Codici Non Malleabili e Applicazioni

La De Cifris Incontra Roma

Prof. Daniele Venturi
Dipartimento di Informatica

SAPIENZA
UNIVERSITÀ DI ROMA

Roma, 4 Ottobre 2018

~~Codici Non Malleabili e~~ Applicazioni

La De Cifris Incontra Roma

Prof. Daniele Venturi
Dipartimento di Informatica

SAPIENZA
UNIVERSITÀ DI ROMA

Roma, 4 Ottobre 2018

Cosa la Crittografia può fare in caso di Sabotaggio

La De Cifris Incontra Roma

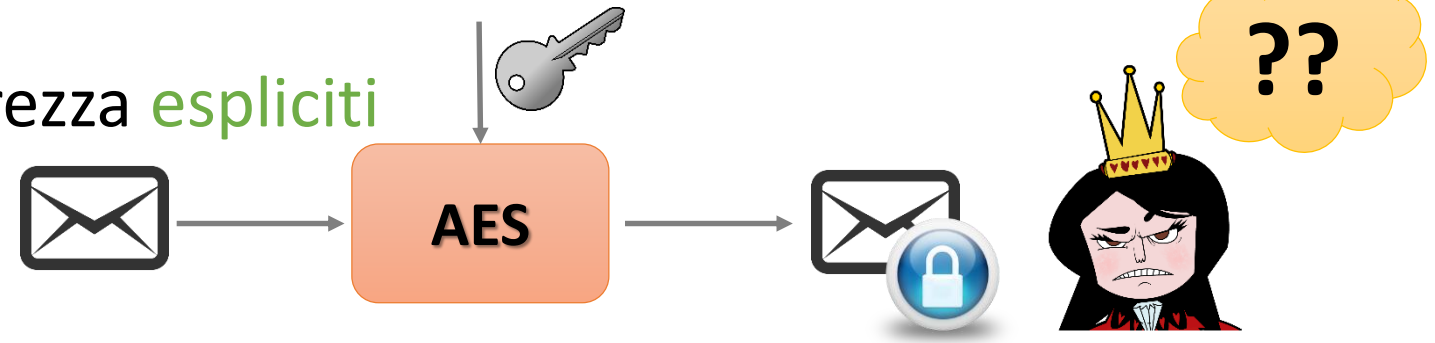
Prof. Daniele Venturi
Dipartimento di Informatica

SAPIENZA
UNIVERSITÀ DI ROMA

Roma, 4 Ottobre 2018

Crittografia Moderna: Sicurezza Dimostrabile

- Definire obiettivi di sicurezza espliciti
  - E.g., per la cifratura

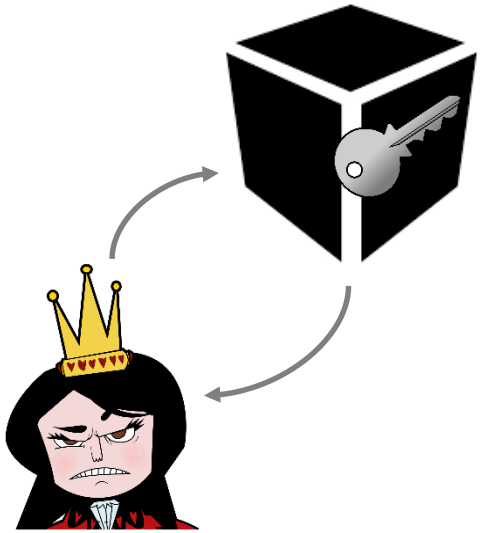


- Progettare un crittosistema (e.g., RSA)
- Dimostrare la sicurezza (per riduzione)

Se una certa assunzione è vera (e.g., fattorizzare è difficile) → *Il crittosistema è sicuro*

