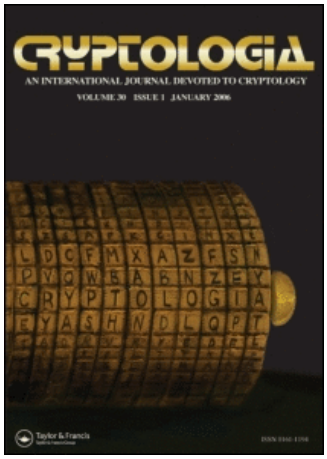
This article was downloaded by:[Winkel, Brian]
On: 11 January 2008
Access Details: [subscription number 789467472]
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t725304178

Lessons Learned from a Mathematical Cryptology Course

Brian Winkel

Online Publication Date: 01 January 2008
To cite this Article: Winkel, Brian (2008) 'Lessons Learned from a Mathematical Cryptology Course', Cryptologia, 32:1, 45 - 55
To link to this article: DOI: 10.1080/01611190701489732
URL: http://dx.doi.org/10.1080/01611190701489732

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.informaworld.com/terms-and-conditions-of-access.pdf

This article maybe used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

Cryptologia, 32:45–55, 2008
Copyright © Taylor & Francis Group, LLC
ISSN: 0161-1194 print
DOI: 10.1080/01611190701489732

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

Lessons Learned from a Mathematical Cryptology Course

BRIAN WINKEL

Abstract We present a description of a mathematical cryptology course taught to undergraduates in which cryptanalysis was a driving force. Historical discovery served to motivate student inquiry, reflection on personal analyses produced improved solutions, and projects permitted students to explore areas of personal interest.

Keywords cryptanalysis, mathematical cryptology, projects, teaching, technology

Introduction – Overview

Over the years I have taught students about cryptology in a number of ways: topics in courses to illustrate the power of mathematics in solving a hard problem, individual directed studies on crypto topics of mutual interest, and complete courses. Learning about and teaching cryptology fascinated me and was one of the driving forces for our beginning *Cryptologia* in 1977 [17]. Topics in courses included group theory in the beginning solutions of the Polish breaking of the Enigma, to polynomial algebra in the study of maximum length linear feedback shift registers, to the statistical notions of the Index of Coincidence, to programming encryption and decryption algorithms. Individual student topics included modeling the problem-solving strategies in breaking simple substitution ciphers, to learning about new parts (for me) of the subject such as hash functions while getting into modern cryptology [14], to the study and working implementation of The Advanced Encryption Standard [2].

During the spring 2002 semester at the United States Military Academy I taught a course entitled Mathematical Cryptology. The course was for any student who had finished the first four semesters of our required core mathematics: modeling with difference equations, single and multivariable calculus, statistics, and some linear algebra.

The intent of this course was to involve the students in cryptanalysis of crypto systems ranging from simple substitutions through historical systems (Playfair and Enigma) to more modern systems (linear feedback shift register encryption, RSA, and other public key systems). The purpose of such involvement was to show the students that despite the apparent complexity and claimed security, these systems had structure and hence had vulnerability if the attacker had some good analytic tools, i.e. mathematics, statistics, and programming. In the case of programming efforts I found that the students did not have good (if any) programming skills.

Address correspondence to Brian Winkel, Department of Mathematical Sciences, United States Military Academy, West Point, NY 10996-1501, USA. E-mail: Brian.Winkel@usma.edu

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

However, those who developed skills in using Mathematica (the software we use at the Academy) did gain deeper analytical results and the joy of breaking the more complicated ciphers.

We did not get into the depth in all systems that I intended. The course schedule, in the outline below, shows the flow of the course. We did not cover the Playfair system as that was introduced in a student presentation talk early in the course. I thought someone would take this up as an individual project at the end, but that did not happen.

This course was not intended to be theoretical in nature. We offered no proofs, but rather gave some intuitive or plausibility arguments to introduce results and quickly supported these with examples, being practical in introducing obtainable and easily understood crypto systems whose algorithms were succinct. Furthermore, we attempted to cryptanalyze as much as we could, because you can only be a good cryptographer if you first become a cryptanalyst, or so we – and many others – believe.

