ANNUAL MEMBERSHIP MEETING, 2004

With a hearty welcome from NCMF President John E. Morrison, the Sixth Annual General Membership Meeting convened on 29 October 2004 in the Kossiakoff Center of the Johns Hopkins University Applied Physics Lab near Columbia, MD. The "brave, new world" of Information Assurance served as the theme, along with an accounting for Foundation activities over the past year. Introduced by President Morrison, NSA Deputy Director William "Bill" Black welcomed the gathering and set the stage in a succinct presentation of an NSA at a dramatic crossroad in its 53-year history. The Information Explosion—the Information Age—Information Technology—the IT world—the quickly changing attempts even to put a name on what was happening– had blurred the fact that earlier dividing lines between intelligence and security, and domestic and foreign responsibilities no longer accounted for what the Agency was about, the challenges it faced and its potential. Constrained by efforts to force its traditional, dual mission into preconceived pigeon-holes—the structures of budget and oversight—NSA had been slow in grasping the changing reality. Black noted that the ubiquitous word, "Coke," had been replaced internationally by an even more "in your face" American brand—"Microsoft." The Information Age was upon us. It was universal. And NSA was at the heart
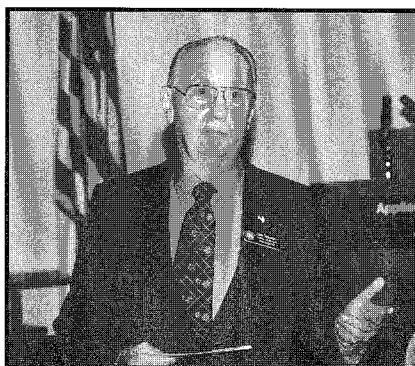
of the government's involvement with "cyber-space." NSA's response had been to develop "mission-blending." Since the first generation of Friedman's disciples, who had been trained from the outset to become proficient in both communication exploitation and communication pr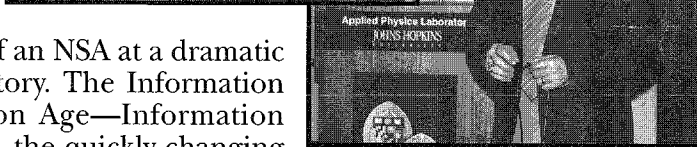otection, the twin mission components had grown apart, with occasional transfers of leadership between the two (recalling the late Walt Deeley and Harry Daniels among those exceptions). Now NSA had, in a sense, returned to its origins, with a synthesis of talent and experience side-by-side, "both in the same box," as he put it: "This is the only way." But to those outsiders accustomed from the past to look at NSA as a source of intelligence information or of cryptographic security (or of computer security, or in other ways), it was difficult for them to get a handle on "the largest and most expensive" of the agencies involved in both intelligence and security. Discussion of a National Intelligence Director and his responsibilities raised new concerns, that the evolving strength discovered in NSA's tools and talents might be diverted or diluted.

Only frank, honest, and careful deliberation was the order of the day, he said, but specialized oversight, and separate budgets, complicated matters. (It seemed to some listeners that "compartmentation"-- usually charged against

OVERVIEW

Our 2004 General Membership Meeting, featured in this issue of The Link, was a resounding success, thanks to the work of Board Member Mike Jacobs, our Program Committee (Bruce Fletcher), and our "headquarters staff." It became obvious from the opening remarks of the Deputy Director of NSA, Bill Black, that we are rapidly distancing ourselves not just from the concepts of the past, but also from the terminology that evolved over the past century. In one sense, "Information Assurance," the program theme, now seems to embrace the totality of the Agency's mission. As we struggle to understand and adopt the new paradigm and its terminology, so must the National Cryptologic Museum expand to embrace the "cyber world" and all that it involves, and place it within the fabric of the centuries-old US cryptologic effort as it interprets that for the public and the professionals of NSA. That, in turn, adds to a sense of urgency for our planning for the "museum of the future."

We apologize for the delay in the issuance of *The Link*, but we wanted those of you who did not attend our annual meeting to see photographs of the speakers and gain some benefit from the program content. The Editor promises swift follow-up of the Winter and Spring issues to get back on track.

William H. Geiger has resigned from our Board, due to other commitments, and I want to thank Bill for his service to the Foundation. A former NCMF Program Chairman, Ralph Adams (who was featured in the opening of the Museum's Viet Nam War exhibit—*The Link*, Summer 1999—and who, at retirement, had been NSA chief of staff) joins us as a Board member. We welcome the return of Ralph, who is also an Association of Former Intelligence Officers (AFIO) board member, and look forward to his renewed involvement in our work.

Our Chairman of Facilities and Services, Rodney B. Sorkin, has suffered a stroke. Our thoughts and prayers for a speedy recovery go out to him and to his family. His deputy, Frank Saus, pursues those activities for the interim, for which we are most grateful.

John E. Morrison
President

DAVID SHULMAN DEAD AT 92

Perhaps forgotten or overlooked by all but the most astute of cryptology historians and students of language, the passing of David Shulman on 30 October 2004 removed from the scene one of the few remaining "true eccentrics" of a breed that once distinguished the field of cryptology, where he labored in secret during WW II, emerging from the shadows to gain notice as a lexicographer and bibliographer, as well as puzzle editor and sports authority. David Kahn—who was acquainted with Shulman for a half century—fondly recalls his frequent encounters with that gentleman at the New York Public Library, most recently just a few weeks before his death. The NYPL was his second home—perhaps it should be thought of as his primary residence, for he came to be regarded as one of its assets and was eventually provided with a desk of his own in the south Rose Reading Room.

Born in New York 12 November 1912, Shulman became attracted to puzzles and ciphers as a boy. He attended Brooklyn College, studying frequently at the NYPL. He became a member of the National Puzzlers' League and, in 1932, a charter member of its offshoot, the American Cryptogram Association. During WW II, he served as a cryptanalyst with the U.S. Army Signal Corps in Alaska.

After the war, he concentrated on critical review of the growing literature on cryptology, as well as compiling puzzles and compiling neologisms for dictionaries, all the while accumulating his own collection of books (later donated to the NYPL—where they reside, "as yet uncatalogued," according to Dr. Kahn, in the rare books room). Athletic, as a younger man, he played tennis and found time to coach a boys' basketball team. Still, his first love was words and their meanings, shared with a fascination for the esoteric field of cryptology.

Dissatisfied with existing bibliographies (including a short 1918 one by William F. Friedman), Shulman compiled his own *A Rational Bibliography of Cryptography* of more than 3,000 entries (published in a 400-page photo edition by Garland in 1976). Although much has appeared since that time, "no work has superseded his early entries," Dr. Kahn has noted. His work as a lexicographer drew special note—he contributed over 5,000 citations to the *Oxford English Dictionary* antedating accepted early usage of words and terms. He was hailed by the then-editor of the OED, Dr. Robert Burchfield, for the accuracy and thorough documentation of all of his submissions, and his name was recorded in volume one. Such unaccustomed notoriety brought him to the attention of the CBS television program, "Sixty Minutes," which did a segment a few years ago showing him at work in the NYPL.

ANNUAL MEMBERSHIP MEETING, 2004

the intelligence professionals as a shortcoming–had permeated the budget and oversight apparatus.) The value of NSA's support to the military has shifted from advice and support to active participation, virtually as a combatant command. And yet non-military recipients have been vocal in their praise of the support they are receiving, without realizing that they are not seeing half of NSA's potential through struggles for control or misapprehension of capabilities. "It's a whole new world," he concluded, before entertaining questions from the audience.

Thanking Mr. Black, Gen. Morrison paused to call Frank Derwin forward for special recognition. Presenting him with a replica of a cryptographic device used by the nation that once represented the greatest threat to the existence of the United States (a Confederate States army cipher "reel"), he praised Derwin's unstinting contributions to the work of the Foundation, especially in organizing and promoting the annual golf tournament, which has become a valued source of income.
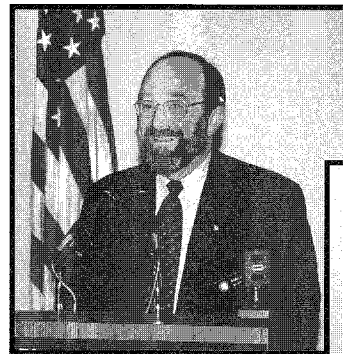
The Keynote Speaker, Mr. Lawrence C. Hale, Deputy Director of the National Cyber Security Division in the U.S. Computer Emergency Readiness Team of the Department of Homeland Security, brought a different sort of perspective to the challenges (and opportunities) facing the Federal government...and NSA. Coming from the FBI himself, he noted that 22 agencies had been combined in the new Department, with all of the complexities that entails, not the least of which was overcoming "cultural inertia." His charge was "to secure cyber space," and he had come to rely on NSA, with an Agency representative as a close team member. Dealing with "break-ins" to steal such things as Social Security numbers and identification, and to draw on bank accounts, weren't familiar targets to the NSA of the past, tightly constrained to avoid involvement in law enforcement, as opposed to "national foreign intelligence." But post-9/11 laws, such as the Patriot Act, the Government Information Security
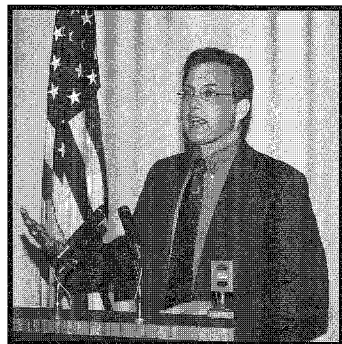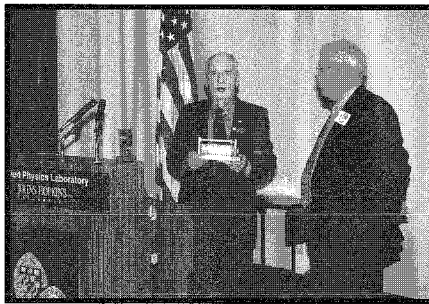
Reform Act, and the Federal Information Security Management Act are facilitating the government's ability to counter such criminal and terrorist-associated manipulation. Considering only the array of defenses an individual has, in the use of a personal computer or connection to the Internet, Mr. Hale recounted the technical and non-technical bulletins issued under the National Cyber Alert System, and the commercial firewalls, pop-up blocks, anti-virus protection, "spyware" protection, etc. now available. He drew on his personal experience with a family member to illustrate the educational or indoctrination task he confronts. He told of setting up a one-year virus protection program on a home computer, only to find it still in use, unchanged, un-updated, two years later. His term for ignoring basic security practices, updates, patches, etc., was "skinny-dipping in the Internet."

As he discussed his work, Hale cited various agency operations centers that had been established, but that tended to remain narrowly focused. Efforts had been made to get them more broadly concerned with the national perspective, to develop staffing rotation and to secure exchange communications to facilitate the growth of trust. Against the old concept of "completed staff work," he cited reluctance to report incidents until they had been thoroughly studied and dealt with—"tidied up." Instead, the emphasis was now on sharing fragmentary information from the outset. (To some hearing his words, the "lessons learned" from the Pearl Harbor investigations must have come readily to mind.)

After a break, and an opportunity to view hall displays of devices and other means of securing communications and computer transactions, the program resumed with remarks by Mike Jacobs, a former NSA deputy director for what is now termed Information Assurance, and his introduction of his former deputy and successor, Mr. Daniel G. Wolf. Wolf's presentation began with a review of the traditional concepts familiar to many in the audience and the modern replacements that had come as a result of technology and technological challenges. As recently (in the minds of some) as "the Viet Nam
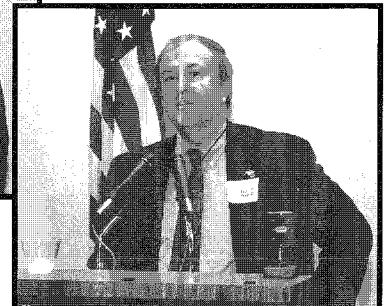
ANNUAL MEMBERSHIP MEETING, 2004

Continued from page 3

era," cryptosecurity thinking had centered on "a radio-plus-comsec." Tens of pounds of added weight was the result. "Security was an under-funded after thought," he said. By contrast, the explosion of information exchange, the "netted world," with its capacity and its speed of change, had produced a "global information grid" and required that "Information Assurance" be addressed at the outset of planning, and not be an afterthought or placed in an advisory role. Some crypto devices and components were up to thirty years old. They had to be replaced. New algorithms had to be developed. Reliable chips required a "trusted foundry." Users were frequently found to be naïve or complacent—the old, old story that anything inconvenient tended to be ignored or overlooked and left unprotected. The old "NTK–need-to-know" principle has now been replaced by "NTS—need-to-share." Cell phones, "Blackberrys," secure Internet access, Internet telephone exchanges, authentication—NSA no longer has a monopoly in addressing communications and computer security.
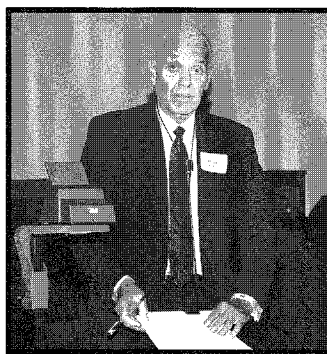
Wolf cited connectivity, speed, and reliability as the driving requirements, and noted that "the shackles of our culture may be the most daunting challenge." He quoted NSA Director Hayden as having remarked that "change is the only thing that's permanent." He concluded with an impressive accounting for accomplishments over the past two years.

Foundation Vice President Gene Becker then presented a review of the work of the NCMF over the past year, highlights of which have been covered in The Link, but he also reported on the financial posture. He noted that 19% of our outlay of funds had been for direct museum support and for education, and he cited specific acquisitions.

Morrie Cove, Program Manager of the popular "a.k.a. Smart" program developed with NCMF sponsorship by CLP, Inc., provided an update on the continued feedback of positive reactions to the "All Kids Are Smart" approach to introducing math learning and exposure to cryptography through competitive computer games at the K-to-12 school levels. Parents, teachers, and school administrator alike have praised the approach, and more than ten new inquiries had been received, including from Anne Arundel and Baltimore counties in Maryland
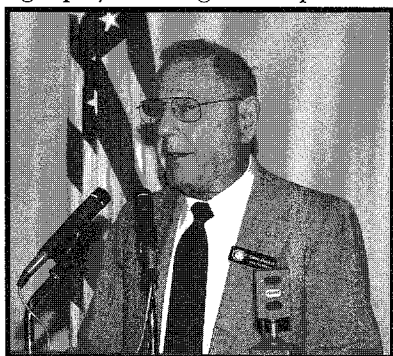
and Fairfax in Virginia. Pacing guides and text books were being produced. Mr. Cove echoed some of the remarks of earlier speakers, when he noted that the cyber world was requiring a "cultural change for teachers," partly to keep up with their students. The program has been offered free to the school systems, within the limited resources available to CLP, and the funding for wider application or adoption remains the principal constraint.

National Cryptologic Museum Curator Jack Ingram delivered a report on the operation of the Museum that was impressive in its numbers, especially in light of the disruption of ease of access for visitors caused by the on-going road construction over the past year. Some 55,645 counted visitors had been tallied, with 62 VIP visits. There were 78 school visits, 18 Scout groups (probably reduced by the reduction in Saturday openings), 413 scheduled tour groups, 397 "walk-in" tours, 19 media visits, and 50 social occasions or dinners in NCM facilities. The two Museum conference rooms were used 402 times, mainly for NSA purposes, but by some touring groups. Special exhibits had been mounted during the year on Women in Cryptology and the role of foreign language knowledge, citing some outstanding individuals from the Agency's work force. PURPLE and MAGIC displays had been re-done, and a telephone relay switch related to PURPLE had been incorporated. (Frank Rowlett had retained one of the switches of the type discovered to have been used by the Japanese, and one day his son had brought it to the Museum to Jack Ingram, saying "Dad said to give you this—that you'd know what it was.") A "Golden Age of Radio" exhibit featuring "code rings," and other cryptographic devices once offered as incentives and premiums to clubs and fans, has become a popular stop for visitors.

A projection of the "museum of the future" was presented by Steve Zigler, AIA, of the Baltimore architectural firm of Zigler/Snead. He recounted how enthusiasm had grown in his firm as more had been learned about cryptology, and the relationship they had come to find between some of the principles of cryptology and architecture, aspects they had incorporated into the design. Among other features, the proposal envisions three times the present exhibit space and three times the present library space (in part to accommodate the David Kahn Collection).

