Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

LA CRITTOGRAFIA È MATEMATICA

Carlo Sanna

Gruppo di Crittografia e Teoria dei Numeri
Dipartimento di Scienze matematiche
Politecnico di Torino

- Cos'è la Crittografia?
- La Crittografia del Passato
- La Crittografia Moderna
- Dimostrare la Sicurezza

Cos'è la Crittografia?

La **Crittografia (Moderna)** è la scienza che si occupa di inventare e studiare dei metodi matematici per proteggere i segreti.

Cos'è la Crittografia?

La **Crittografia (Moderna)** è la scienza che si occupa di inventare e studiare dei metodi matematici per proteggere i segreti.

Non va confusa con la **Sicurezza Informatica**, che è la disciplina che si occupa della corretta implementazione dei suddetti metodi nei sistemi informatici e delle problematiche collegate.

La Crittografia del Passato (L'Alchimia)

La crittografia del passato (prima della fine della seconda guerra mondiale):

La Crittografia del Passato (L'Alchimia)

La crittografia del passato (prima della fine della seconda guerra mondiale):

Era principalmente per usi militari;

La Crittografia del Passato (L'Alchimia)

La crittografia del passato (prima della fine della seconda guerra mondiale):

Era principalmente per usi militari;

Si occupava solamente di cifratura e decifratura di testi.

I suoi principi fondanti erano i seguenti.

I suoi principi fondanti erano i seguenti.

Inventa un metodo ingegnoso per cifrare e decifrare.
(Cifrario di Cesare, cifrario di Vigenére, macchina Enigma...)

I suoi principi fondanti erano i seguenti.

Inventa un metodo ingegnoso per cifrare e decifrare.
(Cifrario di Cesare, cifrario di Vigenére, macchina Enigma...)

Tieni il metodo segreto al nemico.
(**Security through obscurity**)

I suoi principi fondanti erano i seguenti.

Inventa un metodo ingegnoso per cifrare e decifrare.
(Cifrario di Cesare, cifrario di Vigenére, macchina Enigma...)

Tieni il metodo segreto al nemico.
(**Security through obscurity**)

Spera che nessuno sia più intelligente di te.

Questi principi **non davano alcun garanzia di sicurezza** e i segreti venivano spesso decifrati dal nemico poiché:

Questi principi **non davano alcun garanzia di sicurezza** e i segreti venivano spesso decifrati dal nemico poiché:

Il nemico imparava il metodo segreto
(spionaggio, corruzione, errore umano, ...); e/o

Questi principi **non davano alcun garanzia di sicurezza** e i segreti venivano spesso decifrati dal nemico poiché:

Il nemico imparava il metodo segreto
(spionaggio, corruzione, errore umano, ...); e/o

Qualcuno più intelligente inventava un attacco allo schema
(analisi delle frequenze, attacco con testo in chiaro noto,
attacco con testo cifrato scelto, crittografia differenziale, ...)

Esempio: La Cifratura Monoalfabetica

Nella **cifratura monoalfabetica** un testo in chiaro viene cifrato sostituendo a ogni lettera un'altra lettera, in accordo con una regola segreta, detta **chiave**, che può essere invertita.

La conoscenza della chiave permette quindi di decifrare il messaggio.

Esempio: La Cifratura Monoalfabetica

Nella **cifratura monoalfabetica** un testo in chiaro viene cifrato sostituendo a ogni lettera un'altra lettera, in accordo con una regola segreta, detta **chiave**, che può essere invertita.

La conoscenza della chiave permette quindi di decifrare il messaggio.

