COURSE DETAIL

MATHEMATICS OF MODERN CRYPTOGRAPHY

Country
Taiwan

Host Institution
National Taiwan University

Program(s)
National Taiwan University

UCEAP Course Level
Upper Division

UCEAP Subject Area(s)
Mathematics Computer Science

UCEAP Course Number
126

UCEAP Course Suffix

UCEAP Official Title
MATHEMATICS OF MODERN CRYPTOGRAPHY

UCEAP Transcript Title
MATH CRYPTOGRAPHY

UCEAP Quarter Units
4.50

UCEAP Semester Units
3.00

Course Description

This course provides an introduction to modern cryptography with a mathematical focus. It covers the basics of abstract algebra and number theory, and introduces cryptocurrencies such as Bitcoin, BlockChain, and FinTech. Topics include data security, stream ciphers, Data Encryption Standard (DES) and alternatives, Advanced Encryption Standard (AES), block ciphers, public-key cryptography, RSA Cryptosystem, elliptic curve cryptosystems, digital signatures, hash functions, Message Authentication Codes (MACs), and key establishment.

Language(s) of Instruction

Host Institution Course Number
MATH5425

Host Institution Course Title
MATHEMATICS OF MODERN CRYPTOGRAPHY

Host Institution Campus

Host Institution Faculty

Host Institution Degree

Host Institution Department
Mathematics

Print