ANNUAL MEMBERSHIP MEETING, 2004

Continued from page 4

The program concluded with Mike Jacob introducing his prize—the Flowers family, a father (Earl) and his two sons (Ronald and Russell) who, together, represented 110 years of service in crypto engineering, design, and application. Earl Flowers, whose service began with the Army at Arlington Hall Station in 1942, presented a fascinating review of wartime efforts at AHS, still proud of the accomplishments of "simple times and more limited means" in days of teletype, telegraph, telephone...and (risking groans from the audience) "tell-a-woman." He described how, in the late 1930s, "cipher machines" were introduced to supersede the hand-held, paper-and-pencil, books and one-time pads of earlier years. With easy familiarity he recalled the M209 "converter" for tactical forces, adapted from a design by the Swedish inventor Boris Hagelin and produced in a volume of some 50-60,000 units (at a cost of about $135 each) by L.C. Smith and Corona typewriter companies; the M134C SIGABA, an off-line machine with 10 26-point rotors, used for top echelon to divisions or special units, produced by the Teletype Corporation of Chicago and believed never to have been "read;" the M228 SIGCOM (also produced by TTY Corp.) for on-line wire or radio teletype; SIGCOT, a one-time tape system used with SIGCOM, and the massive SIGSALY, developed by Bell, with its 12 terminals costing a million dollars each and weighing 55 tons each, requiring ten 10-ton trucks for transport. Bell's SIGSALY, Earl emphasized, represented the first use of digital technology, a milestone paving the way for modern technology. As the first voice security system used by the United States, he said, it was "the only voice security other than the Navaho codetalkers" used by US forces in WW II. He considered it to have been the largest, most complicated, and probably the most expensive cryptographic machine ever produced. [A mock-up of a SIGSALY terminal is a feature of the Information Assurance area of the National Cryptologic Museum –ed.] He briefly described other efforts— SIGDIP, Bell's analog approach, using time-delay scrambling, intended to provide push-to-talk secure service to pilots, but rejected by the pilots because of the speed/reaction time essential in combat situations;
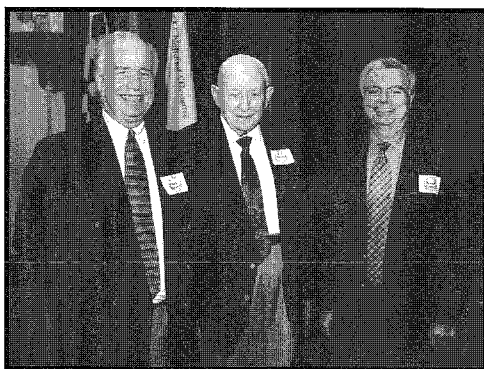
M325 SIGFOY, developed by NCR, Dayton, with rotors, pluggable lighted keyboard, hand copied from a second light (à la Enigma) but never produced or used; and SIGWIN, developed near the end of the war by TTY Corp., in a first attempt to integrate teletype and voice in a tactical environment—also never produced or used.

Here Mr. Flowers paused to note that the Army, at the time, had no R&D, that it depended on private industry, and that private industry had done an outstanding job for the Army and the nation, with timely response and the very best brains, but off-the-shelf technology and no time to develop "mil spec" equipment. As a result, the Army decided to develop its own in-house R&D in late 1946-'47, and the workhorse KL-7 for high speed printer was its initial product, "the last rotor machine used by the US." These years from 1950 to 1970, Flowers termed "the Golden Years" of crypto-development. Transistors–solid-state technology- -were coming in, leading to large scale micro-chip use. Traffic flow, with simpler operation and improved reliability was tackled, to produce continuous on-line security and improved reliability. Products included the KW-7 and KW-26, the KG-13 key generator, the KY-3 for high-level, broad band voice, the interoperable family of KY-8/-28 (air)/-38 (manpack) for tactical voice, used in Viet Nam, and the KI-1A secure Identification Friend or Foe (IFF) used by aircraft, ships, and tanks. Following his father, Ron Flowers, now in the private sector after having spent 26 years working in the field of "space" COMSEC, traced from the Soviet launch of Sputnik in October 1957 and the US Explorer 1 in January 1968. He discussed the KI-5, -4, -2, the KG-28 and -29 and support to the National Reconnaissance Office (remarking how strange it still seemed to say "NRO" in an open forum, after decades of guarded mention). He discussed the developing technology, with VSLI, embedded chips, and requirements in support of communications satellites, ending with the KI-37 launch on MILSTAR.

Younger brother Russ Flowers, still working at NSA, picked up with the current Information Assurance evolution, and the driving considerations since 9/11, such as support to trans-national groups, the challenges of "ID theft," and "asymmetric warfare" (which he likened to "jets compared with flying carpets"). He touched on the transformation underway, with the crypto modernization initiative and the challenge of "programmability"—the ability to reprogram crypto protection quickly.

What an ending for the day! And what a stellar array of speakers and insights was offered.

