Colloquium

Date, time & venue: Tuesday, November 28, 2017, 1:15-2:15 in UAB 419

Title: **Securing Emails from Service Providers**

Speaker: **Dr. Priyanka Singh, University at Albany, SUNY**

Abstract: Email communication is one of the very frequent communication modes nowadays. Besides regular sharing of day-to-day business emails, we often share our most confidential information over email which may include passport information, social security numbers, credit card scans, medical reports, etc. without paying much attention to the underlying security concerns. Though the existing email services provide enough security from external malicious adversaries and eavesdroppers by employing network security mechanisms, they still remain vulnerable to the security of the confidential content stored at the third party email service providers (ESPs). Once the content is outsourced at these ESPs, it is at their discretion and they can access and breach the security of the content if they choose to. Initially, this talk covers some of these issues and challenges.

Many third-party solutions like Pretty Good Privacy (PGP) exists but due to their limitation of key management and reliance on other infrastructure their popularity decreased. The talk will cover the key idea of how we can secure all the contents exchanged between the two entities without the overhead of maintaining the secret keys or reliability on third-party solutions. A couple of results achieved during our experimentations against various attacks like cross-linkage attack, brute force attack and collusion attack prevalent in practical scenarios will be presented

Speaker's brief bio:

Priyanka Singh is currently working as a Postdoc in the Department of Computer Science, College of Engineering and Applied Sciences, University at Albany. Prior to this, she did one year postdoc from Indian Institute of Technology Roorkee, India. She got her PhD from Motilal Nehru National Institute of Technology Allahabad, India in 2016. Her current area of research interests are Cyber Security, Privacy and Security issues in Cloud Computing, Encrypted Domain Processing, Secure Data Deduplication, Multimedia Security, and Visual Cryptography. Currently, she is serving as the reviewer for many prestigious journals like ACM Transactions on Multimedia Computing Communications and Applications, Information Sciences, Signal Processing: Image Communication, Journal of Systems and Software, Digital Signal Processing, Journal of Information Security, IET Image Processing, and Signal Processing.