Cifratura	**A** B C D E F G H I L M N O P Q R S T U V Z
	Q E S O L U A I R T H V M C G D P B Z N F

Decifratura	A B C D E F G H I L M N O P **Q** R S T U V Z
	G T P R B Z Q M H E O V D S **A** I C L F N U

Testo in chiaro:

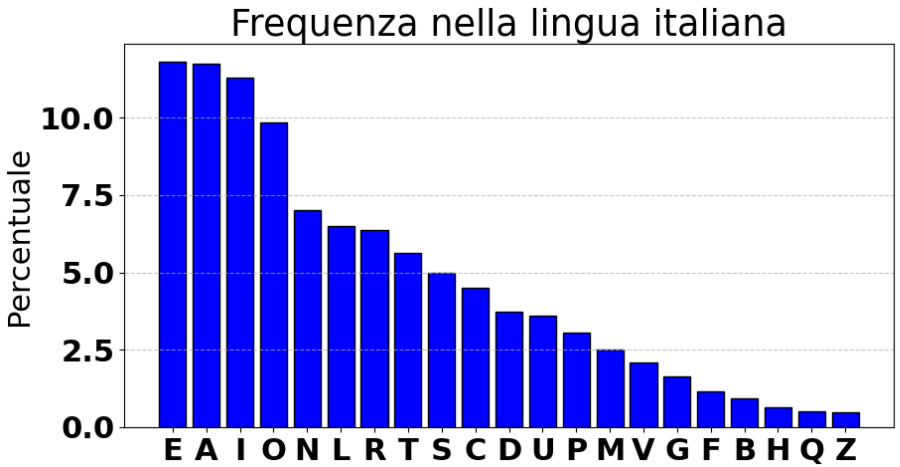
NELLACIFRATURAMONOALFABETICAUNTESTOINCHIAROVIENE
CIFRATOSOSTITUENDOAOGNILETTERAUNALTRALETTERAINAC
CORDOCONUNAREGOLASEGRETADETTACHIAVECHEPUOESSEREI
NVERTITALACONOSCENZADELLACHIAVEPERMETTEQUINDIDID
ECIFRAREILMESSAGGIO

Testo cifrato:

VLTTQSRUDQBZDQHMVMQTUQELBRSQZVBLPBMRVSIRQDMNRLVL
SRUDQBMPMPBRBZLVOMQMAVRTLBBLDQZVQTBDQTLBBLDQRVQS
SMDOMSMVZVQDLAMTQPLADLBQOLBBQSIRQNLSILCZMLPPLDLR
VNLDBRBQTQSMVMPSLVFQOLTTQSIRQNLCLDHLBBLGZRVORORO
LSRUDQDLRTHLPPQAARM

