Vincent Wilson, Jr.

The Callimahos Course

Theories and Techniques, Merriment and Marmalade Jars

(b)(3)-P.L. 86-36

"Through these doors pass the Agency's best cryptanalysts" reads the sign above the door of the classroom used for the Intensive Study Program in General Cryptanalysis, and this sign, like the course itself, bears the unmistakable imprint of the man responsible for both — Lambros Demetrios Callimahos. For over twenty years he shaped and conducted this course, which became the Agency's most advanced course in cryptanalysis. At the time of his death in October 1977, Mr. Callimahos had taught thirty-two classes and over 270 students.

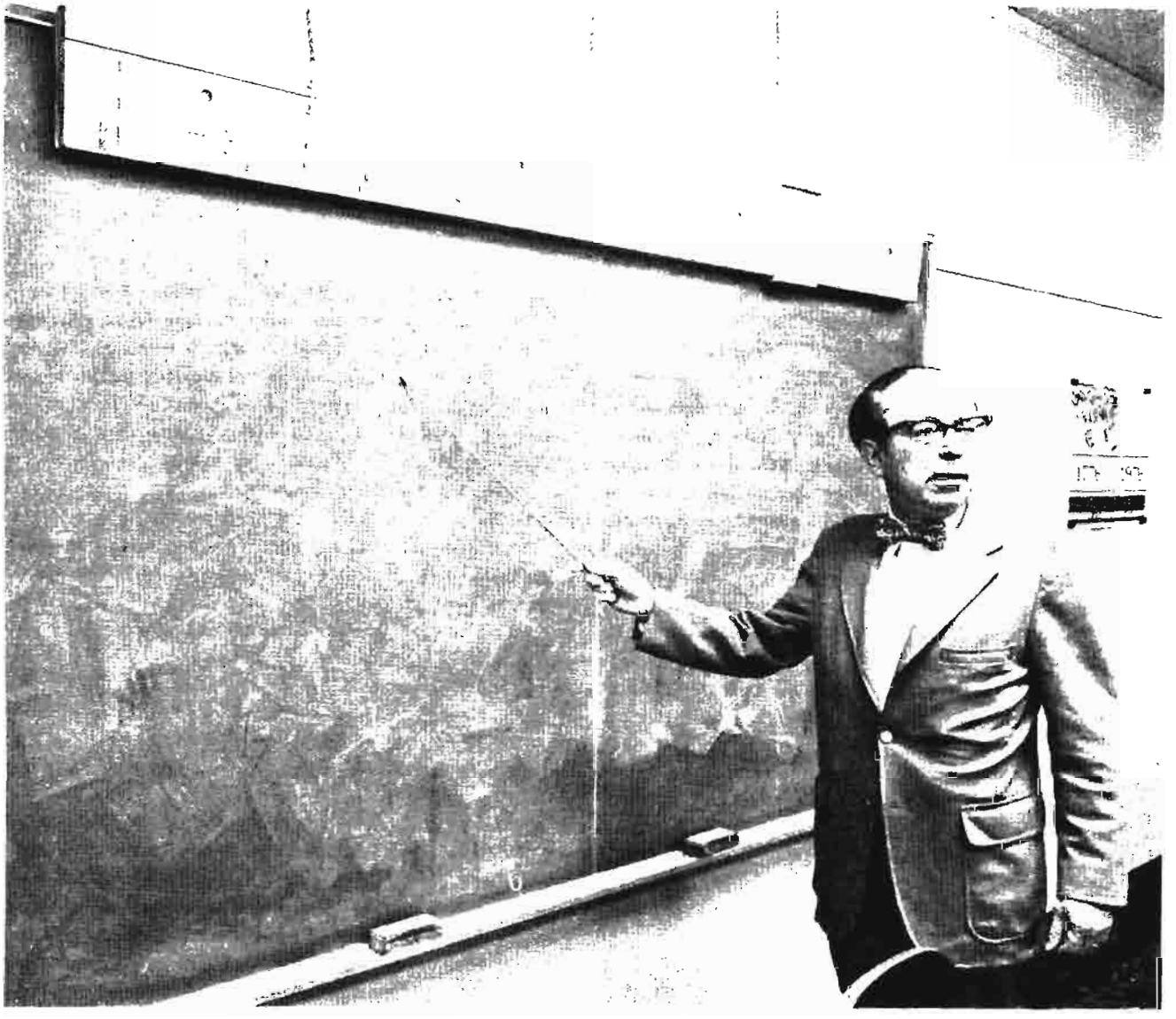
Perhaps it was inevitable that the man selected to revise and expand the textbooks originally prepared by William Friedman would eventually find himself, like his mentor before him, teaching cryptanalysis as well as writing about it. The Intensive Study Program in General Cryptanalysis is the lineal descendant of the two-year course created and conducted by William Friedman in the Army's Signal Intelligence Service during the 1930s. The examples and problems that Mr. Friedman used made up, in part, his *Military Cryptanalysis I and II*, which were by far the most complete U. S. cryptanalytic training manuals at that time. Later editions of Mr. Friedman's texts are the ones Mr. Callimahos revised and expanded into *Military Cryptanalytics I and II*.

