Le definizioni non sono facili

- ▶ Cosa dovrebbe prevedere il modello delle minacce?
 - ▶ specificare il potere dell'avversario, le sue abilità
 - ▶ non porre alcuna restrizione alle strategie d'attacco, cioè non fare alcuna assunzione su come usa le proprie abilità
- ▶ Nel contesto della cifratura, i modelli sono 4
- ▶ Ciphertext only
 - ▶ l'attaccante può solo osservare cifrati c , prodotti usando una chiave k
- ▶ Known-plaintext:
 - ▶ l'attaccante acquisisce coppie (m, c) in qualche modo, prodotte usando una chiave k



Le definizioni non sono facili

- ▶ **Chosen-plaintext**

- ▶ l'attaccante acquisisce coppie (m,c) , scegliendo i valori di m , prodotte usando la chiave k

- ▶ **Chosen-ciphertext**

- ▶ l'attaccante acquisisce coppie (m,c) , scegliendo i valori di c , prodotte usando la chiave k



Nota: definizioni e cybersecurity

- ▶ Definizioni: due componenti
 - ▶ garanzie di sicurezza (**security goal**): da quali tipi di azioni di un attaccante lo schema protegge
 - ▶ un modello delle minacce (**threat model**): che potere ha l'attaccante

- ▶ La definizione dei security goal e del threat model (attack model) è un principio di base che si applica in generale nella cybersecurity, non soltanto in crittografia



Prove incondizionate

- ▶ La maggior parte delle costruzioni crittografiche moderne non possono essere provate sicure “incondizionatamente”
- ▶ richiederebbe la risoluzione di questioni della teoria della complessità che oggi non hanno ancora risposta (e.g., $P \neq NP$?)



Intuizione: dato uno schema di cifratura

- ▶ Sono $c_1, c_2, \dots, c_n$ le cifrature di $m_1, m_2, \dots, m_n$?
- ▶ Supponiamo che l'unico modo per rispondere alla domanda richieda la decifratura e di *poter provare* che la decifratura non può essere effettuata efficientemente (i.e., in tempo polinomiale) – a meno di possedere uno specifico 'hint' (i.e., la chiave).
- ▶ Se qualcuno ci fornisse la chiave usata per cifrare i messaggi, potremmo *verificare efficientemente* se è vero. Ma senza non potremmo.
- ▶ Ciò implicherebbe che la classe di complessità P , che contiene tutti i problemi che possono essere risolti efficientemente, è strettamente più piccola della classe NP , dei problemi le cui soluzioni possono essere verificate efficientemente
- ▶ Ovvero, ciò implicherebbe che $P \neq NP$ – che sarebbe una soluzione alla questione più importante nella teoria della complessità computazionale



Principio 2: assunzioni

- ▶ Le prove di sicurezza poggiano su **assunzioni** enunciate con *chiarezza e rigore matematico*



richiesto dalle prove ma
anche per i motivi che
seguono



Rigore matematico: permette

- ▶ **Validazione delle assunzioni**

- ▶ enunciati che si “congettura” risultino veri
- ▶ più sono studiati, maggiore è la confidenza che vi riponiamo
- ▶ formulazioni imprecise ostacolano lo studio

- ▶ **Comparazione di schemi**

- ▶ uno schema basato su un'assunzione più debole è preferibile ad uno schema basato su un'assunzione più forte
- ▶ se due assunzioni non sono confrontabili, dovrebbe preferirsi lo schema basato sull'assunzione studiata di più



Rigore matematico: permette

- ▶ **Comprensione delle assunzioni necessarie**
 - ▶ se uno schema è basato su “blocchi” e un blocco viene rotto, possiamo verificare se il problema è nel blocco o nell’assunzione



Assumere che uno schema è sicuro?

- ▶ Quando uno schema ha resistito con successo ad attacchi per molti anni, può essere ragionevole
- ▶ In generale questo approccio non è **mai** da preferirsi
- ▶ Ragioni più specifiche:
 - ▶ un'assunzione scrutinata per diversi anni è preferibile ad una nuova, magari ad hoc
 - ▶ assunzioni semplici sono preferibili
 - ▶ assunzioni di basso livello possono essere usate in svariate costruzioni
 - ▶ la progettazione può essere modulare, blocchi sostituibili