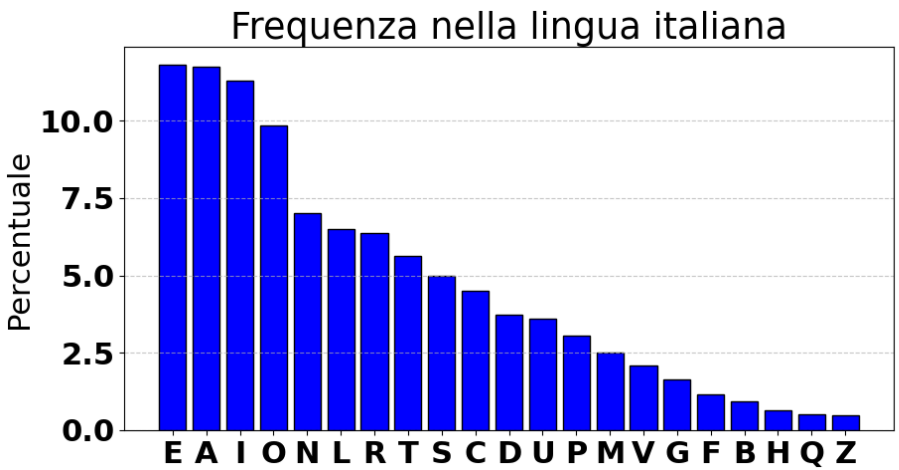
Un Attacco: Analisi delle Frequenze

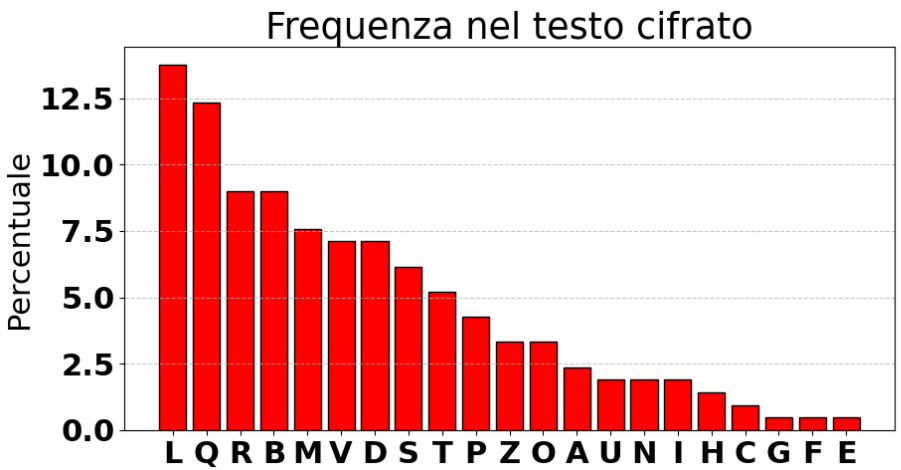
Nella lingua italiana (e in ogni altra lingua) le lettere non compaiono tutte con la stessa frequenza.



Un Attacco: Analisi delle Frequenze

Nella lingua italiana (e in ogni altra lingua) le lettere non compaiono tutte con la stessa frequenza.

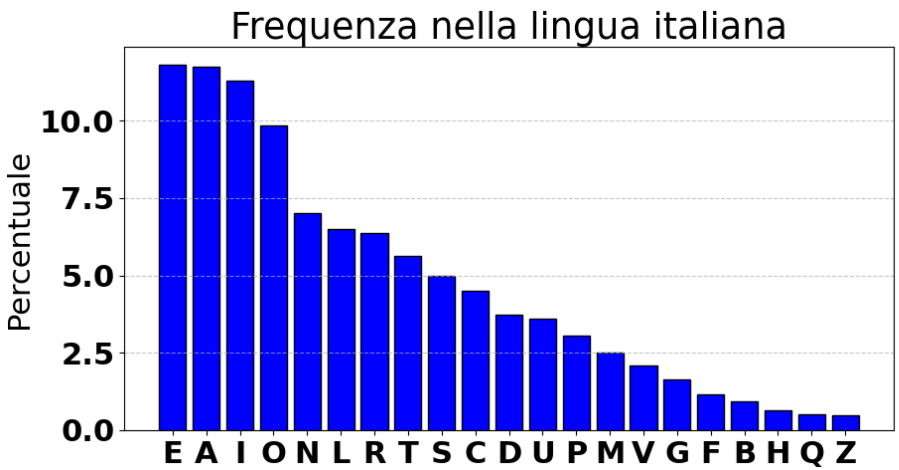


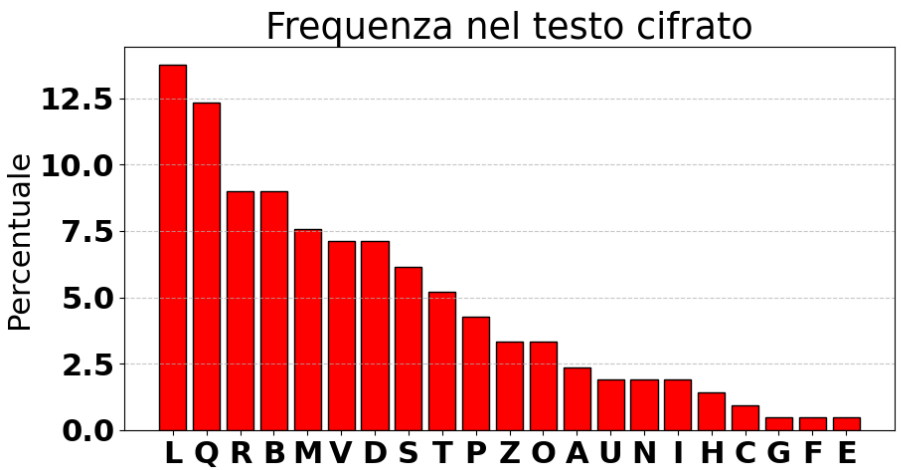


Calcolando la frequenza delle lettere nel testo cifrato possiamo quindi intuire la chiave.

