History

1. The Forschungsamt: Nati Germany’s Most Secret Communications Intelligence Agency
   David Kahn Vol. 2 (1)

2. James Lovell and Secret Ciphers During The American Revolution
   Ralph E. Weber Vol. 2(1)

3. My Recollections of G.2 A.6
   J. Rives Childs Vol. 2 (3)

4. Early Work on Computers at Bletchley
   I. J. Good Vol. 3 (2)

5. The Origins of Russian Navy Communications Intelligence
   Thomas R. Hammant Vol. 8 (3)


7. Agnes Meyer Driscoll
   Lt. Susan M. Lujan Vol. 15 (1)

8. Origins of Cryptology: The Arab Contributions
   Ibrahim A. Al-Kadit Vol. 16 (2)

9. An Enigma Chronology
   David Kahn Vol. 17 (3)

10. The Story of the Hagelin Cryptos
    Boris C. W. Hagelin & David Kahn Vol. 18 (3)

11. Soviet Comint in the Cold War
    David Kahn Vol. 22 (1)

12. The History of Non-Secret Encryption
    J. H. Ellis Vol 23 (3)

13. Brigadier John Tiltman: One of Britain’s Finest Cryptologists
    Ralph Erskine & Peter Freeman Vol. 27 (4)

14. Zimmerman Telegram: The Original Draft
    Joachim vonzur Gathen Vol. 31 (1)

15. From the Archives: Inside a Cold War Crypto Cell. Polish Cipher Bureau in the 1980s
    Jan Bury Vol. 32 (4)
16. How I Discovered World War II’s Greatest Spy
David Kahn Vol. 34 (1)

17. Alexander Von Kryha and his Encryption Machines
Klaus Schmeh Vol. 34 (4)

Jose Ramon Soler Fuensanta, Francisco Javier Lopez-Brea Espiau & Frode Weierud Vol. 34 (4)

19. Enigma Message Procedures Used by the Heer, Luftwaffe and Kriegsmarine
Dirk Rijmenants Vol. 34 (4)

20. Was Herbert O. Yardley a Traitor
John F. Dooley Vol. 35 (1)

21. An Accidental Cryptologist: The Brief Career of Genevieve Young Hitt
Betsy Rohaly Smoot Vol. 35 (2)

22. Frank Miller: Inventor of the One-Time Pad
Steven M. Bellovin Vol. 35 (3)

23. US Navy Cryptologic Mathematicians during World War II
Chris Christensen Vol. 35 (4)

24. Operation Stonka. An Ultimate Deception Spy Game
Jan Bury Vol. 35 (4)

25. Leibniz’s *Machina Deciphratoria*: A Seventeenth-Century Proto-Enigma
Nicholas Rescher Vol. 38 (2)

**Mathematics**

1. Assessment of the National Bureau of Standards Proposed Federal Data Encryption Standard
Robert Morris, N. J. A. Sloane & A. D. Wyner Vol. 1 (3)

2. The Hagelin Cipher Machine (M-209) Reconstruction of the Internal Settings
Robert Morris Vol. 2 (3)

3. Mathematical Solution of the Enigma Cipher
Marian Rejewski Vol. 6 (1)

4. A “Weak” Privacy Protocol Using the RSA Crypto Algorithm
Gustavus J. Simmons Vol. 7 (2)
5. A Further Weakness in the Common Modulus Protocol for the RSA Cryptoalgorithm
   John M. Delaurentis Vol. 8 (3)

6. Chosen-Key Attacks on a Block Cipher
   Robert Wintemitz & Martin Hellman Vol. 11 (1)

7. On the Derivation of a “Chaotic” Encryption Algorithm
   Robert Matthews Vol. 13 (1)

8. Mimic Functions
   Peter Wayner Vol. 16 (3)

9. The Use of Genetic Algorithms in Cryptanalysis
   Robert A. J. Matthews Vol. 17 (2)

10. A Self-Study Course in Block-Cipher Cryptanalysis
    Bruce Schneier Vol. 24 (1)

11. Alan M. Turing’s Critique of Running Short Cribson the U.S. Navy Bombe
    Alan M. Turing Vol. 27 (1)

12. The Voynich Manuscript: Evidence of the Hoax Hypothesis
    Andreas Schinner Vol. 31 (2)

13. Rejewski’s Catalog
    Alex Kuhl Vol. 31 (4)

14. Improved Related-Key Attacks on DESX and DESX+
    Raphael C. –W. Phan & Adi Shamir Vol. 32 (1)

15. Algebraic Attacks on the Courtois Toy Cipher
    Marin Albrecht Vol. 32 (3)

16. Attacks and Improvement of an Efficient Remote Mutual Authentication and key Agreement Scheme
    Mark Holbl, Tatjana Welzer & Bostjan Brumen Vol. 34 (1)

17. John F. Byme’s Chaocipher Revealed: A Historical and Technical Appraisal
    Moshe Rubin Vol. 35 (4)

    Alan M. Turing & D. Bayley Vol. 36 (4)

19. The Making of KECCAK
    Guido Bertoni, Joan Daemen, Michael Peeters & Gilles Van Assche Vol. 38 (1)
20. Cryptanalysis of Two GOST Variants with 128-Bit Keys
Nicolas T. Courtois Vol. 38 (4)

Miscellaneous.

1. Poe Challenge Cipher Finally Broken
Brian J. Winkel Vol. 1 (1)

2. The Solution of a Cromwellian Era Spy Message (Circa 1648)
Peter P. Fagone Vol. 4 (1)

3. Cryptographic Reflections of the Genetic Code
Solomon W. Golomb Vol 4 (1)

S. Brent Morris Vol. 7 (1)

5. A Conversion with Claude Shannon One Man’s Approach to Problem Solving
Robert Price Vol. 9 (2)

6. The Matrix Cipher of C. L. Dodgson
Stanley H. Lipson & Francine Abeles Vol. 14 (1)

7. The Legendary William F. Friedman
Lambros D. Callimahos Vol. 15 (3)

8. A Brief History of the Signal Intelligence Service
William F. Friedman Vol. 15 (3)

9. Cryptography as a Teaching Tool
Neal Koblitz Vol. 21 (4)

10. Solved: The Ciphers in Book III of Trithemius’s Steganographia
Jim Reeds Vol. 22 (4)

11. The Navajo Code Talkers: A Cryptologic and Linguistic Perspective
Stephen Huffman Vol. 24 (4)

12. Codes and Ciphers in Fiction: An Overview
John F. Dooley Vol. 29 (4)

Joshua Holden, Richard Layton, Laurence Merkle & Tina Hudson Vol. 30 (1)
14. How I Broke the Confederate Code (137 Years Too Late)  
Kent D. Boklan Vol. 30 (4)

15. Reading Encrypted Diplomatic Correspondence: An Undergraduate Research Project  
Jeffrey D. Adler, Ryan W. Fuoss, Michael J. Levin & Amanda R. Youell Vol. 32 (1)

16. The Future of the Past – Questions in Cryptologic History  
David Kahn Vol. 32 (1)

17. Using Cartoons to Teach Internet Security  
Sukamol Srikwan & Markus Jakobsson Vol. 32 (2)

Whitfield Diffie Vol. 32 (4)

19. Secret Keeping 101 – Dr. Janice Benario and the Women’s College Connection to ULTRA  
Robert Edward Lewand Vol. 35 (1)

20. Breaking the BTK Killer’s Cipher  
Jeanne Anderson Vol. 37 (3)