CCSU

DEPARTMENT OF MATHEMATICAL SCIENCES

VIRTUAL COLLOQUIUM

Friday, November 13
3:00 – 4:00 PM
https://ccsu.webex.com/meet/gotchev

PUBLIC-KEY CRYPTOGRAPHY

CARMAN CATER

CENTRAL CONNECTICUT STATE UNIVERSITY

Abstract: In this talk we will cover a few of the basic encryption schemes used to establish a shared secret key over a public network. Once established, the key is used with a symmetric-key algorithm for bulk data transfer. As we will see, many of the algorithms we explore rest on results from algebra and number theory.

I hope you will learn a brief history of cryptography, the difference between symmetric and asymmetric encryption, Diffie-Hellman Key Exchange over finite cyclic groups, Elgamal Encryption, RSA Cryptosystem, and the mathematics that underly such algorithms. The security of the schemes discussed relies on the "difficulty" of two problems: The Discrete Logarithm Problem and the Factorization Problem.

Students of any level should be able to enjoy and understand the majority of what will be discussed.

For further information:
gotchevi@ccsu.edu 860-832-2839
http://www.math.ccsu.edu/gotchev/colloquium/