KHOA BUI
STUDENT, MATHEMATICAL AND PHYSICAL SCIENCES

USING THE LLL-ALGORITHM TO BREAK THE RSA CRYPTOSYSTEM

The Rivest-Shamir-Adleman (RSA) cryptosystem is one of the most popular cryptosystems being used in secure data transmission. Until today, the cryptosystem is still considered to be safe due to the hardness of the factorization problem. The Lenstra-Lenstra-Lovãisz (LLL) algorithm offers various methods to attack the RSA cryptosystem, even going as far as potentially breaking the system by solving the factorization problem. In this presentation, we will discuss how a weak parameter creates deadly vulnerabilities in the RSA cryptosystem, and the usage of LLL-algorithm in the factorization problem.

Research Advisor: Dr. Ha Tran