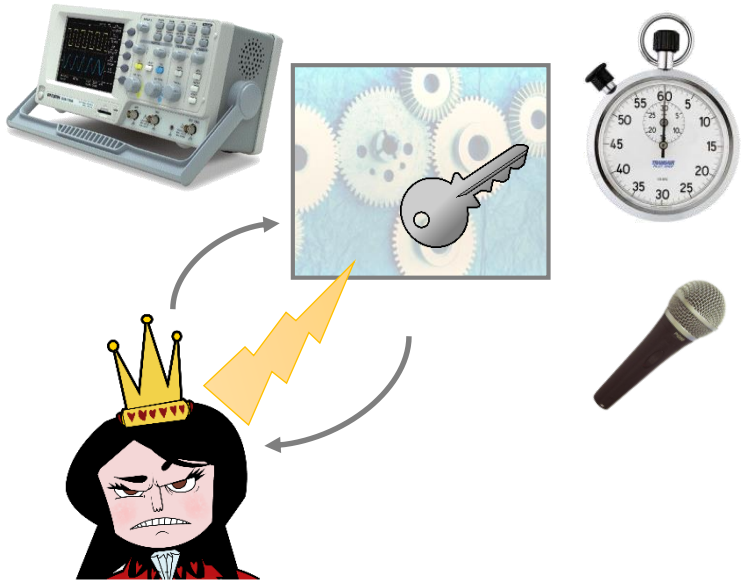
  - Situazione io vinco-tu vinci

Crittosistemi a Scatola Nera



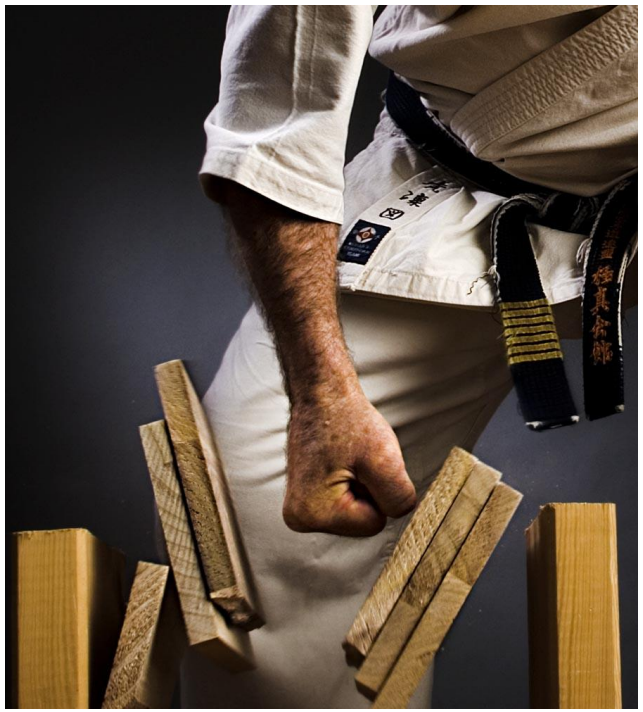
- L'attaccante può interagire con il sistema senza però poter guardare al suo interno
  - Possibilità di specificare input ed imparare gli output corrispondenti
  - Chiavi segrete completamente inaccessibili
  - L'implementazione di un crittosistema segue fedelmente la sua specifica

Attacchi Collaterali Passivi (a.k.a. Leakage)



- Attacchi passivi basati sulla misura di caratteristiche fisiche di un dispositivo crittografico a lavoro
  - Tempo necessario a compiere alcune operazioni
  - Potenza e campo magnetico emessi
  - Suono emesso dalla tastiera del computer o dalle componenti interne
- Tali attacchi sono pratici ed efficaci
  - In assenza di opportune contromisure, consentono di ricostruire l'intera chiave!!!

