

# NSA's Role in the Development of DES

Richard M. George

Information Assurance Directorate

National Security Agency

`r.george@radium.ncsc.mil`

**Abstract.** 38 years ago, NIST put out a call for submissions of candidates for data encryption standard to address the needs of encryption for the commercial world. Of the submissions, the IBM submission stood out as arguably the best candidate. However, before the algorithm was ready to be chosen as the Data Encryption Standard (DES), some changes were required. The National Security Agency (NSA) worked with IBM on the modification of the submitted algorithm. This talk will discuss what role NSA played in this effort, the rationale for the changes that were made, and the impact that DES had at that time.