

# 2013 Cryptologic History Symposium

## *Technological Change and Cryptology: Meeting the Historical Challenge*

### **Johns Hopkins Applied Physics Laboratory - Kossiakoff Conference Center**

11100 Johns Hopkins Road, Laurel, MD 20722-6099  
(Located approximately 1/2 mile west of U.S. Route 29)

Session location in parentheses:

A=Auditorium, C1=Classroom 1, C2=Classroom 2, L=Lobby, M=Mezzanine

**DAY ONE: THURSDAY, October 17, 2013**

### **Morning**

7:00–8:00 **Reception** (Registration Opens) (L)

8:00-8:30 **Welcoming Remarks and Opening Address** (A)  
Moderator: **Dr. William J. Williams** - Chief, Center for Cryptologic History (CCH)

**OPENING KEYNOTE: Mr. John C. (“Chris”) Inglis** - Deputy Director, National Security Agency (NSA)

8:30-8:45 **BREAK**

8:45-10:15 **PANEL 1: “Turing at a Century: Revelations and Legacies”** (A)  
Moderator: **Dr. David Kahn** - Independent Scholar

- **Dr. David Hatch**, CCH - *Turing in the Context of History*
- **Dr. Craig Bauer**, York College of Pennsylvania - *Alan Turing’s Work on Voice Encryption*
- **Dr. Sandy Zabell**, Northwestern University - *Commentary on Alan M. Turing: The Applications of Probability to Cryptography*

10:15-10:45 **BREAK**

10:45-12:00 (concurrent sessions)

**PANEL 2A:** “Intelligence Preparations for the Next War” (A)

Moderator: **Ms. Betsy Rohaly Smoot**, CCH

- **Mr. John F. Dooley**, Knox College - *SIS and Cipher Machines, 1930-1940*
- **Dr. Timothy S. Wolters**, Iowa State University - *Mechanical Encryption in the U.S. Navy, 1917-1940*
- **Dr. Colin Burke**, University of Maryland at Baltimore County - *What OSS Black Chamber? What Yardley? What ‘Dr.’ Friedman? Ah, Grombach?: The Effort to Launch a World War II Black Chamber*
- **Dr. Mark Stout**, Johns Hopkins University - *Herbert Yardley’s (Unknown) Wartime Career*

**PANEL 2B:** “Cipher Systems and Methods” (C1)

Moderator: **Mr. Barry Carleen**, CCH

- **Mr. Tom Vidar Olsen**, Norwegian National Security Authority - *Holvand and the Invention of the Rotor Machine, 1904-1910*
- **Mr. Ralph Simpson**, Cisco Systems (ret.) - *The Invention of the One-Time Pad*
- **Dr. Chris Christensen**, Northern Kentucky University - *Hall’s Weights and Shinn Weights*
- **Dr. Steven M. Bellovin**, Columbia University - *The One-Time Pad and the Index of Coincidence*

**Afternoon**

12:00-1:00 **LUNCH** (M)

Moderator: **Dr. William J. Williams**, Chief, CCH

- **LUNCHEON KEYNOTE 1: Ms. Carol B. Davis**, CCH (ret.)  
*Russian Plaintext: An Early Cold War COMINT Success*

1:00-1:30 **DEMONSTRATION 1:** “Cryptology as Musical Entertainment” (A)

Moderator: **Dr. David Hatch**, CCH

- **The Parkway Chorale** - *A Musical Showcase of Cryptology*

1:30-2:15 (concurrent sessions)

**DEMONSTRATION 2:** “Research in Progress” (A)

Moderator: **Dr. Timothy J. Mucklow**, CCH (ret.)

- **Dr. Whitfield Diffie**, Sun Microsystems - *The ECM Mark I: How It Worked*

**PANEL 3:** “Cryptography in the Ancient World” (C1)

Moderator: **Mr. Gregory J. Nedved**, CCH

- **Mr. Ralph D. Sawyer**, University of Calgary - *Clandestine Communications in Historic China*
- **Dr. Frank Russell**, University of Transylvania - *Cryptography in Ancient Greece: Information Security or Recognition Device?*

2:15-2:45 **BREAK**

2:45-4:00 **PANEL 4:** “Evolution of NSA’s Cutting Edge” (A)

Moderator: **Mr. Brian Snow**, Information Assurance Directorate (ret.)

