Texas Southern University

MATHEMATICS DEPARTMENT SEMINAR

Secure Communication over the internet

Professor Parag K. Lala
Texas A&M University, Texarkana

Friday, Nov. 21, 2014
2:00 pm – 3:00 pm

Room 153 at Science Building

Abstract

The exchange of information is a key component of private and economic activities. Much of the information communicated electronically on a daily basis, such as financial transactions, employee personal data and medical records, emails etc., must be kept confidential. The problem of unsecure communication is aggravated by the fact that the information sent over the internet may be accessed by third parties. The goal of secure communication is to prevent unauthorized access of information traffic to its intended destination. Therefore, a necessary condition for secure communication is that data to be transmitted must be encrypted that can only decrypted by the intended receiver. In order to encrypt and decrypt data, the sender and recipient need to share a secret that is typically a *key*. This talk will discuss some of the terms and concepts behind encryption and decryption techniques , and will present in detail the symmetric and the asymmetric systems that are used to provide information confidentiality and integrity.