Un Attacco: Analisi delle Frequenze

Nella lingua italiana (e in ogni altra lingua) le lettere non compaiono tutte con la stessa frequenza.





Calcolando la frequenza delle lettere nel testo cifrato possiamo quindi intuire la chiave.

In effetti **E**, **A**, **I** erano state cifrate in **L**, **Q**, **R**, rispettivamente. Invece **O** era stata cifrata in **M**, non in **B** (questo è un metodo statistico, non può essere esatto).

Inventa un metodo ingegnoso per cifrare e decifrare.
(Cifrario di Cesare, cifrario di Vigenére, macchina Enigma...)

Tieni il metodo segreto al nemico.
(**Security through obscurity**.)

Spera che nessuno sia più intelligente di te.

La Crittografia Moderna (La Scienza)

La crittografia moderna:

La Crittografia Moderna (La Scienza)

La crittografia moderna:

È usata da tutti ogni momento:
Internet surfing, emails, electronic banking, mobile phones, apps, video calls...

La Crittografia Moderna (La Scienza)

La crittografia moderna:

È usata da tutti ogni momento:
Internet surfing, emails, electronic banking, mobile phones, apps, video calls...

Si occupa di una moltitudine di tematiche:
cifratura e decifratura, firme digitali, schemi di identificazione e autentificazione, crittografia omomorfa, dimostrazioni a conoscenza zero, blockchain e criptovalute, calcolo distribuito...

I suoi principi fondanti sono i seguenti.

I suoi principi fondanti sono i seguenti.

Definisci chiaramente le assunzioni sulle capacità del nemico. (**Assunzioni di sicurezza**)

I suoi principi fondanti sono i seguenti.

Definisci chiaramente le assunzioni sulle capacità del nemico.
(**Assunzioni di sicurezza**)

Definisci chiaramente cosa intendi per sicurezza.
(**Definizioni formali**)

I suoi principi fondanti sono i seguenti.

Definisci chiaramente le assunzioni sulle capacità del nemico.
(**Assunzioni di sicurezza**)

Definisci chiaramente cosa intendi per sicurezza.
(**Definizioni formali**)

Assumi che lo schema sia noto a tutti.
(**Kerckhoffs's principle**)

I suoi principi fondanti sono i seguenti.

Definisci chiaramente le assunzioni sulle capacità del nemico.
(**Assunzioni di sicurezza**)

Definisci chiaramente cosa intendi per sicurezza.
(**Definizioni formali**)

Assumi che lo schema sia noto a tutti.
(**Kerckhoffs's principle**)

Dimostra matematicamente la sicurezza dello schema.
(**Dimostrazioni di sicurezza**)

Ma Come Dimostrare che non Esistono Attacchi?

Dimostrare che **esiste** un attacco è concettualmente semplice:

Ma Come Dimostrare che non Esistono Attacchi?

Dimostrare che **esiste** un attacco è concettualmente semplice:

Basta trovarlo!

(Come abbiamo trovato l'attacco che usa l'analisi delle frequenze.)

Ma Come Dimostrare che non Esistono Attacchi?

Dimostrare che **esiste** un attacco è concettualmente semplice:

Basta trovarlo!

(Come abbiamo trovato l'attacco che usa l'analisi delle frequenze.)

Ma come dimostrare che **non esiste** un attacco?

Ma Come Dimostrare che non Esistono Attacchi?