Topical Coverage

We did not really use a text, but rather I had the students buy a copy of Robert Lewand's *Cryptological Mathematics* [9] and gave the students a copy of Abraham Sinkov's *Elementary Cryptanalysis: A Mathematical Approach* [13] as resources and references to notation and approaches. I provided back issue articles from *Cryptologia*, but now with complete on-line archives for institutional subscribers I would simply refer them to search these archives for solid background material.

We introduced the students to Mathematica as a tool and we found several on-line cryptanalytic tools (including some from Lewand's text [9]) as well as methods for cryptanalysis in the texts.

We introduced notions such as the Index of Coincidence, always talking about the history – in this case William Friedman's work at Riverbank Labs in the early 20th century.

The systems and the depth that we planned to cover in this course are given in this outline:

1. Simple substitution (word breaks). Routine analysis using language skills.
2. Simple substitution (no word breaks with five letter groups). Deep coverage, with heavy use of web tools for frequency counts, pattern words, and some (but not often) presumed plaintext. We tackled mostly English, but also went after French and German ciphers, using statistics on letter counts.
3. Polyalphabetic with standard alphabet shifted, i.e. Vigenère. Deep coverage using the Index of Coincidence (IC) and other tests to "nail" the period and then using IC on shifted alphabet frequencies against plaintext frequencies to determine the alphabet shifts. This was quite successful. We assigned some classic ciphers, including a challenge cipher to Edgar Allan Poe when he was a columnist for a Philadelphia journal [18, 19], and a literary cipher (in French) of Jules Verne from his novel *La Jangada* (The Raft) [15, 5].
4. Polyalphabetic with mixed alphabets. We inadvertently assigned one of these without discussing it and it was a killer. Those that doggedly pursued it experienced great frustration. We later gave out a WWI handout discussing the strategy without addressing it in class, in the hopes that some student would pick this up as a final individual project. That did not happen.

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

5. Hill matrix encryption. Using the Sinkov text [13], we introduced this system with its modular arithmetic and the students used Mathematica to encrypt and actually busted a system using combination of trial and error (programmed) and number theory to recover the coefficients of the encryption matrix (2 by 2) when given underlying plaintext.
6. Enigma Machine. Here I faltered. We could have done a great deal more, but they were working on a long and difficult problem set and so I did not plan to go into detail. Again I thought one of them would take up the cryptanalysis of the Enigma for a final individual project, but that did not happen. However, we did cover the "weakness" of sending the message rotor setting (three letters) twice in the setting for the day and how the Polish cryptanalysts were able to extract information from this weakness. We brought the Enigma machine owned by the journal, *Cryptologia*, to class on several occasions and had them work it as well as use simulations on the web which matched perfectly the machine we had in class, a German Naval Enigma machine with five rotors for three rotor slots. Articles from *Cryptologia* on Enigma were used. Currently the journal's web site [1] cites over 325 articles with information on the Enigma. We did show them the complexity of the system with all the variations and we discussed the machine's development including its US Patent and attempts to market it in the US before WWII [8, 9]!!! In this case one of the top students in the class did a final project related to Enigma, not the mathematics or cryptanalysis, but a video web page on how to actually use the machine, step-by-step.
7. Linear Congruential Generators. We discussed their structure and then we had the BEST cryptanalysis collectively in class in this regard on a message we assigned. Basically the LCG generates pseudorandom numbers and they are added digit by digit (mod 10 with no carries) to the message which has been converted to numbers, e.g., $A = 01$, $B = 02, \ldots, Z = 26$. This analysis stemmed from a paper by Jim Reeds which appeared in an early issue of *Cryptologia* [12]. We gave the students a copy of the paper AFTER the analysis.
8. Linear Feedback Shift Register. Basically, the sequence of 0s and 1s generated by tapping the last bit off a running LFSR is used as additive (mod 2) key to the text which has been converted to base 2 numbers, i.e. $A = 00001$, $B = 00010, \ldots,$ $Z = 11010$. The object here was to show the students that despite the claims that an n register LFSR could possibly have a period of $2n - 1$, using a known plaintext/ciphertext yielding some $2n - 1$ consecutive bits of keystream (not unreasonable in the patterned messaging of the military) the system was simply a linear system of equations.
9. Public Key CryptoSystems. We laid the number theoretic foundation for the RSA system and discussed the security and authentication notions involved, as well as the revolutionary idea of "public key" systems and what would make them secure. We implemented both encryption and decryption in Mathematica. We never attempted any RSA cryptanalysis, not even for small number systems.

The students cracked a table cipher from the Hayes-Tilden Presidential Election of 1876 [7, pp. 221–229]. We had presentations on non-technical items such as the Zimmerman Telegram and the VENONA project (the post WWII ciphers from Russia which the USA was reading, but not always busting), and other areas. See Projects below.

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

In addition to the cryptanalysis we had several sessions of "story telling" based on my own experiences as an analyst at NSA in the 60s, my own life-long interest in cryptology, and my editorship of *Cryptologia* for these 26 years at that time. All of this was to show them the uncertainty in this field and yet the power of analysis (i.e. compute brute force attack numbers AND artful cryptanalysis). We shared with them several personal copies of "rare" materials such as original Riverbank Laboratories cipher manuals, e.g. [4, 3]. We had several readings and discussions on topical issues. In particular, we discussed at length the touchy issue of open cryptography vs. government control. The students finally concluded we will have open crypto and our society will have to live with its consequences, i.e. VERY difficult ciphers used by the "bad guys."

The class was always open to questions, more detail, jumping about. We changed the schedule to suit our interests and to reflect the hardness of material and notions presumed easy by the teacher as well as the emerging interests of the students.

Evaluations

Basically I asked the students to submit a sort of stream of consciousness as to what they were thinking (or not thinking!) as they tackled their ciphers. This led them to write up some fascinating material on paths leading to dead ends, inspiration, hints, solid analysis, some "Eureka," and great satisfaction upon success. Of course, in this stream they demonstrated the solid analysis for success. They never balked at writing up this analysis, for just submitting the solution did not let them show off as to how they got it.

Points were assigned for each problem and for projects – there were no exams – and then totaled for the final grade. Since these students were tough, tenacious, indeed, survivors, the grading scheme rewarded their efforts, hence the need for stream of consciousness presentations in their analyses, and not just their success. The grades were high, but not unduly for an upper level elective course. From the 8 students who finished the course there were 3 A+, 1 B+, 2 B, 1 C+, and 1 C.

Here is the final breakout on points, although this clarity and final resolution in homework points was NOT known at the beginning of the course.

Homework	4675
Projects	2000
Total Points	6675

Exemplary Student Work

For all assignments, students were required to render a stream of consciousness write-up on the process, blind alleys, dead ends, idea sources, and emotions as they progressed. I modeled this after the work of Newell and Simon [11] who recorded every word (thought?) of solvers of the cryptarithm SEND + MORE = MONEY in which each letter stands for a single digit number so that the arithmetic works. My goal was to get them to reflect upon their solution strategies, even as they were in the midst of the "battle." I could also see how they were progressing as the semester went on. The Top Gun in the course was Wes Loyd. In addition to high marks,

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

he was the best at sharing his thoughts during his analyses. We include one here so the reader can see just what we mean. His write-ups were the essence of analysis with the most concise reporting.

CDT Wes Loyd 2/13/02
CT Lessson 3/4/5, Problem 4

Polyalphabetic Substitution: Lesson3Challenge[1]

Cipher: `GE JEASGDXV ZIJ GL MW LAAM XZY ZMLWHFZEK EILVDXW KWKE TX IBR ATGH IBMX AANU BAI VSMUKKES PWNVLWK AGH GNUMK WDLNZWEG JNBXVV OAEG ENWB ZWMGY MO MLW WNBX MW AL PNFDCFPKH WZKEX HSSF XKIYAHUL MK NUM YEXDM WBXY SBC HV WYX PHWKGNAMCUK`

Decoded:
`MR. ALEXANDER,`

`HOW IS IT, THAT, THE MESSENGER ARRIVES HERE AT THE SAME TIME WITH THE SATURDAY COURIER AND OTHER SATURDAY PAPERS WHEN ACCORDING TO THE DATE IT IS PUBLISHED THREE DAYS PREVIOUS. IS THE FAULT WITH YOU OR THE POSTMASTERS?`

Analysis:

1. Index of Coincidence = .0455, Says cipher is most likely not monoalphabetic, Aprx. Length of keyword = 3.506 (VERY ROUGH)
2. Kasiski Test – Found difference between digraph (`MW` $= 108 = 2^2 * 3^3$) leads me to believe keyword is length 2, 3, or 6
3. Decimated IOC for 2 (.05, .048), 3 (.048, .046, .056), 6 (.047, .065, .082, .086, .052, .054), all look good, but my gut instinct leads me to believe keyword is length 6 (2 & 3 are just too small)
4. For decimated 6 alphabets, I first tried the fully automated Mathematica method (keyword = `TITESS`) that yielded no good result.
5. Next I tried the grammatical approach by trying to find a two-letter beginning with the same letter, who's last letter is the end of a three-letter word (`MK`, `MW`, `MLW`)... I tried OR/OF, IT/IF but these paths ended up leading nowhere...
6. I also tried to think of a way to begin a letter with a two-letter word I tried "To" and "Mr"neither path worked I think maybe it's a name...
7. Maybe my keyword is the wrong length? I quit again...?
8. UPDATE: CDT Acosta clues me in that `GNUMK` = `OTHER`. I tried it and got close but it only seems to make some words fit, not all of them I also think that the difference in the Lesson3Challenge.txt file and what is on CT Lesson 8 for the enciphered message, was throwing me off. (I'll just work strictly with the Lesson3Challenge.txt file)

---

[1]This was a message that Edgar Allan Poe had received in his position as columnist for *Graham's Magazine* in which he challenged readers to send him ciphers (always simple substitutions he requested) and had proven in a tight analytic paragraph that the message was NOT a simple substitution [11]. However, Poe never tried to solve it, nor did others in history until 1977 [18].

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

9. In class we discussed that the keyword is "long." I began to instantly think about step 7 above where I said that the six-letter approach wasn't working (5 hours worth) and I possibly had the wrong keyword length.
10. We pretty much decided the keyword was of length 12 (which works with my Kasiski test above). This also seems to make sense based on the trends I was getting from my six-letter analysis because only SOME definite words would appear, but others wouldn't make sense Now this should be easy
11. After plugging in the GNUMK = OTHER, we get the keyword UNIT_ _ _ _ _ _S. We get some good stuff See "MR" as first word. XYZ=_HE, try X=T ⇒ E for 11th letter of keyword.
12. Noticed "how is _ _," try MW=IT ⇒ ED for 5th/6th keyword letters Looks very good, seeing "the same" "arrives." (Keyword currently = UNITED_ _ _ _ES)
13. I see EUBZWMQY = ACCORDIN_, try Y=G ⇒ S for 7th keyword letter... Almost home... The keyword UNITEDS_ _ _ES looks like UNITEDSTATES, so I tried it SUCCESSSSSSS!!! (waaayyy too much work put into this one)

As an extra treat we asked students to write a letter to Poe in the style of the early 19th century to show Poe how to break this message, advising him of how the tools they were learning at West Point (a school that had kicked out Poe earlier in his life!) were working nicely for them in their analyses. The cadets caught on and their flowery writing style showed they had captured the excesses of the language of the day. Several of these modern-day cadets suggested (tongue in cheek) that if Poe had stayed on at West Point and been commissioned as an officer he might have been able to break the cipher.

Visitors

If one can get speakers with experience and passion about things crypto, by all means bring them into the class. They will enjoy meeting with a group of "informed" crypto studiers and your students will be ready for and appreciate their technical or historical information as well as their anecdotal stories. During the course we were most fortunate to have two speakers:

Paul Greenough, retired Foreign Service author and PhD in mathematics, had published papers on the cryptanalysis of a Swedish machine and I scheduled an evening session and a next day in class session. The students were wonderfully involved in Paul's presentation, to the point of asking the next question Paul was about to ask AND answering it!!!

Peter Wayner, author of a number of books on crypto issues and a current "best seller" on steganography [16] presented a department wide seminar, which the class attended, on steganography. This was very much appreciated due to recent issues involving Osama Bin Laden and the like, using images to hide information.

Projects

I selected a number of topics and after a written survey of their interests and backgrounds, as well as interactions in and out of class, I assigned individuals to go out and find material on assigned topics and report back to us what interested them. In some cases I provided material or direct pointers to sources. In all cases they went

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

beyond the minimum as they were drawn into the material by the same curiosity that drew them into the course in the first place. Students liked the assigned project early in the course as the instructor obtained some idea of their interest through survey and then assigned them a "fun" project.

