CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
September 7, 1995

SUMMARY

I can not tell you how much it means to me be President of the ACA. It is an acceptance by ones peers at the highest level. It took nearly 32 years to arrive in this seat. I could not be more proud. I want to put back into the organization some of the trust, knowledge and friendship afforded to me so freely over the years. I intend for this course to be my positive legacy and will work towards that end with enthusiasm.

We are taking a bold step with the first "electronic cryptography course." I hope that we can develop enough material to collate into a book (or notes) that shall be donated to the ACA at no cost. As long as I can underwrite the project, all members would have free access to the ACA 's "Course in Classical Cryptography " for their enjoyment and learning. We work as a team, we share technology as a team, we solve as a team, we succeed as a team.

As of this writing, I have received about forty five (45) responses from KREWE interested in participating. Here is my preliminary plan of action that has been approved by our EB to commence October 1, 1995:

GOALS

1) ACA correspondence course will act as an "in-depth" review of the various cipher systems. The "how to's" can be explored with an experienced ACA facilitator.

2) Classical cipher systems can be attacked in several different ways with the object of learning the basic tools for cryptanalysis as well as the history.

3) There are lots of 'entries' into cryptograms, so both student and teacher can learn together. We will publish these procedures to build a tool kit.

4) Cipher variants and special cases can be discussed as appropriate. ACA experts will be asked to help in these areas.

5) The historical significance and development of important cipher systems will be covered.

FACILITATOR

Since the class size (as of this writing) is still reasonable at (45), I have volunteered to act as an ACA course facilitator. Fifty (50) concurrent "honor" students is about my limit for the first course.

(I also teach Tae Kwon Do three nights /week plus demo team on Saturdays. CCPD has asked me to teach two Rape-Defense courses this winter, so my plate is semi-full.) LEDGE has graciously offered his expert help on the Cryptarithms section.

STUDENTS

Students will be asked to classify their classical crypto experience so that responses can be directed appropriately. There will be no tests or unsolvable challenges, just the pure intellectual enjoyment of learning the history, science and recreation of cryptography. We do not pass or fail, we improve our abilities, we become more adept, we laugh together, we grow together. We are self-directed. We attack cryptographic problems. Those who survive will be awarded a ACA Diploma as valued as any degree on your wall.

READING LIST AND REFERENCES

A reading list will be sent/published for all students. As the course progresses and we (facilitator/student) find more, then the list will be improved/updated. The reading list will be publicly available. References will be updated frequently by all to improve our practical "tool kit."

COURSE NOTES AND ASSIGNMENTS

Classical Cryptography will run for approximately a year and cover most of the ciphers in "ACA and You." The notes that we generate as facilitator/student become the property of ACA and may be published at the discretion of the EB or Editor of the Cryptogram. First rights of refusal of course materials is expressly given to the ACA. Notes, assignments {yes, I give plenty of homework and special projects} will be available on the ACA-L or from the facilitator. I have asked XAMEN EK to monitor course assignments as 'specials' to be added to member SOL totals.

COURSE EXPENSES

Expenses for course materials are the responsibility of the student. ACA facilitator efforts are complimentary.

TENETS

Some of the greatest "solves" in cryptography have been accomplished by those with little professional experience and with a different approach to offer. All levels of student are in my class, from beginner to PHD and beyond. When we write to each other or use the ACA-L list, I would ask that we endeavor to aspire to the tenets of courtesy, integrity and respect. All student questions are not only encouraged but are essential to our collective growth.

EXCEPTIONS AND SUGGESTED ACCESS

Although public key cryptography will be discussed, it is not a primary focus of this course. The course is limited to ACA members only. Students agree not to export to the INTERNET any ACA materials and to respect the copyrights of the various authors referenced. Those with access via computer and modem are recommended (but not required) to subscribe/use:

ACA-L@vm1.nodak.edu, [ACA LIST]

and Crypto Drop Box [CDB]

run superbly by NORTH DECODER and his team.

Call Dr. Metzger or E-Mail him: metzger@rs1.cc.und.nodak.edu to get details and copies of my recent papers.

Let me know what your interests are so I can plan/direct this course appropriately. You are my customers and I shall do my best to meet your needs. Let ACA help you learn more about cryptography. Enjoy the fun and pain. Persevere.

Best regards,

LANAKI

[Contact information removed]