"How Cryptosystems Are Really Broken"

GTISC/ARC Distinguished Lecture
Thursday, March 8, 2012, 3pm
Klaus 1116E&W
Reception immediately following

Professor Adi Shamir

Abstract

Most of the cryptosystems we currently use are highly secure, and cannot be broken by mathematical cryptanalysis. However, over the last fifteen years researchers have developed many types of physical attacks on their implementations which can easily bypass their mathematical security. In this talk I will survey some of the latest attacks, and show how difficult it is to build a truly secure communication system. The talk will not require any prior knowledge in cryptanalysis.

Bio

Adi Shamir was born, July 6, 1952. He is an Israeli cryptographer. He is a co-inventor of the RSA algorithm (along with Ron Rivest and Len Adelman), a co-inventor of the Feige-Fiat-Shamir identification scheme (along with Uriel Feige and Amos Fiat), one of the inventors of differential cryptanalysis and has made numerous contributions to the fields of cryptography and computer science.

GEORGIA TECH INFORMATION SECURITY CENTER

Georgia Tech Algorithms & Randomness Center