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

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

403
798

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

# *THE LEGACY OF LAMBRO*

*The Agency is very fortunate to have the legacy of Lambros Demetrios Callimahos: the course which he spent the last 22 years of his life developing and teaching. The extraordinary Callimahos course is a beautifully engineered collection of problems, writings, and ideas designed to give Agency cryptanalysts technical knowledge, breadth of experience, and a sound professional approach. Mr. Callimahos created a course which presents an overwhelming variety and volume of material to the students and at the same time fosters class and individual contribution to an unusual extent. The well-organized subject matter, colorful presentations, and the promotion of a healthy combination of competition and cooperation among his students all contribute to the Guru's remarkable success as a teacher.*

*He was completely at home with the subject matter of the course, and he had an uncanny knack for composing problems which gave just enough information to permit solution — and he was frequently able to inject some humor into the problems to keep them interesting. It was, however, his talent for inspiring teamwork among his students that I found most impressive.*

*Students would arrive at the classroom on the first day of class as twelve individuals from different organizations. They would be greeted by twelve well-stocked desks, each with a student's nameplate, and as soon as the students sat down, they became six teams of two — just by virtue of the arrangement of the desks in the room. For the next eighteen weeks each student had a responsibility to his partner, to the class, and to the course. The student who best met all these responsibilities would get the most from the course.*

*Students' responsibilities to each other included being prepared to help clarify any unclear points which might arise. This is clearly a two-way street. Let us take a hypothetical situation: suppose Yuri and Svetlana are seated at adjacent desks (how did they get in the class?). And suppose also that the class is studying* [redacted] *(a feature of* [redacted] *a portion of the course which has not yet been fully — or even partly — developed). The whole concept is unclear to Svetlana, but not so to Yuri, who explains the matter to her. She catches on but doesn't understand why the* [redacted] *Yuri had never thought of this point, so he tries to figure it out. Before he does, though, Svetlana has tumbled to the answer and explains it to him. By the time both are satisfied that they know what's going on, they have both either learned something or reinforced what they had already known.*

*Armed with this knowledge, Yuri and Svetlana attack the first problem and solve it quickly. Then they discover that they are the only ones who have the picture, so they check with their classmates to see what the hang-up is. The rest of the class is stalled because they, too, don't understand the implications of the* [redacted] *So Yuri and Svetlana go the the blackboard, and with a few deft sweeps of the chalk, they explain the solution to the class.*

*If this had been the first class to work on these problems, the Guru would have asked them to write up their solutions to each problem. The class would then have become a committee of the whole and, having appointed a scribe, would have created a report which describes the whole solution process. In this report they might have emphasized the impor-*

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 [redacted] ciphers, some codes and enciphered codes, [redacted] key analysis, a [redacted] 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

~~This article is unclassified.~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

S

# *DEMETRIOS CALLIMAHOS*

*tance of understanding the implications of the [redacted] and suggested that the amount of time required to solve the problem could be cut in half if students were given more data with which to work.*

*As this example illustrates, the course grew through class contributions. Problems were discarded because they failed to demonstrate enough new points, or because they were inordinately difficult, or for some other reason. New problems might be created to demonstrate a different technique or to show other forms of the problem. Such changes in the course were often the result of student comment or reaction.*

*The class was also a natural environment for one to develop the qualities of leadership. Typically, the backgrounds of students varied considerably. As a class started a new problem area, whoever had experience in that area became a consultant to the rest of the class and might lead the class through that set of problems.*

*Many graduates of the Callimahos course were fascinated by the wit and cultural ebullitions of the exalted Guru. This was such an integral part of the course that members of classes 17 through 20 compiled a list of 100 questions, culled from the parenthetical musings of the Guru, which any attentive student should have been able to answer by graduation day. Entitled "Dundee Society Introductory Placement Test," the list includes questions covering a wide range of subjects: mathematics, physics, history, gastronomy, music, philosophy, medicine, English, etymology, geography, language, chess, communications, cinematology, literature, and biology. Questions ranged from "What are the first 10 digits of pi after the decimal point?" to "The Anarchist Congress held in Brussels in 1914 was conducted entirely in what language?" From "Give the date when combination snuff boxes and slide rules first appeared in England?" to "What is the plural of Sphinx?" Legend has it that anyone who could pass this test needn't take the course.*