The Friedman course of the 1930s spawned a number of specialized cryptanalytic courses which, at the more elementary levels, were further developed and widely used during World War II. But, until Callimahos began his course in the 1950s, there was no comprehensive high-level course for middle and senior analysts. As an analyst observed, "Callimahos kept the flame alive through the Agency's Dark Ages."

In tracing the history of the course, we find that it evolved with something less than a clear design from the beginning. It all started in October 1956 when Dr. William Wray, chief of one of the analytic offices, detailed an analyst to assist Mr. Callimahos in testing cryptanalytic problems he was devising for use in the textbooks he was preparing. At that time Mr. Callimahos was assigned to the Office of Training. In arranging for the analyst's detail, Mr. Callimahos later acknowledged that he quite arbitrarily chose four months, with no idea that he was setting a pattern for a formal course. The first detail proved of such value to both the analyst — Mrs. [redacted] — and to Mr. Callimahos that it immediately led to further details. As time passed, the training value of the details began to overshadow the original purpose of the first detail — to test problems intended for the textbook, and the word apparently spread sufficiently for the chiefs of other analytic offices to seek this detail for some of their analysts. Thus the number on detail — all for four months — was increased, first to two people, and in 1958 to four; shortly thereafter, the detail was transformed into a class — of six — at which time it acquired its present title.

The pattern of the course was beginning to form, but its size was not yet set. It was not until August 1963, after Mr. Frank Raven, Chief of P1, had sent a general announcement about the course throughout the Production organization, that the matter of size was settled. Mr. Raven's memorandum states, in part:

> The Intensive Study Program in General Cryptanalysis offers a unique opportunity for advanced professional training in a stimulating environment. This concentrated, 18-week Program is designed for career cryptanalysts, especially those in middle



The Guru strikes a familiar pose.

and senior grades, who wish to broaden their technical knowledge beyond the limits afforded by their operational assignments. It will enable them to gain a thorough understanding of cryptanalytic theory and applications in a wide variety of cryptosystems and thereby equip them to apply appropriate diagnostic and exploitation techniques in the solution of operational problems....I am impressed by the technical coverage and mode of instruction, which compresses an extraordinary amount of subject matter within the 18 weeks, and I therefore heartily endorse the purpose, scope, and substance of this Program.

Such a strong recommendation had a predictable result: applications poured in, and to accommodate the demand, the class was expanded to twelve students — the size it has retained throughout the years.

The flow of applications continued, and, during the period from April 1958 to October 1964, the first 19 classes followed on the heels of one another, one class graduating on a Friday and a new class starting the following Monday. This schedule kept Mr. Callimahos tied to the classroom with no time to prepare new material for the textbooks, so, beginning with Class No. 20 in 1965, classes were scheduled only once a year, from February to June.

(C) The method of teaching the course changed considerably over the years. In the beginning Mr.

Callimahos served principally as a monitor, letting the students work as much as possible on their own. Class No. 1 had few lectures and no handouts or study aids. The students covered *Military Cryptanalytics II* in eleven weeks, spending the remaining weeks on the solution of some transposition ciphers, some codes and enciphered codes, Hagelin key analysis, a wired-wheel problem, analytic aspects of traffic analysis, and elements of cryptodiagnosis. In subsequent classes Mr. Callimahos introduced handouts to reduce the time spent preparing worksheets, etc. By Class No. 29 the time necessary for *Military Cryptanalytics II* had been reduced to 15 days. Other subjects were also gradually compressed, as teaching aids were devised and improved, to make room for new material. By the mid-1970s, the course covered in four months what would have taken approximately 12 months — without the aids and partial analyses.

The aids accomplished more than simply shortening the course: they reduced the clerical labor of the student, permitted each student to progress at his own rate, and recapitulated the steps of a solution. Students in this course soon learned to be wary, for Mr. Callimahos often introduced handouts with logical

Intensive Study Program in General Cryptanalysis

Invitation to Learning

___ February 19___

WELCOME, _____!

You are now a member of Class No. ___ of the Intensive Study Program in General Cryptanalysis, the most comprehensive and advanced course in the subject offered in the Cryptologic Community. In this course you will gain a thorough understanding of cryptanalytic theory and applications in a wide variety of cryptosystems, thereby equipping you to apply appropriate diagnostic and exploitation techniques in the solution of your operational problems.

The threefold purpose of the Intensive Study Program is (a) to augment the technical background, (b) to stimulate the imagination, and (c) to instill a professional attitude. These aspects will permeate all 720 hours of the course, and will be frequently underlined in the lectures.