Manomissione (a.k.a. Tampering)



- Attacchi basati su fenomeni fisici
  - Calore e radiazione infra-rossa: Deviazioni di temperatura possono indurre inversione di bit
  - Attacchi ottici: La luce può essere usata per (re)settare singoli bit della memoria
  - Correnti di Eddy: Settare/reset/invertire singoli bit sfruttando campi magnetici
- Tali attacchi sono pratici ed efficaci
  - Ad esempio un singolo bit manomesso durante la computazione di una firma permette di fattorizzare facilmente il modulo RSA [BDL97]

Sabotaggio Furtivo di Algoritmi

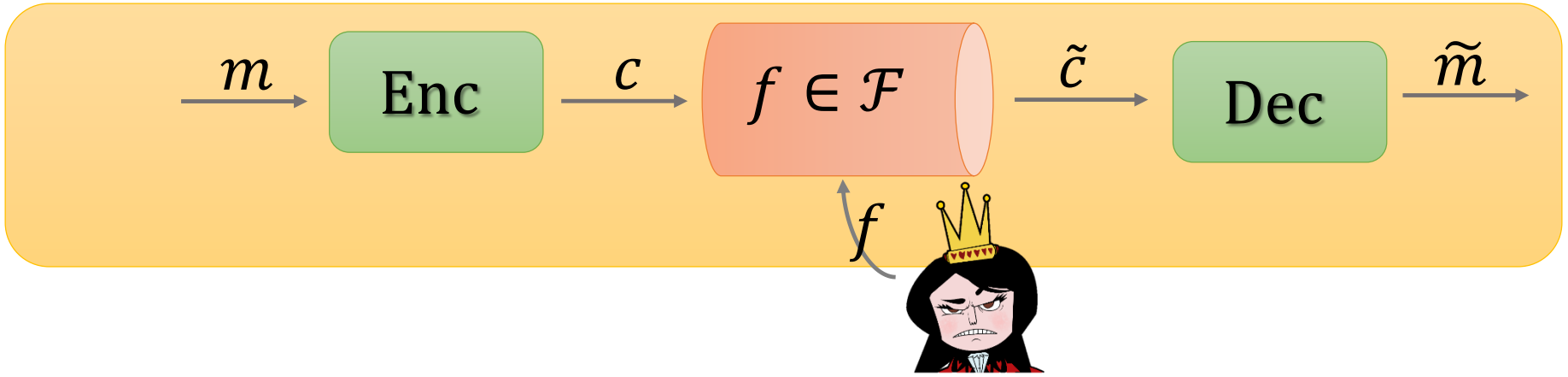
- Implementazioni malevole di crittosistemi il cui output è polarizzato in modo da poter violare la sicurezza data una certa informazione ausiliaria
  - Seppur gli output prodotti appaiano corretti dal punto di vista dell'utente
- Rivelazioni di Edward Snowden: L'NSA ha indebolito alcuni crittosistemi deliberatamente, allo scopo di sorvegliare le masse
  - NIST Dual EC PRG, basato su parametri pubblici P, Q
  - La conoscenza di $d = \mathrm{dlog}_Q P$ consente di distinguere l'output del PRG da random


20

Che Cosa Può Fare la Crittografia?

- Crittografia resistente agli attacchi fisici
  - Modellare avversari in grado di manomettere ed ottenere informazioni parziali sulla memoria di un crittosistema al lavoro
  - Costruire crittosistemi con sicurezza dimostrabile anche in presenza di attacchi fisici
- Crittografia Post-Snowden
  - Modellare crittosistemi la cui implementazione è stata manomessa furtivamente da un attaccante
  - Costruire crittosistemi con sicurezza dimostrabile anche nel caso in cui l'implementazione di una data specifica crittografica non è fidata

