

Are your secrets safe? From Cesar to WhatsApp

A seminar by Jesùs Manuel Soto

*Department of Mathematics
University of Sevilla*

11 March 2021 | 4:30 p.m.

Live Zoom

[https://unipd.zoom.us/j/81621658875?
pwd=QU5WOElFT3RpRGpOdno3ckFmNTVWZz09](https://unipd.zoom.us/j/81621658875?pwd=QU5WOElFT3RpRGpOdno3ckFmNTVWZz09)

We use cryptography every day. Thousands of times. Once for each WhatsApp message we send, for instance. How does it help us keep our conversations confidential? In this talk, we will quickly review some historical ciphers, and we will introduce the state-of-the-art crypto problem: the discrete log problem over elliptic curves. Also, I will show how to hack WhatsApp. Don't do this at home.