Hoping that students would pick up on something and include it in a final individual project is done with great peril. If you step into the student's project mindset with too many specifications it is not a student project, but a professor driven presentation. Thus, if you really want to be fair to students and be sure to cover something then you better do it yourself, in class, and not depend upon them to run with it as a final individual project. Moreover, IF they do run with it as a final individual project there is no assurance that the other students will "get it," indeed, they may not be involved as we only had a 25 minute presentation for final projects in the last two weeks with no accountability.

Figure 1 lists the topics assigned to the class very early in the course as Project One and then the project topics selected by the students as Project Two. All projects had a written and an oral portion.

Project One was assigned 1000 points with 200 points for class presentation and 800 points for paper. Project Two (Individual Final Project) was assigned 1000

Project One Topics – Teacher Selected

Date	Keywords for Topic Meant to be flexible
22-Feb-02	Bletchley Park
22-Feb-02	German Enigma Machine - and ULTRA
22-Feb-02	Marian Rejewski
25-Feb-02	American - British exchanges concerning ULTRA intelligence pre- and during World War II
25-Feb-02	William Friedman the man
25-Feb-02	Zimmerman Telegram World War I cryptology
27-Feb-02	Alan Turing's contribution to codebreaking
27-Feb-02	Herbert Yardley - *The American Black Chamber*
27-Feb-02	Codes and Code issues in the movies
5-Mar-02	Transposition ciphers
5-Mar-02	Some interesting encryption issues concerning uses of Web
5-Mar-02	National Cryptologic Museum and other crypto museums
7-Mar-02	Playfair cipher
7-Mar-02	Steganography
7-Mar-02	Literature Ciphers - Sir Arthur Conan Doyle, Dorothy Sayers, Edgar Allan Poe, Jules Verne

Project Two Topics – Student Selected

1) Attempt to use permutation elements to generate cipher
2) Video/web page of actual operation of the Enigma machine
3) Investigation into Japanese cipher machine - Purple
4) Current on-line encryption schemes PGP study
5) Investigate current packet and communications protocols for communications and WWW
6) Push further on the mathematics of various public key systems
7) Write black box simple substitution bust with dictionary look-up
8) VENONA Project - what it was, what it meant

Figure 1. List of topics for two projects.

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

points with 400 points for class presentation and 600 points for paper. Project One was given 10 minutes for presentation and Project Two was given 25 minutes for presentation, hence the difference in scores.

Technology

There are many possibilities here depending upon the experience of the students, (e.g., writing in C or Visual Basic), the institution (we use Mathematica in our classes here), or the teacher. Cadets used a number of Mathematica notebooks I wrote to do some things, e.g., encipher, decipher, assist in cryptanalysis. I provided some before asking students to perform analyses in order that they see how one could do certain things in Mathematica. Other files I provided after assignments to offer one "solution" for students to see.

- Simple Substitution.nb – Enables user to encrypt and decrypt a simple substitution cipher with or without spaces and punctuation.
- ClassSimpleSubstitution.nb – Enables user to encrypt and decrypt a simple substitution cipher with or without spaces and punctuation. Gives five letter groups for cipher text.
- FrequencyContactTools.nb – Permits frequency counts of text, digraphs, and trigraphs.
- NewFrequencyCountTools.nb – Permits frequency counts of text, digraphs, and trigraphs. Also does contact charts.
- PolyAlphabeticVigenereNSA.nb – Practically an automatic bust of Vigenère using IC to determine decimation and decimated IC's to confirm and then using slides of standard alphabets and max comparisons with standard English to determine the Vigenère.
- ICV1.nb – Does almost automatic Index of Coincidence bust of Vigenère cipher.
- VerneCipherSolve.nb – Does the bust of the Jules Verne novel (*La Jangada*) [15] Vigenère cipher.
- HillSystems.nb – Covers Hill system, construction of invertible and also involutory matrices, encrypts, decrypts and cryptanalyzes the Hill System.
- MAT4EncryptDecrypt.nb – Does encryption/decryption of test message using the Hill System.
- LinearCongruentialGenerator.nb – Does the encryption and decryption of such systems.
- ShiftRegisterEncryption.nb – Does the encryption and decryption of such systems.
- RSAStuff.nb – Does the encryption and decryption of such systems.

Course Experiences – Suggestions

The worst thing I did was to start off the course with too many ciphers to work on and too much tough cryptanalysis required. My goal was to let the students experience the "challenge" of cryptanalysis without killing themselves. Indeed, I told them they did not actually need to bust the ciphers, but rather turn in their stream of consciousness analysis description that I always required and they would receive full credit if they were acting smart. I failed to recognize the tenacity and relentlessness of a student who would gain entrance to West Point. Several of these students were A to A+ overall GPA students who were taking a seventh course overload! They would not quit until they had success on these ciphers. However, such diligence took

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

its toll on them as they spent hours on these "puzzles," unable to put them down, unable to give up. Thus from a starting group of 15 I lost 7 and the class finished with 8. *Mea culpa*. If I had paced the course better at the start, asked for partial solutions after a short time, spent more time in class on the analysis to give them leading ideas for success, paid more attention to their frustration, acted wisely after the first drop, and more, then we would have retained more and they would have truly enjoyed the course, for they were intellectually engaged with the material even as they were being beaten up by the cryptanalysis.

The best thing we did was to involve the class in "public" cryptanalysis, e.g., we all got excited as we broke the Linear Congruential Generator [12] in class together, with shouts of contributions and ideas and conjectures. Terrific!!! Keeping the approach open, for we worked as a group, driven by their ideas, was a good approach. In this way the instructor did not offer a path for success, but rather tried to get the students to build their own approach, collectively in class – but certainly on their own back at their own desks.

The students made some remarkable presentations the best of which were Les Craig's impersonation of the "confident" William F. Friedman and Neil Lofland's *tour de force* of current issues in web security. Les, who was very high in the cadet chain of command, arrived "late" for class on the day of his presentation – something unheard of for such a high ranking cadet. However, he sauntered into class, saying, "Hi. Billie Friedman here to tell you how I personally saved US cryptography!" He did a marvelous theatrical presentation and opened up to questions, responding in a very confident manner about his many achievements with great detail. Clearly Les enjoyed his role playing.

The web proved an invaluable resource for much crypto work is on-line, from Enigma machine simulators, to historical material (e.g., ALL of Edgar Allan Poe's writings are on-line – compare this to finding the magazine articles in dusty libraries or interlibrary loan when I did this course some 25 years ago), to the latest technical issues.

Meeting in a room with computers to permit real-time, group work on cipher busting proved wise. Since the time of this course, all cadets possess laptops and this would make things even easier.

We gave no exams, only graded homeworks and two projects.

Course Improvements

What would we do to improve the course?

- Moderate the pace at the beginning. Make sure students are not killing themselves on homework.
- Use a text book and layout a time table syllabus ahead of time for all to see so we can measure and pace ourselves. This will not permit us to ramble and will permit us to get to new topics and some topics deeper.
- Get all students Mathematica (or whatever system one uses) literate and functioning early on in the course so that they have a shot at using the technology effectively to tackle the tough cipher material coming down the road.
- Require students to "buy-in" somehow to other students' presentations on projects.
- Have more team work. We did on occasion; certainly class was one big team. Perhaps have teams of two working on complex ciphers.

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

- Require students to encipher according to some of the algorithms and perhaps invent one of their own and analyze it for weaknesses in light of the course knowledge.
- Do more with the Enigma and its remarkable cryptanalysis in more detail. Permit the students to play with the machine we own here. We did bring it to class and explain how the Polish codebreakers started their analysis, but we should have done much more.
- Involve other security issue personnel, e.g., visitor from NSA, security personnel, other possible visitors.
- Take a field trip to the National Cryptologic Museum in Fort Meade MD. Perhaps to NSA itself.

