An Introductory Cryptography Course for Non-Technical Backgrounds

By: Emily Estrada (eestrada@andrew.cmu.edu) and Dr. Hanan Hibishi

Introduction and Background:

- In the era of technology, we rely on computers for storing all our data, including making transactions
- Cryptography allows us to secure our data online against potential hackers through math and algorithms
- It is even used in digital forms of currency such as cryptocurrency (Bitcoin, Ethereum) which doesn't require banks
- Cryptography allows us to send a secret message without any one who isn't the recipient intercepting that message
- PicoCTF is a website for middle school through college students to practice different kinds of cyber security skills, including cryptography
- **Can we design an introductory cryptography course for students with non-technical background?** Yes! See the "Methods and Designs" section to see how we did it

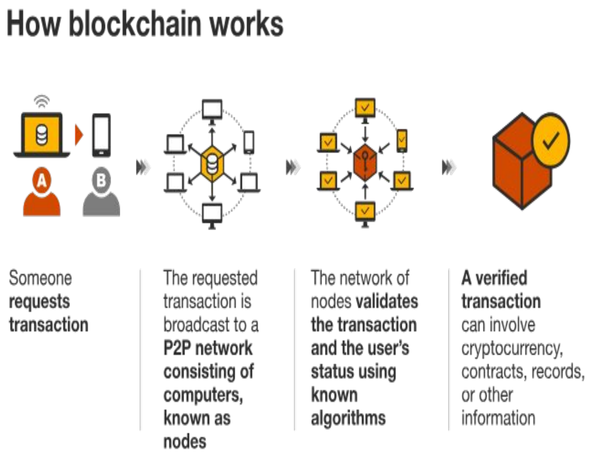
Methods and Designs:

- Created challenges and included diagrams to facilitate the learning experience by researching how other courses and websites teach cryptography
- Used "ramp up" strategy to slowly increase the difficulty of the topics and challenges for a smooth experience
- 3 units: **ciphers**, **encryption methods**, **cryptocurrencies and blockchain**
- For each unit, we had challenges to test the understanding of the student along with solutions

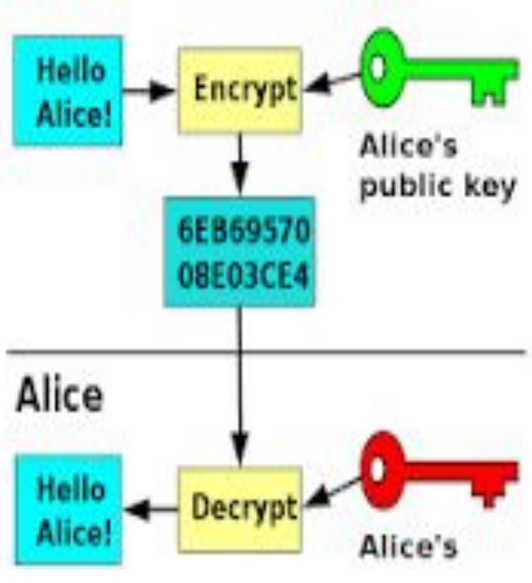
Discussion and Future Work:

- **Key takeaway:** Anyone (non-technical backgrounds) can learn from this course, it was designed with everyone in mind
- **Future:** we plan to make this content available on PicoCTF to assist with learning the cryptography section and analyze how many times people take the course and collect data on which challenges are the more solved

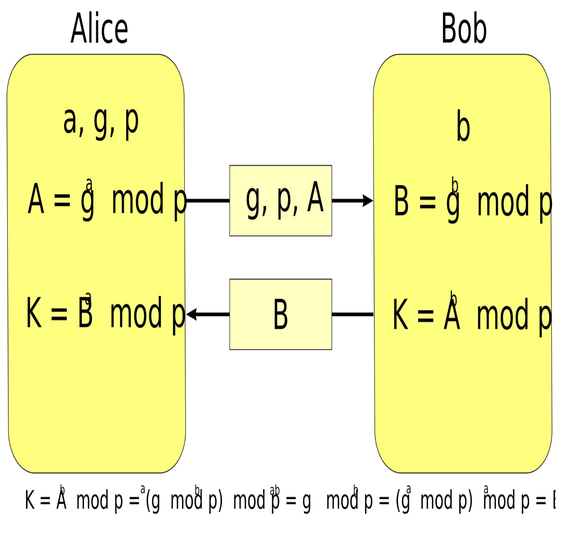
Cryptocurrencies and Blockchain Application



Encryption and Decryption of Ciphertexts



How Diffie-Hellman works



Challenge Design 0: Encrypting ciphers with ROT13