Journal of
INDUSTRIAL
TECHNOLOGY

Volume 18, Number 2 - February 2002 to April 2002

Cryptography Decrypted – Book Review

By David A. Rosenthal, MPA

KEYWORD SEARCH

Computer Programming
Computer Science

Non-Refereed Article

The Official Electronic Publication of the National Association of Industrial Technology • www.nait.org

David Rosenthal has been an Information Technology professional at both the technical and managerial levels for the past 20 years, and is currently the Project Coordinator for the Health Insurance Portability and Accountability Act (HIPAA) compliance project at University Health Systems of Eastern Carolina in Greenville, North Carolina. David is a doctoral candidate in Indiana State University's Technology Management program, and a member of NAIT and the Project Management Institute. He has been published in the journal *Information Systems Management*, and his most recent article entitled "Managing Non-Technical Factors within Healthcare I.T. Projects" will appear in the spring 2002 issue of the *Journal of Healthcare Information Management* ®. He can be reached by e-mail at drosent@pcmh.com.

Cryptography Decrypted – Book Review

By David A. Rosenthal, MPA

The recent terrorist attacks have further engendered into the minds of IT professionals the need to become more acquainted with the concepts of security and the safeguarding of digital assets. Far from what could be considered a traditional textbook, *Cryptography Decrypted* (H.X. Mel & Doris Baker, Addison-Wesley, 2001) is a useful reference work and a practical introduction to the science of cryptography, providing insight into the technology and methodology associated with the various cryptographic capabilities that exist today.

Technical writer Doris Baker and computer consultant H.X. Mel detail cryptography concepts and explain cryptographic terminology in such a way that the reader need not have a background in computer security to understand the topics at hand. From the use of ciphertext messaging by historical figures such as Julius Caesar and Vigenere, to the use of public key encryption (PKE) and secure socket layer (SSL) technology by e-commerce giant Amazon.com, *Cryptography Decrypted* provides a timeline of the innovation and evolution of cryptography and cryptanalysis throughout history. This book can be used to solidify one's existing knowledge of cryptography, or to provide an introduction to fundamental security concepts, and it's sure to be useful to both IT security professionals and CIOs alike.

Divided into four parts, *Cryptography Decrypted* covers secret key cryptography, public key, key distribution and real world systems. A helpful "key points" chart prefaces the book's table of contents and contains a single-sentence description of the major cryptographic topics covered within each chapter of the book, allowing the reader to quickly proceed to an area of interest without the need to first review the table of contents. Specific chapter topics include public and private keys, digital signatures, digital certificates, secure socket layer (SSL), Public Key Infrastructure (PKI), and Internet Protocol Security (Ipsec). Two appendices follow the text and contain information on public key mathematics and random numbers, as well as additional details on the use of Ipsec and IKE authentication.

The chapters within *Cryptography Decrypted* are relatively short in length (most are10 pages or less), and are written in a clear, conversational manner that novices to cryptography will find welcome, but may not appeal to readers who prefer a more "technical" style or approach to the subject matter. Mel and Baker's use of a fictitious pair - "Alice and Bob" - to illustrate many of the cryptographic concepts within the book will be helpful to those who rely on visualization to better comprehend an idea or concept. And in addition to a conclusory review of the concepts previously covered, each chapter also contains interesting and informative illustrations and historical "sidebars", which highlight key events and people within the development of cryptographic systems and the evolution of the various methods of cryptanalysis over the past decades and centuries.

For those interested in exploring the detailed data-element specifications associated with encryption and decryption technology, this is not the book for them. *Cryptography Decrypted* speaks to the person who takes an interest in the safeguarding and security of information and digital possessions, and who wants to understand and comprehend the essentials of computer cryptography, without all of the technical jargon. This book is a must for any IT professional's personal library, and Mel and Baker receive a *decrypted* "thumbs up".