Principio 3: prove

- ▶ Definizioni ed assunzioni permettono di fornire prove che una costruzione soddisfa una data definizione sotto le assunzioni specificate
- ▶ Le prove sono assicurazioni del fatto che nessun attaccante, **relativamente** alla definizione ed alle assunzioni, avrà successo
- ▶ Meglio di un approccio “euristico” e non strutturato



non basato su principi chiari



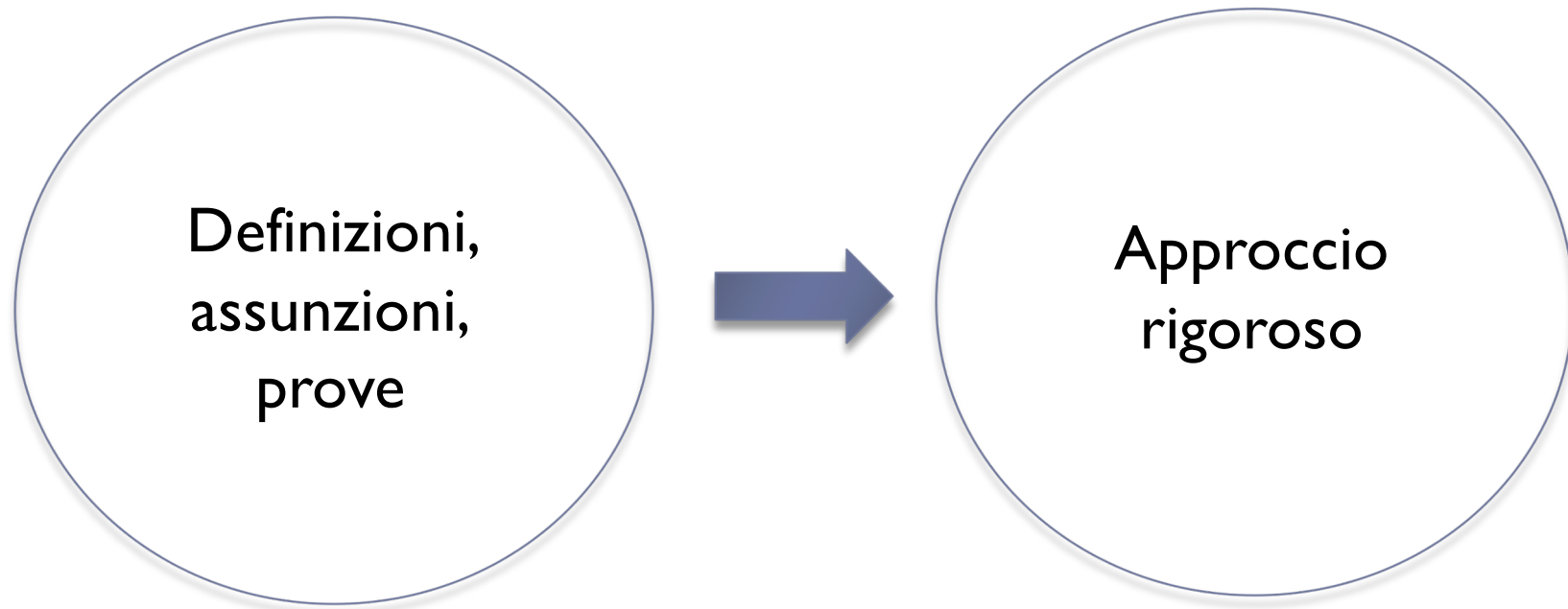
Terminologia: prove ...

- ▶ Useremo entrambi i termini “dimostrazione” e “prova”
- ▶ Una locuzione più precisa ma più lunga sarebbe **riduzione di sicurezza (security reduction)**
- ▶ gli enunciati che dimostreremo saranno del tipo: “se le **Assunzioni** $x, y \dots$ valgono, allora la **Costruzione** Π soddisfa la **Definizione** Z ”



specifica il
security goal ed
il threat model

Conclusioni: rigoroso vs ad hoc



... ma nel mondo reale soluzioni veloci sono spesso progettate seguendo un approccio ad hoc e valutazioni euristiche



Crittografia moderna: “scienza” e “arte”

- ▶ Molta della crittografia moderna poggia su solidi fondamenti matematici
- ▶ Ma è anche un’arte: occorre creatività nello sviluppo di
 - ▶ definizioni
 - ▶ assunzioni
 - ▶ prove
 - ▶ progettazione di primitive e protocolli crittografici
 - ▶ progettazione di strategie e tecniche di attacco



“Mondo reale” e “mondo delle prove”

- ▶ Che relazione c'è tra i due mondi?
- ▶ Occorre **non sopravvalutare** cosa una prova offre
 - ▶ le garanzie sono in relazione alla definizione considerata ed alle assunzioni utilizzate
 - ▶ sono un suggerimento all'avversario circa le “direzioni d'attacco” da **non** seguire ...
 - ▶ l'efficacia di una prova dipende in **maniera cruciale** da quanto il mondo reale sia ben modellato dalla definizione



Conclusione

L'approccio delle riduzioni di sicurezza non conclude sicuramente l'eterna battaglia tra attaccanti e difensori, ma sposta sicuramente l'ago della bilancia dalla parte dei difensori