Although in the beginning of the course you will struggle independently, you may work as a team of 12, or any partitions of 12. You may confer freely with each other, consult any Agency elements, and have access to any machine aids in addition to those normally furnished in the course. For group discussions, you are encouraged to use the blackboard to illustrate a point to the other class members. You will feel considerable time pressure, especially at the beginning of the course; but you will soon relax and be able to assimilate the instruction at the speed at which it is conducted. The method of instruction, aided by hundreds of classroom handouts and partial analyses, maximizes the training time and makes possible the compression into only 18 weeks of what would otherwise have been a full-time 12-month course.

Understanding the text assignments is the most important consideration: problem solving is only a means of insuring understanding, or of discovering what has not been absorbed. Read over the text assignment, not too slowly; work the problems, and reread portions of the text as necessary.

Errors (but nonduplicative!) are encouraged, as they are particularly instructive to the entire class; without errors, there is no assurance of complete understanding. In other words, if you breeze through problems, you are on the wrong problems, or in the wrong course.

Aids will be furnished from time to time to reduce clerical labor and compress the instruction; but don't sit on your gluteal muscles eagerly awaiting the next gift from heaven. Do eschew pygidial lethargy.

Solution of a problem entails the recovery of all alphabets, diagrams, keys, and conventions, together with some extrapolated plain text. Do not waste time in mechanical decryption of the entire plain texts of messages.

You can now look forward to 18 weeks of sheer delight!

Guru and Caudillo

Figure 1.

mistakes or erroneous hypotheses that had been made by students in the past.

These aids, like every other element of the course, reflect Callimahos's passion for accuracy and detail, one of the marks of the premier cryptanalyst — as well as the premier musician.[1] Some of these aids (such as the "Invitation to Learning" in Figure 1) also reflect his whimsy and wit. As intense as he was about cryptanalysis and the effective application of the principles and techniques he taught, he yet had a quick and unerring sense of the humorous and the ludicrous — which often provided a class refreshing relief.

Not that a Callimahos class was likely to be boring: students were not only exposed to his wit and sometimes sardonic humor — their horizons were inevitably widened by the vast amount of information about languages, cryptanalytic inventors, musicians, exotic food and drink, extraterrestrial communications, snuff, etc. that salted Callimahos's lectures.

in the early 1970s. These monographs represented unique expository treatments of the subjects. In the foreword to Monograph 18, *"Ars Conjectandi:* The Fundamentals of Cryptodiagnosis," Deputy Director Louis W. Tordella wrote:

> This monograph represents a milestone in cryptologic literature: the first detailed and comprehensive exposition of the fundamentals of cryptodiagnosis....Any cryptanalyst, whether he has two years' or 20 years' background, will profit from the study of this pioneering work. For the experienced cryptanalyst, it is an indispensable *vade mecum*.

The monographs have been used as additional texts in the course, as well as by graduates and other professional analysts.

The materials used in the course increased over the years. By the mid-seventies each student was given over sixty books and documents comprising representative literature in the field. With the help of these aids, class lectures, and demonstrations by both the instructors and fellow students, the student worked

(b)(3)-P.L. 86-36

Mr. Callimahos lecturing the last class he taught.

After Mr. Callimahos established the schedule of one class a year, he had more time to devote to developing the examples, problems, and other materials for *Military Cryptanalytics III,* which was completed early in 1977. When the material destined to become a chapter in the book was completed, it was published as a monograph in the *Technical Literature Series*. "An Introduction to Teleprinter Key Analysis" was published in 1968, and a half dozen more appeared

his way through some 400 cryptanalytic problems in a variety of manual and machine cryptosystems. Approximately twelve weeks were devoted to manual, six to machine systems. At the end of the course, the student attacked the Zendian Problem, which consists of a volume of traffic simulating a large-scale communications-intelligence operation.

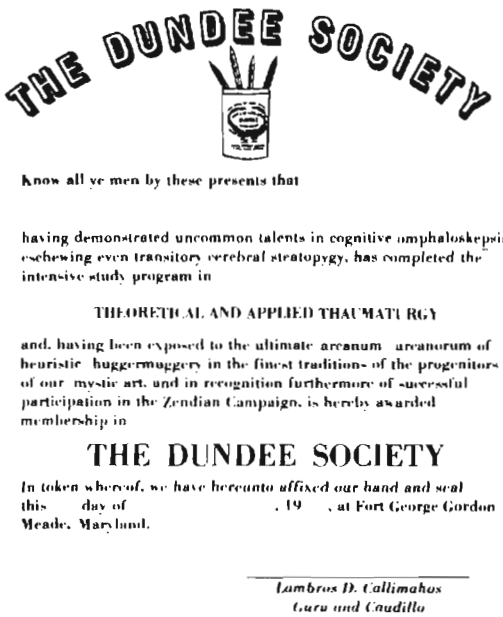
Of all the course materials, the Zendian Problem is perhaps the best example of Callimahos's almost overwhelming thoroughness, as well as his creativity. His Zendia is no Lilliput or Brobdingnag, but a country of third or fourth world rank complete with a culture

