Jeffrey Overbey

Title of Poster Presentation: On the Keyspace of the Hill Cipher

Abstract:
In its most general form, the Hill cipher's keyspace consists of all matrices of a given dimension that are invertible over Z_m. We present a formula for the number of such matrices, outlining a proof that uses only undergraduate mathematics. We also compare this result with the total number of matrices and the number of involutory matrices for a given dimension and modulus, identifying the effects of change in dimension and modulus on the order of the keyspace.