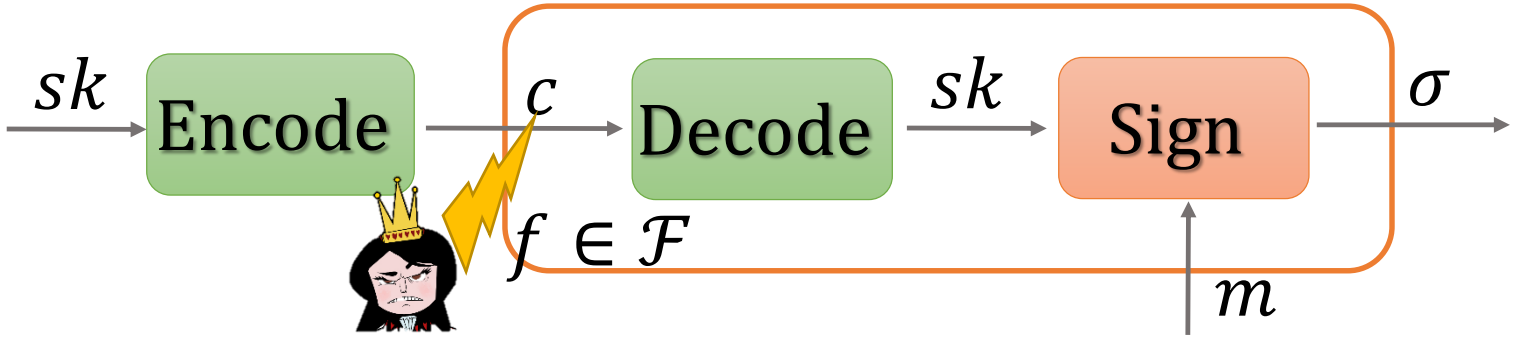
Codici Non Malleabili [DPW10]



- Intuizione: Ottenere una qualche garanzia utile sul messaggio decodificato $\tilde{m}$ per classi generali $\mathcal{F}$
  - Correzione di errore: $\tilde{m} = m$
  - Rilevazione di errore: $\tilde{m} = m$, oppure accorgersi che $\tilde{c}$ è invalida
  - Non Malleabilità: $\tilde{m} = m$, oppure $\tilde{m}$ indipendente da m
- Proprietà più debole, ma ottenibile per classi $\mathcal{F}$ più grandi

Crittosistemi a Prova di Manomissione

- Problema: Progettare una firma digitale sicura in presenza di manomissione della memoria (rispetto una certa classe di attacchi $\mathcal{F}$)
  - Attaccante può scegliere $f \in \mathcal{F}$ da applicare alla chiave segreta, ed osservare il relativo effetto sull'output
- Soluzione: Codificare la chiave con un codice non-malleabile (rispetto ad $\mathcal{F}$)

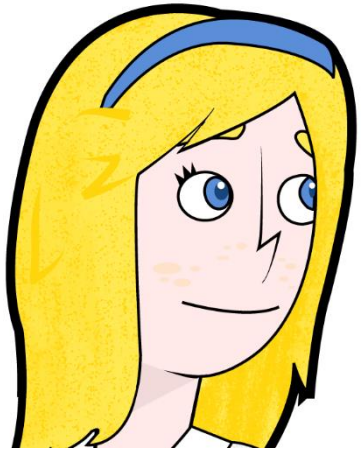


- $\mathbf{Decode}(f(\mathbf{Encode}(sk)))$ è (1) uguale ad sk, oppure (2) indipendente
  - Caso (1) ok per inforgiabilità, e caso (2) inutile per l'attaccante

Conclusioni e Prospettiva

- Codici non malleabili offrono soluzione generale rispetto al problema di manomissione della memoria
  - Ricerca focalizzata sulla costruzione di codici per famiglie $\mathcal{F}$ di interesse
  - Altre applicazioni: Crittografia non malleabile, ovvero progetto di crittosistemi resistenti contro attacchi attivi
- Sicurezza dimostrabile contro attacchi fisici e sabotaggio di algoritmi
  - Dovere morale della crittografia moderna [Rog15]: *"I call for a community-wide effort to develop more effective means to resist mass surveillance. I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work."*
  - Area di ricerca piena di sfide aperte

Grazie!



Per approfondire:

http://danieleventuri.altervista.org/