Dimostrare che **esiste** un attacco è concettualmente semplice:

Basta trovarlo!

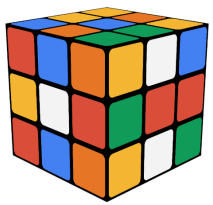
(Come abbiamo trovato l'attacco che usa l'analisi delle frequenze.)

Ma come dimostrare che **non esiste** un attacco?

Scendere nei dettagli ora sarebbe complicato, ma possiamo fornire una illustrazione.

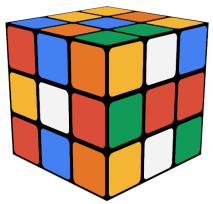
Dimostrare la Sicurezza

Si assume che il nemico non sia in grado di risolvere un determinato problema matematico



Dimostrare la Sicurezza

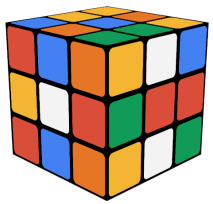
Si assume che il nemico non sia in grado di risolvere un determinato problema matematico



Alcuni problemi utilizzati in crittografia sono:

Dimostrare la Sicurezza

Si assume che il nemico non sia in grado di risolvere un determinato problema matematico

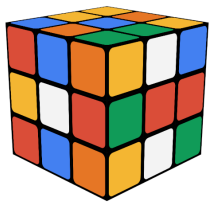


Alcuni problemi utilizzati in crittografia sono:

- la fattorizzazione del prodotto di due grandi numeri primi,

Dimostrare la Sicurezza

Si assume che il nemico non sia in grado di risolvere un determinato problema matematico

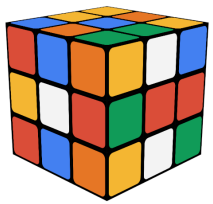


Alcuni problemi utilizzati in crittografia sono:

- la fattorizzazione del prodotto di due grandi numeri primi,
- il problema del logaritmo discreto,

Dimostrare la Sicurezza

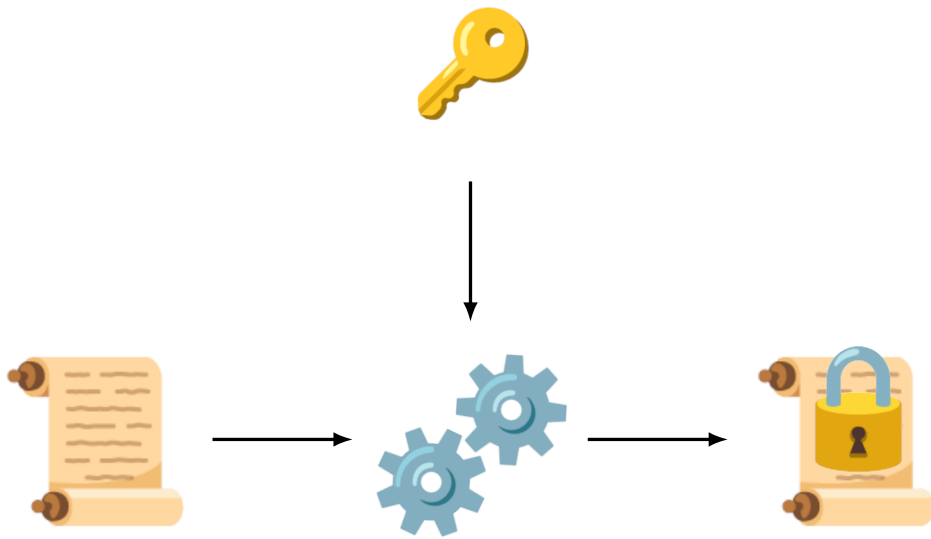
Si assume che il nemico non sia in grado di risolvere un determinato problema matematico



Alcuni problemi utilizzati in crittografia sono:

- la fattorizzazione del prodotto di due grandi numeri primi,
- il problema del logaritmo discreto,
- il problema di invertire una funzione di hash...

