La Crittografia nella didattica dei corsi di Teoria della Complessità

Filippo Mignosi

Roma, 4 Ottobre 2018

Schema del talk

- Coorti di Studenti al DISIM: caratteristiche
- Didattica Centrata sugli Studenti
- Precedenti
- Come motivare in pratica usando la Crittografia
- Se $\mathbb{P} = \mathbb{NP}$ crolla la Crittografia - Classi di complessità
- Corsi con Crittografia al DISIM

COORTI DI STUDENTI al DISIM

Dipartimento di Ingegneria, Scienza dell Informazione e Matematica

INFORMATICI

MATEMATICI

INGEGNERI

Caratteristiche (parere a titolo personale):

Gli informatici: in maggioranza non amano le dimostrazioni matematiche e teorie matematiche.
I matematici: senza dimostrazioni che matematica si fa?
Gli ingegneri: Sono vicini agli informatici ma accettano di più i sacrifici matematici.

DIDATTICA CENTRATA SUGLI STUDENTI

Metodologia didattica molto studiata. Si può associare alla teoria dell'apprendimento prossimo (prossimale) di Vygotskij, alla idea dello scaffolding di Bruner e all'apprendimento attivo di Dewey.

- La Teoria della Complessità è ostica agli informatici. Non viene insegnata alle altre due coorti. Concetti e tecniche sono estremamente importanti nella Crittografia Moderna.
- La crittografia è nota, come uso, agli informatici. Molti studenti desiderano averne padronanza.

Quindi ha senso sfruttare la fama e la rilevanza della crittografia (e i desideri) al fine di motivare gli studenti a studiare la teoria della Calcolabilità e della Complessità.

On the Use of Complexity In Cryptography

A computational complexity gap, captured in the definition of one-way functions, is a necessary and sufficient condition for much of modern cryptography. Loosely speaking, one-way functions are functions that are easy to compute but hard to invert (in an average-case sense). The existence of one-way functions implies that P is different from NP, which means that such a complexity gap is only widely conjectured to exist (rather than known for a fact). We

key-generation procedure outputs a (random) pair of corresponding (n-bit long) encryption and decryption keys, (e, d), such that for every bit string x, it holds that $D_d(E_e(x)) = x$, where $E_e(x)$ (resp., $D_d(y)$) denotes the output of the encryption (resp., decryption) procedure on input (e, x) (resp., (d, y)).

The difference between the two cases lies in the way in which the scheme is employed and this will be reflected in the definition of security. In the first case,

In the second case, known as the public-key case, the receiver invokes the key-generation process, publicizes the encryption key e (but not the decryption key d), and the sender uses e to generate encryptions as before. This allows everybody (not only parties that the receiver trusts) to send encrypted messages to the receiver; however, in such a case the adversary also knows the encryption key e. Thus, the information available to the adversary in this case is a sequence

this assumption is implied by widely believed conjectures such as the conjectured intractability of factoring integers.

BEYOND ENCRYPTION SCHEMES

Cryptography encompasses much more than methods for providing secret communication. Another basic cryptographic task is that of providing authenticated communication, which in turn is reduced to

COME MOTIVARE IN PRATICA

Corso obbligatorio: Teoria della Calcolabilità e della Complessità. Terzo anno secondo semestre.

Libro di testo: Hopcroft Motwani Ullman: Introduction to Automata Theory, Languages, and Computation

Altri libri per approfondimenti. Arora-Barac, Goldreich, Sipser.

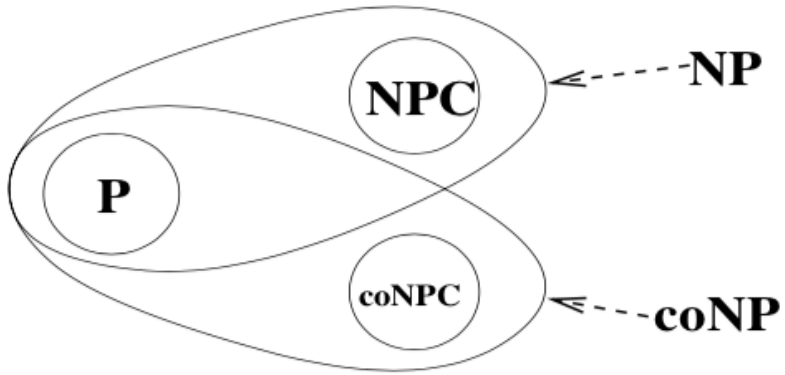
Crittografia Inizio Corso (non determinismo, simulazioni, fattorizzare) ma soprattutto all'inizio della seconda parte.

Se $\mathbb{P} = \mathbb{NP}$ allora non esiste crittografia come la conosciamo ora (non esistono funzioni one-way). One-time-pad esisterà sempre.

E svolgere un esercizio quando si parla di $\mathbb{NP} \cap co - \mathbb{NP}$, con semplificazione translata da una prova di Goldrech di un teorema diverso.

Se $\mathbb{P} = \mathbb{NP}$ crolla la Crittografia - Classi di complessità

Esercizio: se esistono permutazioni one-way allora esiste un linguaggio che sta in $\mathbb{NP} \cap co - \mathbb{NP}$ e non sta in $\mathbb{P}$.



Opzionale per i voti alti. Un buon terzo degli studenti porta la prova all'esame, ma l'efficacia motivazionale mi sembra superiore.

Alcuni corsi con argomenti di Crittografia al DISIM

Distributed Systems. 4 ore.

Information and Network security (per informatici). 20 ore.

Combinatorics and Criptography (tutto).

Network Systems and Applications. Un terzo del corso.

Teoria dell'informazione. Un terzo del corso.

Chiedo scusa ai colleghi che insegnano crittografia il cui corso non è nominato.

Corsi (e ore) con argomenti legati alla sicurezza sono molti di più.

GRAZIE