[1] Mr. Callimahos was recognized as one of the world's leading flutists in the 1930s. A short biography will appear in a future issue of the *Cryptologic Spectrum*.

and a history — and a ruler, Salvo Salasio, whose portrait bears more than a passing resemblance to pictures of the young Callimahos. This small island nation was placed in the Pacifika Ocean by U. S. Army cartographers right where God forgot to put it. There are topographical maps and maps showing the distribution of industry and agriculture. There is also a more detailed map of the Loreno province, where most of the action takes place in this post-World War II war game.

The problem includes a collection of 375 Zendian military messages (one day's intercept) enciphered in a variety of manual and machine systems. Students have the opportunity to reconstruct, from message preambles and the day's chatter, the Zendian Order of Battle. They then attack the cipher messages, and within two weeks they diagnose and solve all the exploitable messages. This is an ideal opportunity for students to practice what they have learned in the course, and to organize and manage their own team's attack against the Zendian communications.

The hundreds of graduates of the course can be found today in many areas in operations — in analytical and managerial positions — and in research and development. A number of them have reached positions of considerable responsibility.



THE DUNDEE SOCIETY

Know all ye men by these presents that

having demonstrated uncommon talents in cognitive omphaloskepsis, eschewing even transitory cerebral steatopygy, has completed the intensive study program in

THEORETICAL AND APPLIED THAUMATURGY

and, having been exposed to the ultimate arcanum arcanorum of heuristic huggermuggery in the finest traditions of the progenitors of our mystic art, and in recognition furthermore of successful participation in the Zendian Campaign, is hereby awarded membership in

THE DUNDEE SOCIETY

In token whereof, we have hereunto affixed our hand and seal this day of , 19 , at Fort George Gordon Meade, Maryland.

Lambros D. Callimahos
Guru and Caudillo

Figure 2.

Salvo Salasio, ruler of Zendia.

All graduates of the course automatically become members of the Dundee Society, next to the U. S. Senate perhaps the most exclusive club in the world. This cryptic organization owes its name to the marmalade jars that serve as pencil holders in the CA-400 classroom. The name was born out of necessity; it served as a harmless cover for the bewildering and lengthy course title when Mr. Callimahos made a reservation for a gathering of course graduates at a local restaurant.

The gathering of graduates soon became an annual event. By the late 1960s it had become a formal banquet with, each year, a mystery guest celebrity who, with much fanfare, was made an honory member of the Dundee Society. Somehow Lambros D. Callimahos became the Guru and Caudillo of the Society and, at the banquets, he played the role with mock solemnity, wearing a Nehru jacket, beads and turban. The first honorary member was Dr. Louis W. Tordella (1968); since then, the honorary members have been Lieutenant General Marshall S. Carter, USA (1969), Vice Admiral Noel Gayler, USN (1970), the Hon. Robert F. Froehlke (1971), the Hon. Albert C. Hall (1972), Lieutenant General Samuel G. Phillips, USAF (1973), Lieutenant General Lew Allen, Jr., USAF (1974), Mr. William Colby (1975), Mr. Benson K. Buffham (1976), Admiral Stansfield Turner, USN

(1977), and Vice Admiral B. R. Inman, USN (1978).

A survey of a sampling of course graduates reveals that most look back on the course as a kind of cryptologic Outward Bound — a unique, intense, and extremely demanding experience which they somehow survived while learning more about cryptanalysis, philosophy, snuff, exotic foods, etc. than they had expected. Although they consider the course an event of major significance in their professional careers, few expressed any desire to undergo the rigors of such a course again. An analyst who is also an instructor stated: "[The ISPGC] is designed to produce a professional cryptanalyst from one who is a journeyman in his field. As such, the depth of treatment is unequaled by any other CA course. The wide range of techniques covered is also unequaled. The pacing is severe but necessary."

Actually more than half of the students in some of the later classes were professionalized before they took the course. One graduate described the course as "a liberal education in cryptanalysis," another as "the most valuable asset I could possibly have in an operational position."

However variously characterized by its hundreds of graduates, the ISPGC is very much the shadow of one man. Lambros Callimahos created a course that became a minor institution in his own lifetime. As could be said of the man himself, there was nothing ordinary about his course. It was crammed to overflowing with problems, examples, jokes, stories, special tests, and other surprises, and, thanks to the Guru's passion for detail, much of it has been faithfully recorded in course plans and study aids — enough to permit his former assistant, [redacted] to carry on.

(b)(3)-P.L. 86-36