Cryptography and Number Theory

Othmane Rih

January 28, 2024

Abstract

Hi everyone ! In this class, I will talk about two of the most important cryptographic protocols, namely RSA and the Diffie-Hellman key exchange, and we will see how to break them. We will talk about algorithms that allow us to factorise large numbers and solve what is known as the discrete logarithm problem. And, if time permits, I will talk a little bit about my project in post-quantum cryptography.

Prerequisites : Modular arithmetics and basic notions of group theory.