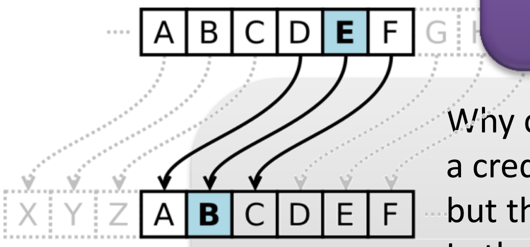
UNIVERSITY OF CENTRAL ARKANSAS™

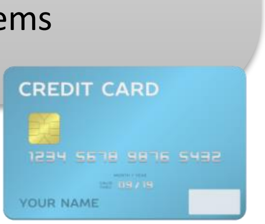
Number Theory with Applications to Cryptography

Course: MATH 6315: Introduction to Number Theory
Semester: Spring 2018
Times: Tuesday, Thursday 4-5:15pm
Instructor: Dr. Jeffrey Beyerl
Department: Mathematics
Prerequisites: Consent of Instructor
Course is open to all majors

$^1/_3$ Applications of Number Theory to Cryptography



Why can the magnetic strip of a credit card be “skimmed”, but the “chip” cannot be?
In the 1970’s the advent of public key cryptography changed the face of communication.
We’ll study both current non-elliptic pubic key cryptosystems, as well as briefly touch on the nature and state of quantum computing resistant public key cryptosystems



$^1/_3$ Classical Number Theory

Classical Number Theory is the study of the structure of integers. Concepts as simple as primality actually have very deep properties that the human race has yet to completely flesh out.

$$17 = 5 \cdot 3 + 2$$

$$\pi(n) = \Theta\left(\frac{n}{\log(n)}\right)$$

$$e_k(x) \equiv x^b \bmod n$$
$$ab \equiv 1 \bmod \varphi(n)$$

$^1/_3$ Applications of Number Theory to Diophantine Equations

If time permits, the last portion of the class will take classical number theory through a roller coaster you never expected. The result is going to be properties of equations an undergraduate math major has never even dreamed of.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Legendre Symbols