- **Mr. David P. Cooley**, CCH - *Voices of SIGINT Technology: Reflections from NSA’s Early Technical Leaders*
- **Mr. Jim Boone**, Research & Engineering (ret.) - *Applying Advanced Technology to Cryptologic Systems: Some Special Management Challenges*
- **Dr. John O’Hara**, Office of Advanced Research (ret.) - *Analog Recording of Telemetry Signals Prior to the Advent of Digital Processing*

4:00-4:15 **BREAK**

4:15-5:30 **PLENARY 1:** “Roundtable on Cyber History” (A)

Moderator: **Dr. Michael Warner**, U.S. Cyber Command

- **Dr. Abraham Wagner**, Columbia University
- **Mr. Jason Healey**, Atlantic Council
- **Dr. Roger Schell**, AESEC Corporation
- **Mr. Sean Kanuck**, National Intelligence Officer for Cyber

# 2013 Cryptologic History Symposium

## *Technological Change and Cryptology: Meeting the Historical Challenge*

**Johns Hopkins Applied Physics Laboratory - Kossiakoff Conference Center**  
11100 Johns Hopkins Road, Laurel, MD 20722-6099  
(Located approximately 1/2 mile west of U.S. Route 29)

Session location in parentheses:

A=Auditorium, C1=Classroom 1, C2=Classroom 2, L=Lobby, M=Mezzanine

**DAY TWO: FRIDAY, October 18, 2013**

### Morning

7:00–8:00 **Reception** (Registration Continues) (L)

8:00-9:15 (concurrent sessions)

**PANEL 5A:** “Cryptology & the Advent of New Technologies” (A)  
Moderator: **Dr. William J. Williams**, Chief, CCH

- **Dr. William Casselman**, University of California – Berkley – *Technical Aspects of the Polish Decryption of Enigma*
- **Dr. Paul E. Ceruzzi**, National Air & Space Museum – *The Culture of Precise Positioning: Origins and Applications of GPS Technology*
- **Dr. Niels Jorgensen**, Roskilde University – *Open Encryption Technology and Social Movements*
- **Ms. Elonka Dunin**, Simutronics – *Origins and Evolution of Geocaching and Cryptology*

**PANEL 5B:** “Wartime Intelligence Operations” (C1)  
Moderator: **Mr. Gregory J. Nedved**, CCH

- **Dr. Chris Christensen**, Northern Kentucky University – *The U.S. Navy’s Attack on JN-25*
- **Mr. Michael W. Pfarr, Jr.**, Department of Defense – *Richard Sorge and the Book Cipher*

- **Dr. Steven Huffman**, Department of Defense – *Codetalkers and Codetalking: The Rest of the Story*
- **Mr. Steven Wagner**, University of Oxford – ‘Blowing the Source’: Britain’s Use of SIGINT in Palestine, 1933-1947”

**DEMONSTRATION 3:** “Bletchley Park Celebrated” (C2)

Moderator: **Dr. David H. Hamer**, National Cryptologic Museum Foundation

- **Mr. Benjamin Gatti** and **Mr. Bob Weiss**, Password Crackers, Inc. – *Breaking the Enigma: A Live Demonstration*
- **Mr. George Keller**, U.S. Navy Reserve (ret.) – *Bletchley Park Revisited: A Photographic Essay*

9:15-9:45 **BREAK**

9:45-10:45 (concurrent sessions)

**PANEL 6A:** “In War’s Aftermath: Cryptology and the Early Cold War” (A)

Moderator: **Dr. David Hatch**, CCH

- **Dr. Thomas Johnson**, CCH (ret) – *American Cryptology during the Cold War*
- **Mr. Robert J. Hanyok**, CCH (ret.) – *On the Edge of Tomorrow’s War: WWII COMINT Confronts Ballistic Missiles and Atomic Weapons*

**PANEL 6B:** “COMINT and the Civil War” (C1)

Moderator: **National Cryptologic Museum Staff**

- **Ms. Jennifer Wilcox**, National Cryptologic Museum – *Signaling the Civil War: The Rise of Two Key Technologies, 1861-1865*
- **Mr. Tim Carver**, Triune University – *Analysis of Espionage: Rose Greenhow’s Cipher Examined*

10:45-11:00 **BREAK**

11:00-12:15 (concurrent sessions)

