UNIVERSITÀ DEGLI STUDI DI TRENTO - LABORATORIO DI MATEMATICA INDUSTRIALE E CRITTOGRAFIA

# Le CryptoWars

Le CryptoWars sono una gara nazionale di Crittografia volta a suscitare interesse in questa materia che al giorno d'oggi trova sempre più applicazioni nella realtà quotidiana.

Singoli appassionati e team si sfidano tra loro, creando codici e rompendo quelli degli altri.

La gara prevede 3 categorie distinte a cui prendere parte:

- ✗ CATEGORIA CLASSICA. **Costruire un algoritmo di cifratura Polialfabetico e attaccare i codici delle altre squadre.**
- ✗ CATEGORIA CHIAVE PUBBLICA. **Provare a rompere chiavi segrete di famosi crittosistemi (come RSA ed ECC) usando tutti i mezzi disponibili.**
- ✗ CATEGORIA CHIAVE SIMMETRICA. **Attaccare il block cipher BunnyTN, montando un attacco efficace per il maggior numero di round.**

Per maggiori informazioni su come partecipare alla gara, consulta il sito internet:

**http://www.science.unitn.it/~sala/cryptowars/**

oppure scrivi all'indirizzo email:

mathnow.unitn@gmail.com

TERMINE ISCRIZIONI **20 OTTOBRE 2011**

Clusit Associazione Italiana per la Sicurezza Informatica — alpha orionis — CONFIDACE — seeweb HIGH QUALITY HOSTING — Privatewave