*Such facets of the Callimahos personality as the observations and parenthetical remarks that prompted these questions, gave the course a character of its own. Here was a teacher who gave instruction in snuff-taking and, on occasion, played the flute. Some classes were lucky enough to have had a flute concert to work by (at least my class did), while Callimahos, flute virtuso, practiced for one of his rare public performances. These were some of the extras — a perfect garnish to the meat of the course.*

*Much of the course is still with us in the form of mimeographs and textbooks, technical problems and papers, and recordings of lectures and even flute recitals. So students can still learn about general cryptanalysis the Callimahos way. Of such is the legacy of Lambros Demetrios Callimahos.*

[redacted]

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

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!

Carlos D. Caudillo

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.

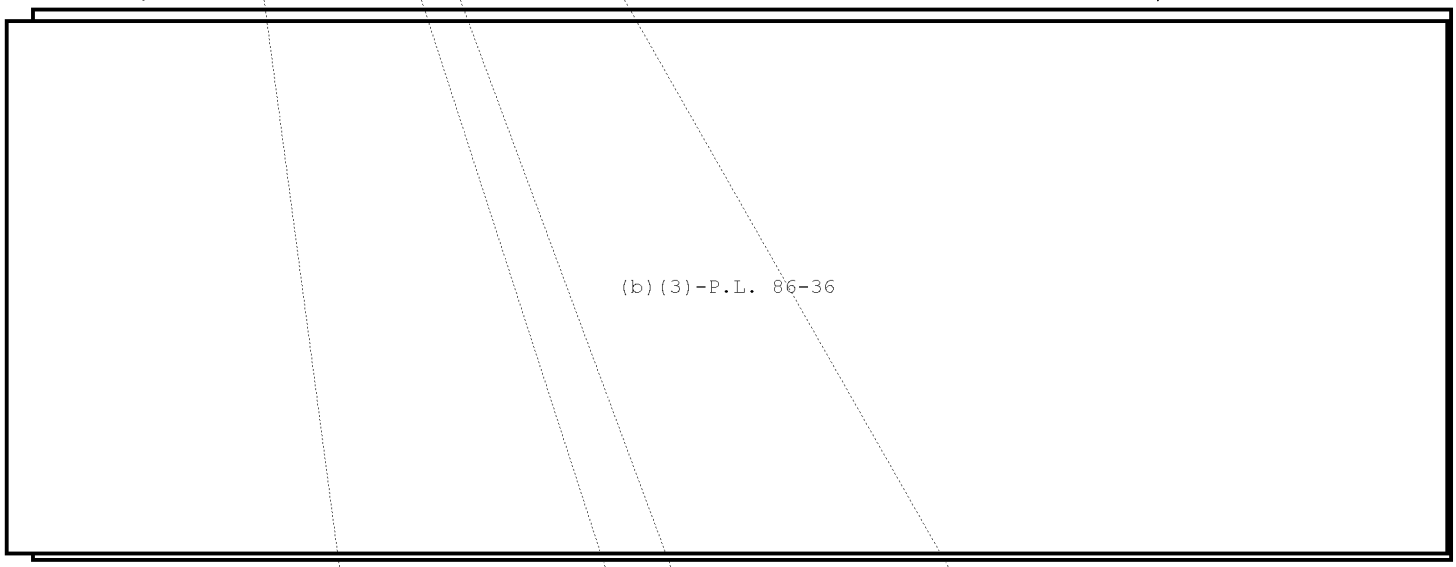
Not that a Callimahos class was likely to be boring: students were not only exposed to his wit and sometimes sardonic humor — their horizons were inevitably widened by the vast amount of information about languages, cryptanalytic inventors, musicians, exotic food and drink, extraterrestrial communications,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




**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 t[redacted] become a chapter in the book was completed, it was published as a monograph in the *Technical Literature Series*. "An Introduction to [redacted] was published in 1968, and a half dozen more appeared

his way through some 400 cryptanalytic problems in a variety of manual [redacted] cryptosystems. Approximately twelve weeks were devoted to manual, [redacted] 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*.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

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 [redacted] 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.

**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

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.*

(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 (b)(3)-P.L. 86-36 to carry on.