Crittografia e telecomunicazioni

Prof. Massimiliano Sala

Roma (da Trento in videoconf) - 6 febbraio 2024

Prof. Massimiliano Sala

Università degli Studi di Trento

- Professore ordinario di Algebra
- Direttore del Laboratorio di Crittografia

Associazione nazionale di crittografia De Cifris

- **Presidente**

Crittografia

Crittografia I

- La **Crittografia** è una scienza antica, nota già agli Egizi e ai Greci.

- Si occupa di nascondere un messaggio, manipolandolo in base a certe regole, note solo alle due persone che comunicano.

Crittografia II

- Al mondo d'oggi, queste **regole** sono scritte in programmi o in dispositivi elettronici.

- Le due persone che comunicano, per esempio usando Whatsapp dal loro telefono, possono farlo solo se usano la stessa **regola**, che prende il nome tecnico di **chiave crittografica**.

Crittografia III

- Purtroppo, al mondo d'oggi le persone che si parlano nemmeno si rendono conto che la loro comunicazione è protetta da una **chiave**, tanto meno la sanno.

De Componendis Cifris

De Cifris I

- La De Componendis Cifris (De Cifris) è l'associazione nazionale di **crittografia** italiana

- Abbiamo quasi quattrocento membri, per metà accademici di oltre **venti** università italiane, oltre a numerosi ricercatori italiani che lavorano all'estero o in importanti aziende del settore.

De Cifris II

- Importanti istituzioni, come la **Banca d'Italia** e la **CONSOB**, collaborano con noi.

- L'Agenzia per la Cybersicurezza Nazionale (**ACN**) ha ultimato il processo di affiliazione alla nostra associazione l'anno scorso.

De Cifris III

- L'anno scorso sono stato eletto **Presidente** dall'Assemblea plenaria di **De Cifris**.

- Oggi vi parlo con delega specifica del Consiglio Direttivo di **De Cifris**.

Conclusioni

Conclusioni I

- La **crittografia** è fondamentale per proteggere sia la privacy dei cittadini, sia la sicurezza delle transazioni finanziarie.

- Vi sono dimostrazioni matematiche rigorose che provano la robustezza delle **chiavi crittografiche** (a meno di quantum computer).

Conclusioni II

- Le **chiavi crittografiche** sono generate da programmi o dispositivi.

- **Quindi** solo chi li produce potrebbe darle. Di conseguenza, gli operatori di tlc **non** possono **decrittare** il traffico.