The Link

Page 5
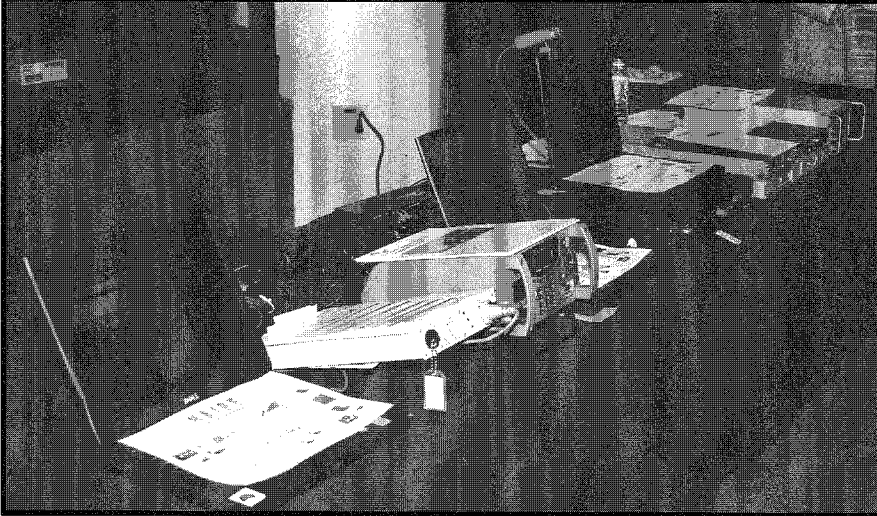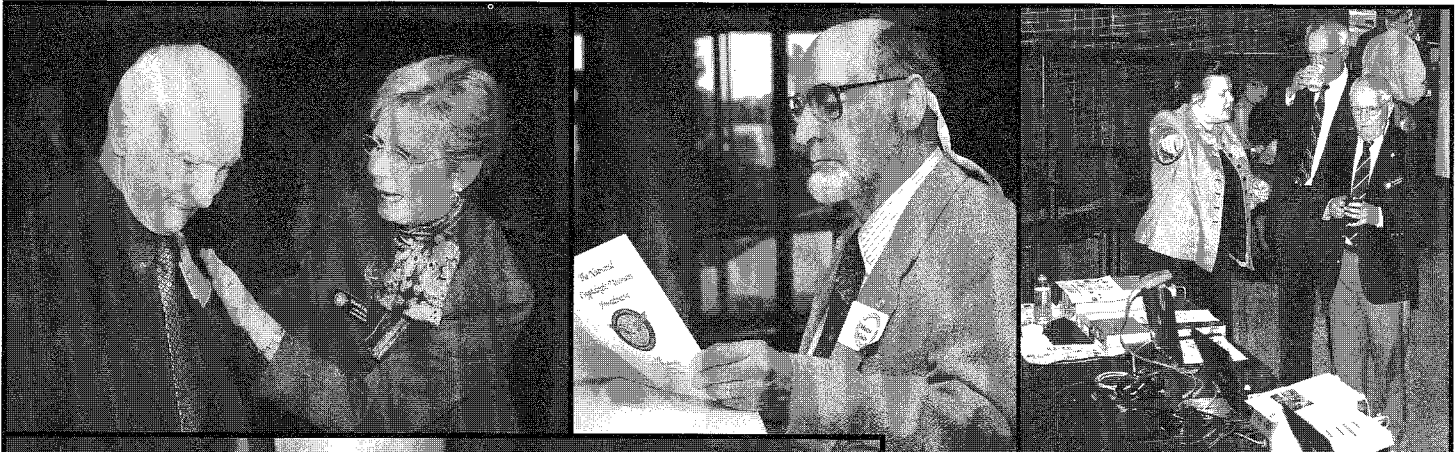
2004
ANNUAL
MEETING
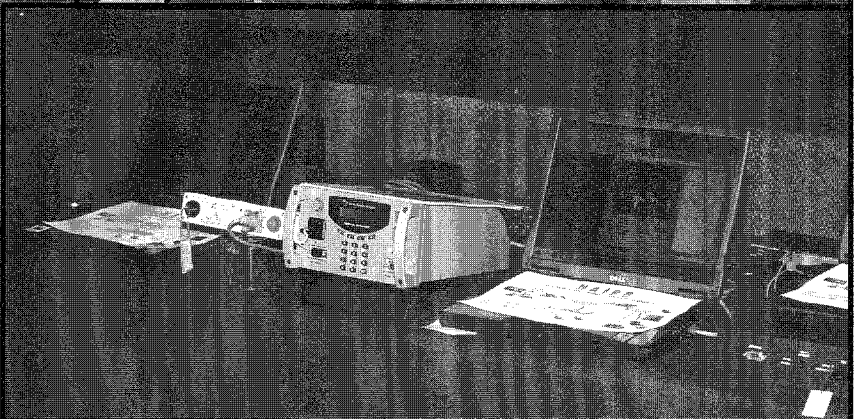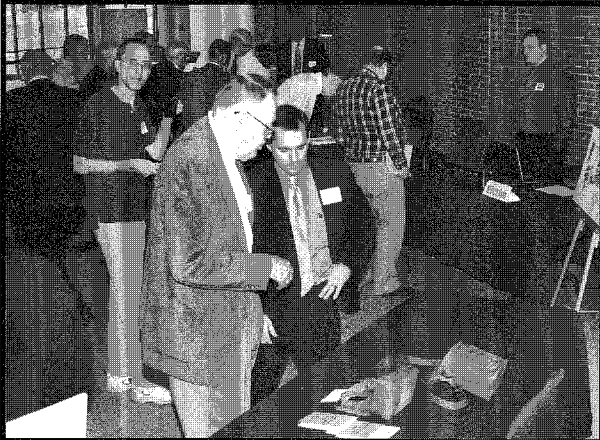
A PERSONAL TRIBUTE TO ART GREEN

By Jack E. Ingram, NCM Curator

I first met Arthur (Art) Green, in early April 1993, when he and another NSA graphics technician Douglas (Doug) Parks, were sent over to the museum to help design and then fabricate exhibits for the new National Cryptologic Museum. Then curator Earl J. (Jerry) Coates and I had been given just three months to be ready for a mid July opening.

Jerry and I would give Art and Doug a sketch or verbal outline of what we had in mind for each of the nine exhibits we were to put in, and show them the artifacts that would be displayed in each one. We would discuss the exhibits one at a time and arrive at a mutual agreement for each one. They worked quickly but most of the time Jerry and I managed to stay one exhibit ahead of them. Although Art had set up a work shop in our storage area, they would often disappear shortly before lunch and return a couple of hours latter or the next morning with something they had fabricated over in the main graphics shop.

My favorite memory of crafting those early exhibits took place while working on the Enigma Exhibit. We had a list of 96 U-Boats sunk by the US Navy, after the location of the target had been derived from Enigma intercepts. Jerry and I really wanted to make it stand out but were afraid all the Enigmas on exhibit would overshadow the list if it were in one of the crowded display cases. Art suggested a U-Boat conning tower with the list superimposed on its side. We agreed and he left for lunch over at HQs. About three hours latter Art returned with a conning tower made of grey felt and foam core board with the information neatly printed on its side. It looked great and to this day it is still a part of the Enigma exhibit.

Jerry Coates retired at the end of January 1994 and I became Curator. Over the next eleven years Art Green and I designed and installed over thirty exhibits. Of course Art would occasionally have help fabricating an exhibit (especially in typing the content) but by in large he did most of the work. Usually I would sketch my ideas and then Art and I would bounce ideas around for a few minutes and quickly arrive at what the exhibit would look like. A good example of this is the NSA 50th Anniversary Exhibit. We stood in the entrance lobby where the exhibit was to be and sort of thought out loud to each other. I had some ideas I wanted incorporated, including the red, white and blue colors and how I wanted the main captions to look. With-in about ten minutes we came up with the complete design concept. Art took some measurements and went back to his shop to begin the fabrication process. The result was a visually stunning exhibit with a lot of information including a continuous play video on the history of NSA.

