Supragyapal Singh
STUDENT, BACHELOR OF SCIENCE - MATHEMATICS CONCENTRATION

Khoa Bui
RESEARCH TEAM MEMBER

Keeping your data safe using Number Theory and Abstract Algebra

Elliptic curve cryptography (ECC) is one of the most popular modern crypto systems being used in secure data transmission because of its efficiency yet providing the equivalent security to crypto systems not based on elliptic curves. In this presentation, we will discuss the mathematical background behind crypto systems that are based on the algebraic structure of elliptic curves over finite fields. Furthermore, we will present real-life applications of ECC by introducing the Diffie-Hellman key exchange and El Gamal asymmetric crypto system.

Research Advisor: Dr. Ha Tran, Associate Professor