Curriculum Vitae of Alan G. Konheim

Contact Information
3735 Essex Street
Santa Barbara, California 93105
☎ (805) 687-1178 (805) 729-2538 agkonheim@cox.net

Education
B.E.E., Polytechnic Institute of Brooklyn (1955)
M.S. (Mathematics), Polytechnic Institute of Brooklyn (1957)
Ph.D. (Mathematics), Cornell University (1960)

Areas of Expertise
Combinatorial algorithms, performance modeling, computer security, cryptography, authentication, hashing.

While a Research Staff Member at the IBM Thomas J. Watson Research Center, I directed and participated in the development and analysis of the FIPS 46-3 Data Encryption Standard (DES).

Work Experience
Mathematics Department, IBM Thomas J. Watson Research Center (1960-82)
Professor, Computer Science Department, UCSB (1982-2005)

Cryptographic Experience
1. National Security Agency, Summers 1983-87;
2. Institute for Defense Analysis/Communications Research Division Summers 1988-1991
3. National Security Agency, Summers 1992-1999;

Publications
1. *Cryptography: A Primer*, John Wiley & Sons, 1982.
2. Computer Security and Cryptography, John Wiley & Sons, 2007; Chinese translation 2011.
3. Hashing in Computer Science, John Wiley & Sons, 2010.
4. Approximately 80 papers in the areas of computer security, hashing functions, performance evaluation, computer communication and combinatorial analysis.
5. Author/coauthor on four US patents, three in the area of computer security.

Teaching
While at UCSB I gave courses in Discrete Mathematics, Computer Networks and Cryptography. I have also lectured at the City University of New York, Courant Institute (New York University) and as a visiting lecturer at Chulalongkon University (Thailand), Monash University (Australia) and the University of Hawaii.