One exhibit in particular had me stumped for a design concept. I was tasked to put in an exhibit on the Battle of Midway, but there was not much space available for it and I could not come up with anything I liked visually. I went over to talk about it with Art, telling him I was dead in the water for ideas and frustrated. Just then he was called over

ACQUISITION OF HARRIS BOOK COLLECTION

As recommended by Board member David Kahn, the Foundation purchased the personal collection of books on cryptology and espionage accumulated over the years by Barbara Harris of New York. Ms. Harris, a brilliant amateur (in the best sense of the word) cryptanalyst and active member of the American Cryptogram Association (under the cryptonym, YUM YUM) is moving into a retirement home without space for her beloved book collection. These were acquired by the Foundation to backstop the NCM Library holdings. Ms. Harris was attracted to cryptography during WW II, while a student at Brooklyn College, where she was introduced to the subject by mathematics professor Jack Levine's superb introductory course. (His three-volume mimeographed text is included in the collection.) Citing just one of her accomplishments, Dr. Kahn recalled her solution of a cryptogram found by Che Guevara biographer James Daniel and brought to him for solution. Dr. Kahn passed it to Ms. Harris, who broke it—an encipherment sheet in which a numerical plain text was added to a one-time key—for inclusion in Daniel's 1970 *Che Guevara: A Biography*. The collection will be inventoried and accessioned as time permits.

REMEMBERING BRITAIN'S PETER TWINN

David Hamer – NCMF-BP Liaison Officer

Peter Twinn, who has died aged 88, was the first mathematician recruited as a codebreaker by Britain's Government Code and Cipher School (GC&CS) – precursor to today's Government Communications Headquarters (GCHQ), the UK counterpart of the U.S. National Security Agency. Later he was credited with being the first British cryptographer to break an Enigma cipher – a statement that embarrassed him.

Recruited from Oxford University early in 1939, Twinn worked for GC&CS in its London headquarters with Dillwyn "Dilly" Knox, then GC&CS' Chief Cryptographer, who at that time was attempting to break into the Enigma cipher system. Twinn transferred to Bletchley Park when GC&CS moved out of London later that year - a precautionary move in anticipation of the imminent outbreak of war. He worked with Knox and later Alan Turing on U-boat Enigma traffic.

Peter Frank George Twinn, the son of a senior Post Office official, was born at Streatham on January 9 1916. He attended Manchester Grammar School and Dulwich College, before going up to Brasenose College, Oxford, to read Mathematics. He was pursuing a postgraduate scholarship in Physics when he was recruited by GC&CS. Twinn recalled that until that point codebreaking at GC&CS had been the domain of classicists who "...regarded mathematicians as very strange beasts indeed, and required a little persuasion before they believed we could do anything practical..."

Twinn took charge of the Abwehr Enigma section in early 1942 following the death of Knox. Its work was of particular importance during the 'Double Cross' deception operation that helped to ensure the success of the D-Day landings. He contributed a chapter, 'The Abwehr Enigma', to the seminal work on Bletchley Park, *Codebreakers* by F.H. Hinsley and Alan Stripp, published by Oxford University Press in 1993.

Peter Twinn, who died on October 29, is survived by his wife Rosamund, whom he married in 1944, and by a son and their three daughters.

MEMORIAL REGISTRY

The following names (and their sponsors) were added to the Memorial Registry book:

53. Honoree: William O. Marks
    Sponsors: Benjamin N. Hoover
    Richard J. Shaker

54. Honoree: Walter G. Deeley
    Sponsor: Anonymous

55. Honoree: Francis X. O'Connor
    Sponsor: Mr. & Mrs. Benjamin N. Hoover

FOR THE BOOKSHELF

ENIGMA: How the Poles Broke the Nazi Code, by Wladyslaw Kozaczuk and Jerzy Straszak. New York: Hippocrene Books, Inc., 2004. 163 pp., illus, appendices. $22.50 + s/h. ISBN 0-7818-0941-X.

In what turned out to be his final contribution to the ENIGMA story, the late Dr. Wladyslaw Kozaczuk, former colonel, historian, and publisher, whose specialty was the Polish role in the exploitation of the German cipher machine of World War II, joined forces with Jerzy Straszak (a Polish naval intelligence officer in Britain during the war, and who had first-hand knowledge of that effort) to produce this small, but fact-filled book to correct misimpressions and set the record straight. His earlier (1967) *Bitwa o tajemnice (Battle for the Secrets)*—never published outside of Poland– was the first to reveal that the Poles had successfully broken ENIGMA before the war. Not simply derived technical information—which in itself could have been worth its weight in gold—but had produced actual working models of the crypto-machine. These were turned over to French and British counterparts, along with complete instructions on how the machine worked, the "bombe" concept, key recovery with perforated paper worksheets, and other technical information. For a variety of reasons—Cold War state secrecy on both sides, bureaucratic egotism and national pride—Kozaczuk felt that the truth had been suppressed or distorted, to the disadvantage of the Polish pioneers, and he set out to correct the record.

(Consulting Prof. Z.J. Kapera, editor of *Enigma Bulletin,* for Col. Dr. Kozaczuk's obituary, we received such an informative response that it is printed below, with permission.)

The first part of the book traces "Enigma Before 1940," much of which will be a revelation to U.S. (and perhaps British) readers for whom names such as Marian Rejewski, Jerzy Różycki, and Henryk Zygalski aren't exactly the "household words" they should rightly be. These are the brilliant young mathematicians, invited to join the ranks of the small Polish Cipher Bureau in 1929, who worked the miracle. (While British cryptology appears to have clung to the classical, literary recruits—see the tribute to Peter Twinn, their first crypto-mathematician, hired in 1939, elsewhere in this issue—and William Friedman had sought disciples with a combination of math and foreign language in the early 1930s, the Poles seem to have first appreciated the elevated role of mathematics as manual cryptography was giving way to machines during the end of the previous decade.)

The "gift package" referred to above was the Polish contribution to the Franco-British treaty commitment to rush to Poland's aid in the event of invasion, and it took place a few weeks before that unfortunate event in 1939. But a team of Polish cryptologists escaped to work covertly with the French, staying just ahead of the Germans, and even moving forward to Algeria, before eventually evacuating to England. (Returning from North Africa to France in January 1942, cryptanalyst Jerzy Różycki perished at sea.)

