abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A fundamental question in cryptography is whether the existence of hard on average problems can be based solely on the assumption that P not equal to NP (more precisely, NP not in BPP). The commonly held belief that average-case hardness requires stronger assumptions than NP hardness was challenged in the mid 1990s by the construction of cryptosystems whose security follows from a worst-case intractability assumption.

Despite many efforts, however, it is not known whether the assumption P not equal to NP is necessary for cryptography. In this talk I will review some of the contrasting evidence with respect to this question.