Si definiscono i dettagli dello schema e cosa si intende per sicurezza.

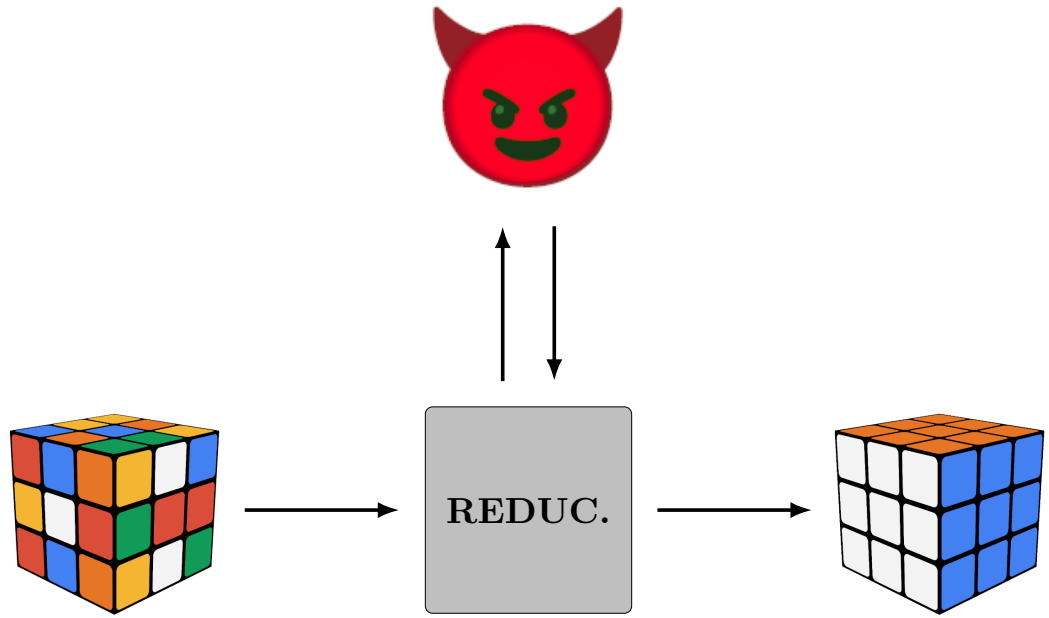


In questo caso si tratta di uno schema di cifratura.

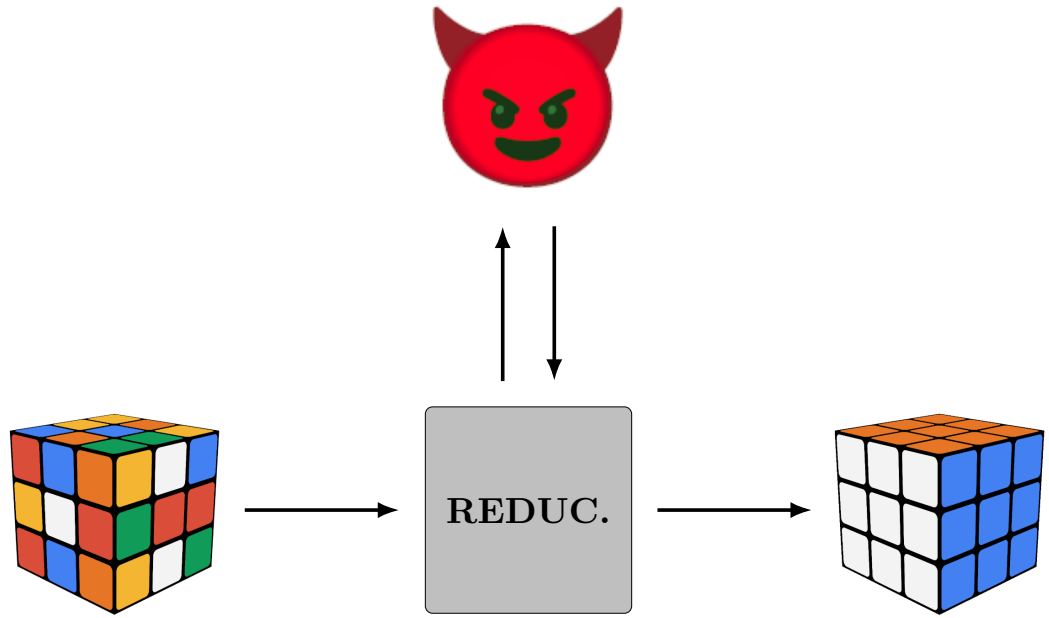
Per sicurezza si intende che il testo cifrato non è decifrabile senza conoscere la chiave secreta.

