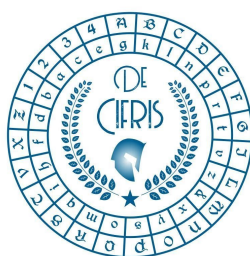


De Cifris Athesis



UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica



ICT
CENTER FOR INFORMATION AND
COMMUNICATION TECHNOLOGY

Thursday 3rd December 2020 – at 10:00
Online Seminar via Zoom

Luca Lusini

Agid

Studiare la crittografia dei ransomware

Abstract: Una parte importante dell'analisi di un ransomware consiste nell'identificare quali schemi crittografici vengano usati. Comprenderli permette di stabilire la fattibilità di un decryptor e offre un importante banco di prova per il crittografo, che viene proiettato nel ruolo di colui che deve decifrare dati senza possederne la chiave.

Un ruolo che pone fortemente l'accento sull'aspetto pratico della sicurezza delle implementazioni crittografiche.

Il seminario mostrerà esempi reali di ransomware con le tecniche usate per l'identificazione delle primitive, ogni volta seguite da un'analisi dello schema risultante. Il tutto finalizzato alla ricerca di possibili vulnerabilità, nell'implementazione crittografica, che possano salvare il lavoro e i risparmi delle vittime.

Iscrizione all'evento online da effettuare entro il 2 dicembre tramite il seguente link:

[click here](#)

Gli iscritti riceveranno l'ID Zoom un'ora prima dell'inizio dell'evento.

Contact person: Massimiliano Sala

CONTATTI

Associazione De Componendis Cifris

seminari@decifris.it

segreteria@decifris.it