**PANEL 7A:** “Legacies of the Great War & the Interwar Years” (A)

Moderator: **Dr. Mark Stout**, Johns Hopkins University

- **Dr. Laurence Lyons**, British Aerospace (ret.) and **Mr. Carl J. Bobrow**, National Air & Space Museum – *WWI and the Paradigm Shift in Wireless Communications*
- **Ms. Betsy Rohaly Smoot**, CCH – *Technology and Radio Intercept: The Site at Houlton, Maine, 1918-1920*
- **Dr. John Ferris**, University of Calgary – *Commercial Codes of World Banking, 1916-1942*

**PANEL 7B:** “SIGINT and the Vietnam War Era” (C1)

Moderator: **Mr. David P. Cooley**, CCH

- **Ms. Theresa Monserrat**, University of Southern Mississippi – *American Prestige Has Suffered: Reactions to the PUEBLO Crisis*
- **Mr. Scott Laidig**, U.S. Marine Corps (ret.) – *SIGINT Marines: Preparing the Marine Corps for Vietnam, 1954-1968*
- **Dr. Tom Glenn**, Department of Defense (ret.) – *Recollections of the Fall of Saigon*

**PANEL 7C:** “Historical Codes and Ciphers (C2)

Moderator: **Mr. Gregory J. Nedved**, CCH

- **Dr. Joel Freeman**, Independent Scholar – *Exactly How the Rosetta Stone was Cracked*
- **Mr. Todd Mateer**, Department of Defense – *Cryptanalysis of Beale Cipher Number Two*
- **Dr. Nicholas Gessler**, Duke University – *The Aspinwall Cypher of the Revolutionary War*

12:15-1:15 **LUNCH** (M)

Moderator: **Dr. William J. Williams**, Chief, CCH

**LUNCHEON KEYNOTE 2:** **Dr. George R. Cotter**, Chief Information Officer, NSA (ret.) – *Mission, Technologies, and Heroes*

1:15-2:30 (concurrent sessions)

**PANEL 8A:** “Cryptology in Life and Literature” (A)

Moderator: **Dr. David Hatch**, CCH

- **Dr. Gerhard F. Strasser**, The Pennsylvania State University – *“Encoded” Communications with Ladies in a Turkish Harem, 17<sup>th</sup> Century Style!*

- **Dr. Benedek Lang**, Budapest University of Technology – *Shame, Sex, and Alcohol: Ciphers in the Context of Everyday Practices of Secrecy in Early Modern Times*
- **Ms. Erin Higgins**, Department of Defense – *Examples of Steganography in de Vigènere’s “Traite des Chiffres”*
- **Mr. Klaus Schmeh**, Independent Scholar – *Encrypted Books: Why Some Secrets Fill Hundreds of Pages*

**PANEL 8B:** “East European COMINT during World War II” (C1)

Moderator: **Dr. Thomas Johnson**, CCH (ret.)

- **Dr. Jerca Vodusek Staric**, University of Maribor – *The Emergence of Partisan Espionage and Counterintelligence during WWII*
- **Dr. Lavinia Ciungu**, University of Iowa – *Romania’s Wartime Cryptologic Activities*
- **Dr. Laszlo Ritter**, Hungarian Academy of Sciences – *A Little-Known Counterintelligence Success Story: SIGINT’s Role in Axis Operations against Allied Intelligence Networks in Central Europe*

**PANEL 8C:** “New Voices in Cryptologic History” (C2)

Moderator: **Dr. Kent Sieg**, CCH

- **Mr. Richard Greeley**, Department of Defense – *SIGINT in the Spanish-American War*
- **Capt Kelly Elizabeth Atkinson**, U.S. Air Force – *Examining the U.S. Intelligence Failures in Detecting the Attack on Pearl Harbor*
- **Mr. Jared Antrobus**, Northern Kentucky University – *Alignment of JN-25 Enciphered Groups and Additives*
- **Mr. Jeffrey Berkey**, Independent Scholar – *Elizebeth Smith Friedman: Cryptologic Pioneer*

2:30-3:00 **BREAK**

3:00-4:30 **PLENARY 2:** “A Technological Advantage: Perspectives on Information & Communications Systems Development” (A)

Moderator: **Mr. Ronald J. Lucas, CCH**

- **Dr. Nancy Welker**, Operational Test Authority
- **Dr. Fernand Bedard**, Laboratory for Physical Sciences
- **Mr. Dan Both**, Microelectronics Solutions
- **Additional Panelists**