Conclusions

This past semester a young Major taught our course in cryptology with an entirely different take on it. It was more number theoretic, with attention to needed algebra concepts as they came up. Students wrote much of the Mathematica code, but were given in-class exams which were of a pencil and paper nature while working on homework sets and an extended project. I shared my extensive End of Course notes from this 2002 course with the incoming teacher as he was "new to cryptology." It is a tribute to the discipline, cryptology, that this teacher did something entirely different than I did while preserving the spirit of teaching students about the making and breaking of ciphers. When we began *Cryptologia* over 32 years ago it was our intent to create a newsletter for the exchange of ideas among those teaching crypto courses through sharing their approach, for the open literature in the field was basically non-existent [17]. Thus, courses were a function of individual teacher's interests and experiences. There was no canonical course in cryptology to be had. Well, the good news is that now, despite a plethora of cryptologic material all around us, there *still* is no canonical course in cryptology to be had and, as such, it is an exciting course to teach, for both teacher and student learn about some of the many fascinating topics in the field due to the different paths one can take. We hope you will consider teaching cryptology or encourage and support a colleague to incorporate crypto ideas into a course, for to do so is to learn much about many topics in mathematics, about the world around us, and about ourselves and our students.

About the Author

Brian Winkel teaches and mentors mathematics and faculty at the United States Military Academy. While his formal studies were in the area of abstract algebra, early on in his teaching career he developed a keen interest in applicable mathematics to include diverse applications of differential equations, mathematical biology, engineering mathematics, and, of course, cryptology. He is the founder and editor of *PRIMUS – Problems, Resources, and Issues in Mathematics Undergraduate Studies* and founder and Editor Emeritus of *Cryptologia*. He has now taught a cryptology course in three settings: a liberal arts college (Albion College), an engineering institute (Rose-Hulman Institute of Technology), and a military academy (United States Military Academy) and he has enjoyed what he has learned in all three settings.

Downloaded By: [Winkel, Brian] At: 23:48 11 January 2008

References

1. http://www.informaworld.com/smpp/title~content=t725304178'~db=all. Taylor & Francis web site for *Cryptologia*. Accessed 7 May 2007.
2. Daemen, Joan and Vincent Rijmen. 1998. *The Design of Rijndael: AES – The Advanced Encryption Standard*. New York: Springer-Verlag.
3. Friedman, William F. *Synoptic Tables for the Solution of Ciphers and A Bibliography of Cipher Literature*. Publication No. 18. Geneva, IL: Riverbank Laboratories.
4. Friedman, William F. *An Introduction to Methods for the Solution of Ciphers*. Publication No. 17. Geneva, IL: Riverbank Laboratories.
5. Gass, Frederick. 1986. "Solving a Jules Verne Cryptogram," *Mathematics Magazine*, 59(1):3–11.
6. Kahn, David. 1967. *The Codebreakers*. New York: The Macmillan Company.
7. Kahn, David. 1993. "An Enigma Chronology," *Cryptologia*, 17(3):237–246.
8. Kruh, Louis and C. A. Deavours. 2002. "The Commercial Enigma: Beginnings of Machine Cryptography," *Cryptologia*, 26(1):1–16.
9. Lewand, Robert E. 2000. *Cryptological Mathematics*. Washington, DC: The Mathematical Association of America.
10. Newell, A. and H. A. Simon. 1972. *Human problem solving*. Englewood Cliffs, NJ: Prentice Hall.
11. Poe, Edgar Allan. 1841. "A Few Words on Secret Writing," *Graham's Magazine*, 19(July):33–38.
12. Reeds, James. 1977. "'Cracking' a Random Number Generator," *Cryptologia*, 1(1):20–26.
13. Sinkov, Abraham. 1966. *Elementary Cryptanalysis: A Mathematical Approach*. Washington, DC: The Mathematical Association of America.
14. Stinson, Douglas R. 1996. *Cryptography Theory and Practice*. Boca Raton, FL: CRC Press, Inc.
15. Verne, Jules. 1891. *La Jangada: Huit cent lieues sur l'Amazone. Paris*: Hetzel. (Translation – *Eight Hundred Leagues on the Amazon*. 1912. New York: A. L. Burt, Co.)
16. Wayner, Peter. 1996. *Disappearing Cryptography*. New York: Academic Press. Second Edition published by Morgan Kaufmann in 2002.
17. Winkel, Brian J. 1977. "Why *Cryptologia*?" *Cryptologia*, 1(1):1–3.
18. Winkel, Brian J. 1977. "Poe Challenge Cipher Finally Broken," *Cryptologia*, 1(1):93–96.
19. Winkel, Brian J. 1977. "Poe Challenge Cipher Solutions," *Cryptologia*, 1(4):318–325.