Short Course
ROTC Vail July 1921

July 11, 1921.

Dear Major Truesdell:

I am enclosing herewith a typed synopsis of the three lectures I gave last week. You will find that I have endeavored to meet with your recommendation that it be made as brief as possible. Perhaps I have gone to the other extreme and have abbreviated the outline too much. If so, please advise me, and I will be glad to extend this one.

My thanks are due you again for the very pleasant visit you enabled me to have, and for the many courtesies which you and your colleagues extended me during the whole week.

Sincerely yours,

Major Karl Truesdell,
Headquarters, R.O.T.C.,
Camp Alfred Vail,
Oceanport, N. J.

Synopsis of a course of three lectures on Codes and Ciphers, given before the students of the R.O.T.C., Camp Alfred Vail, Little Silver, N. J., July 6-8. 1921,

by

W. F. Friedman, Code Compilation Section, Office of the Chief Signal Officer, Signal Corps, U.S.Army.

First Lecture, July 6.

1. Introductory remarks. Brief historical survey of subject. Great advances made in recent years both in methods and in analysis.

2. Definitions. Cryptography. Cipher. Enciphering;Deciphering. Plain text; Cipher Text. Code. Encoding;Decoding. Plain text;Code text. Enciphered Code.

3. Comparison of advantages and disadvantages of codes and ciphers. Sharp distinction between code and cipher in modern cryptography.

4. Limitations of both code and cipher. The time element in solution most important in military ciphers or codes, because no practical system yet devised is insoluble.

5. Influence of recent rapid advance in radio on the use of cryptographic means of communication in warfare.

6. Necessity for proper training of officers and specialists in the use of code and cipher. Seriousness of results of failure to observe fundamental rules and precautions. An appreciation of this feature is to be found in a study of the principles used in the solution, or analysis of ciphers.

7. Analysis of Ciphers. Principles of Mechanism of a written, alphabetical language. Frequency tables. Proportions of vowels and consonants. Relative order of frequency of various letters, and combinationsof letters. The two principal classes of ciphers: Transposition Ciphers; Substitution Ciphers. Examples of each. Method of distinguishing. Various types of transposition ciphers. Method of Solution.

8. Substitition Ciphers. The kinds of alphabets. Cipher alphabets, normal alphabets, direct, reversed, mixed, reciprocal. Simple or single alphabet substitution ciphers. Multiple alphabet substitution ciphers. The U.S.Army Disk. Playfair.

Second Lecture, July 7.

1. Review of general principles of transposition and substitution ciphers.

2. Demonstration of the solution of a typical four-alphabet substitution cipher. Repetitions or recurrences. Principle of factoring the interval between these recurrences in cipher text. