Title: Signcryption = Achieving Confidentiality and Authentication at the Same Time

Speaker: Sumit Kumar Pandey, CR Rao AIMSCS, Hyderabad

Abstract:
Confidentiality and Authentication are two of the most important goals of cryptography. Confidentiality is achieved through encryption schemes whereas message authentication is achieved through signature schemes in public key setting. Simple patching of encryption and signature schemes may not provide confidentiality and authentication both. For example, "encrypt & sign" and "encrypt then sign" do not give desired security but "sign then encrypt" provides so. In the year 1997, Zheng introduced the notion of signcryption scheme whose motivation was to provide confidentiality and authentication at the same time with lower computational cost and lower communication overhead than "Sign then Encrypt" approach.
In this talk , we shall discuss some existing paradigms to construct signcryption schemes and then investigate their security in different security models.