

COLLOQUIUM

3:30 P.M.

OCTOBER 22, 2007

BOEHM HALL 262

Public Key Crypto Systems

PROFESSOR DEEPAK KHANNA

KUTZTOWN UNIVERSITY OF PENNSYLVANIA

ABSTRACT

We will present the basic concept of Public Key Cryptosystems—the advantages they offer and their applications both in terms of privacy as well as authentication. They are designed to resist unlimited chosen-plaintext attack, and their security is based both on the difficulty of extracting the private key from the encryption key and the difficulty of deducing the plaintext from the ciphertext. This allows for an encryption key to be publicly revealed and transmitted over non-secure channels without compromising the privacy of the corresponding decryption key.

Also, Public Key Cryptosystems allow for a message to be digitally signed—these digital signatures can not be forged or repudiated. We will discuss the algorithm used by the most widely successful and adopted Public Key Cryptosystem—RSA Cryptosystem. The underlying one-way 'trapdoor' function will be presented. It will be shown that factoring the product of two very large prime numbers is a computationally hard problem. The security of the system, and why it has withstood various cryptanalysis attacks, will be discussed. Modern advances in Public Key Cryptography will also be presented.

Finally, we will share some interesting facts about various cryptographic challenges.

3:00 p.m.**refreshments served****3:30 p.m.****talk begins**