Per assurdo, si suppone che il nemico sia in grado di violare la sicurezza dello schema, cioè decifrare il testo cifrato senza conoscere la chiave.

Si costruisce un algoritmo (**riduzione**) in grando di risolvere il problema matematico utilizzando l'ipotetico nemico come sottoprocedura.

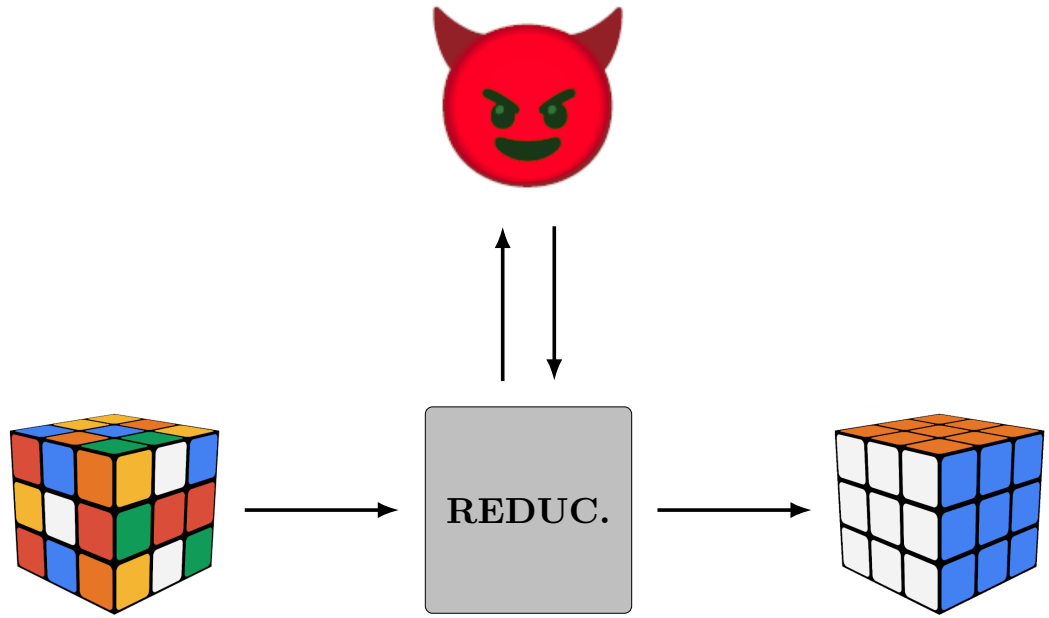


Si costruisce un algoritmo (**riduzione**) in grando di risolvere il problema matematico utilizzando l'ipotetico nemico come sottoprocedura.



Quindi il nemico **è** in grado di risolvere il problema matematico, **assurdo!**

Si costruisce un algoritmo (**riduzione**) in grando di risolvere il problema matematico utilizzando l'ipotetico nemico come sottoprocedura.



Quindi il nemico **è** in grado di risolvere il problema matematico, **assurdo!**

Dunque si conclude che il nemico **non** può essere in grado di violare la sicurezza dello schema. ■

GRAZIE PER L'ATTENZIONE!

(Domande?)