Whatever the reason—and the case may remind Americans of the treatment of the brilliant Cdr. Rochefort by the U.S. Navy—Polish cryptologists were marginalized by the British effort, excluded from the Bletchley Park effort and kept out of Enigma exploitation. This forms the second part of the book, "Enigma in Great Britain: Ultra." At war's end, Rejewski returned to Poland, leading a quiet, scholarly life, while Zygalski remained in England as a teacher. (He died in 1978.) The names of these men finally emerged with the spotlight on Enigma exploitation popularized by Winterbotham (1974) and French cryptologist Bertrand the year before. Senior, and the most accomplished of the trio, Rejewski was able to receive some public recognition for their accomplishments before his death in Warsaw on 13 February 1980.

Given the Cold War climate that had helped to conceal the Polish record in WW II cryptology, a Polish commemorative stamp issued in 1983 hailed the work of these three men. And a decade later, in the aftermath of Solidarity, the fall of the Berlin Wall, and the collapse of the Soviet bloc, the curator of the National Cryptologic Museum "stuck his neck out" and quietly, but proudly, hung a framed copy of the stamp on the wall of the Museum as a salute to the "Grand Masters."

The book is complemented by six appendices drawn from Dr. Kapera's *Enigma Bulletin* and over 60 photographs, most of them previously unpublished. Notwithstanding its sub-title, this is not a highly technical "how to" book, but a concise and straightforward account that holds the reader's interest and relates incidents that have largely escaped Western attention before. It belongs on the bookshelf of both historian and cryptologist.

■

COL. DR. WLADYSLAW KOZACZUK (1923-2003)

By Dr. Zdzislaw J. Kapera

Jagiellonian University

Born in the small village of Babiki, Sokólka district, in northeast Poland on 23 December 1923, as a boy of sixteen, Kozaczuk found himself in the Russian-occupied part of Poland. After the July 1941 German Blitzkrieg, instead of being in school he had to work on a farm, and later on the railroad, to avoid being taken to do forced labor in Germany. He cooperated with the Soviet partisans. In October 1944 he was conscripted into the Polish Army, and spent a half-year at a military school in Lublin, receiving the rank of lieutenant in February 1945. For five years he was in the Ministry of Interior troops, fighting both Polish and Ukrainian post-war underground (i.e., anti-Communist) forces. In 1951 he entered Warsaw University as a non-regular student and in 1956 he received an MA at the Department of Polish Philology. A talented officer, with knowledge of several languages, he spent the year 1954-55 in Korea and 1957-58 in Vietnam. His connection with the army and the Interior Ministry ended in 1969. His last post was as deputy chief of the Department of Training and Analysis at the WSW (Army Counterintelligence).

Interested in historical research, and a member of a seminar at the Institute of History of the Polish Academy of Sciences, he was transferred at his own request to the *Wojskowy Instytut Historyczny* (Military History Institute), where he was promoted to the rank of colonel in 1973. At the WIH, he was (until 1980) associate professor at the Modern (post-1945) Military History Section. He was a highly esteemed expert on the German army in the twentieth century, and on the achievements of the special forces. His PhD dissertation, defended in 1978, was a monograph on "Wehrmacht, 1933-1939." (This has appeared in book form in four editions, to date.)

Col. Kozaczuk was not only a professional soldier, but also a talented and prolific writer. His name will be forever connected with the publicizing of the greatest achievement of pre-war Polish military intelligence. In 1967, seven years before the release of books by G. Bertrand and F. Winterbotham, Kozaczuk had already announced to the public (in his history of Polish military

intelligence in 1922-1939) that the Poles had broken the Enigma as early as the 1930s. (See his *Bitwa o tajemnice. Sluzby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939* [The Battle for Secrets: Polish and German Military Intelligence Services, 1922-1939], Książka i Wiedza, Warszawa, 1967, pp. 124-128. The book has had several editions, all corrected and amended, the last in 1999.)

The problem of military radio communication interested him very much. His 1979 monograph, I. W. kręgu Enigmy [In the Circle of Enigma], Książka i Wiedza, was revised in a second edition in 1986, in a total of 140, 000 copies. It had a number of foreign editions, each of them changed and brought up to date—an East German edition (*Im Banne der Enigma*, Militärverlag der DDR, Berlin, 1987); an American edition with numerous supplements (*Enigma: How the German Machine Cipher was Broken and How it was Read by the Allies in World War Two*, University Publications of America [Washington], 1984, two printings); and a West German edition, (*Geheimoperation WICHER: Polnische Mathematiker knacken den deutschen Funkschlüssel „Enigma,"* Bernard & Graefe Verlag, Koblenz, 1989, plus reprint.) His last publication, *ENIGMA: How the Poles Broke the Nazi Code* (Hippocrene Books, Inc. New York, 2004,) appeared posthumously. It is regrettable that Kozaczuk's best contribution on the Enigma, *Geheimoperation WICHER* has not yet appeared in Polish. He wrote not only serious historical monographs on the Enigma story, but also a popular version titled *Zlamany szyfr* [The Broken Cipher], Wyd, MON, Warsaw, two editions, original and revised one, both in 1976, a total of 200,000 copies! Besides that, Kozaczuk presented a very interesting history of radio intelligence in the twentieth century in his synthesis, *Wojna w eterze* [War in the Ether], Wydawnictwa Radia i Telewizji, Warsawa 1982, two editions.

Kozaczuk's interest in the history of Polish pre-war radio intelligence has already been mentioned. His monograph of 1967 was widely approved and opened the way for further

COL. DR. WLADYSLAW KOZACZUK
(1923-2003)

publication in the field. The ban on publications concerning the famous pre-war Second Bureau of the Polish General Staff ended. It is regrettable that his idea of coming back to the person of Rotmistrz Jerzy Nalęcz Sosnkowski and preparing his scholarly biography was never realized. Kozaczuk wrote about him only in a popular book called *Berlińska misja* [The Berlin Mission], Wyd. MON, Warszawa, 1967.

Dr. Kozaczuk wrote over twenty books altogether, a few pamphlets and a lot of articles, published especially in the 1970s and early 1980s, in connection with the Polish Enigma. Some of them became available also in German and English and are usually listed in scholarly bibliographies. He took part in some scholarly conferences and colloquia on military history; his personal friendship with Prof. Jürgen Rohwer was well known and its fruit was the German edition of *Operation WICHER.*

He was widely known in Poland among his readers, but not very popular with professional historians, especially those from anti-communist opposition circles—particularly after the rise of Solidarity. His previous military career and connections with the infamous Interior Ministry cast a black shadow on the final twenty-odd years of his life. Despite that, in an obituary written by Dr. Czeslaw Szafran, from which I have drawn („Przegląd Historyczno-Wojskowy" Vol. 5, No. 1, 2004, pp. 223-225) there is a high estimation of Kozaczuk's independence of judgment and self-reflection, and his outstanding position as an officer and historian. It is worth stressing that Kozaczuk himself kept his distance from current politics and did not engage in direct political support for the communist rule. This lack of engagement earned him critical opinions from his superiors.

As a person, Kozaczuk was kind, easy to approach and helpful to his younger colleagues. I myself came in closer touch with him when he unexpectedly recommended my name to Prof. Jürgen Rohwer, Chief of the Intelligence History Study Group in 1992, having known me as editor of *Enigma Bulletin.* Dr. Kozaczuk died on 26 September 2003.

A PERSONAL TRIBUTE TO
ART GREEN

to the main graphics office across the hall. As he walked out the door I suddenly had the whole concept just pop into my head. I wanted it to look like the interior of a ship and be as realistic as we could make it. By the time Art came back I had made a sketch. He looked at it and immediately began coming up with some great ideas. Of course it didn't hurt any that Art had served in the Navy! The result a few weeks later was a great looking display which fit perfectly into the small space available for it.

I always enjoyed going over to watch Art work on exhibits and help pick colors and text size etc. When new exhibits were in the making, I spent as much time with Art as I could manage. Together we made about thirty exhibits. Some were small and some were large, but they were all crafted with the pride of an expert. Some exhibits like the Zimmerman Telegram, even included some left over materials from Art's home projects. The great full size replica WW-II SIGSALY Secure Voice Terminal, is very popular and it was Art's idea to make it full size which made a lot of extra work for him, but it turned out better than anyone would have dreamed.

On several occasions, I stated publicly that "Art Green makes my dreams come true". Art is very proud of his craftsmanship and of the exhibits he made for the museum and well he should be. Curators from major national and international museums including the Smithsonian, have been surprised and amazed at the quality of the NCM exhibits, as have the national and foreign media and of course our tens of thousands of yearly visitors.

Art Green and I became very good friends over the years and I think it is appropriate that we both decided to retire at the same time. People say the NCM will be my legacy and while that may be true, I believe in no small way it is Art Green's legacy too, because for eleven years he really did "make my dreams come true"!

ANNUAL MEMBERSHIP APPLICATION

☐ Please begin/renew my membership in the Foundation

☐ Benefactor $10,000   ☐ Patron $5,000
☐ Sponsor $1,000   ☐ Donor $500
☐ Supporter $250   ☐ Contributor $100
☐ Sustainer $50   ☐ Individual $25

The Foundation is certified as a non-profit organization by the I.R.S.

Name _____

Address _____

City _____

State _____ Zip _____

Phone _____ E-Mail _____

Date _____

Please make your check payable to:
NCMF

The National Cryptologic Museum Foundation, Inc.

PRESIDENT
Maj. Gen. John E. Morrison, Jr.
    USAF (Ret.)

VICE PRESIDENT
Mr. Eugene Becker

VICE PRESIDENT EMERITUS
Mr. Robert E. Rich

SECRETARY
(Vacant)

TREASURER
Ms. Geraldine G. Garrett

TREASURER EMERITUS
Mr. William T. Kvetkas, Jr.

GENERAL COUNSEL
Leonard E. Moodispaw, Esq.

BOARD OF DIRECTORS
CHAIRMAN
Maj. Gen. John E. Morrison, Jr.
    USAF (Ret.)

MEMBERS
Mr. Ralph W. Adams
Mr. Eugene Becker
Ms. Ann Z. Caracristi
Lt. Gen. Lincoln D. Faurer USAF (Ret.)
Mr. Robert J. Fitch
MG Thomas J. Flynn USA (Ret.)
Mr. David W. Gaddy
Ms. Lee Hanna
Dr. Robert J. Hermann
Mr. Michael J. Jacobs

MEMBERS CONTINUED
Dr. David Kahn
Mr. James W. Pryde
ADM William O. Studeman, USN (Ret.)

ADMINISTRATIVE STAFF
Mrs. Sherri Legere
Mrs. Mary J. Faletto

COMMITTEE CHAIRMEN
Mr. William Arrington, *Finance & Audit*
Dr. Sarah L. Botsai, *PAO*
Mr. David M. D'Auria, *Acquisition*
Mr. Edward Jacobs, *Membership*
Maj. Gen. John E. Morrison, Jr.,
    USAF (Ret.), *Development*
Mr. Rodney B. Sorkin, *Facilities*
Mr. Bruce Fletcher, *Program*
Mr. Milton Zaslow, *Recognition*
Mr. David W. Gaddy, *Bulletin Editor*

CONTACT US:
(301) 688-5436 & 5437
Fax (301) 688-5619
email: cryptmf@aol.com
http://www.
    nationalcryptologicmuseumfoundation.com

MUSEUM TELEPHONE:
(301) 688-5849
Library (301) 688-2145

MUSEUM HOURS:
Monday - Friday - 9:00 a.m. - 4:00 p.m.
1st & 3rd Saturdays - 10:00 a.m. - 2:00 p.m.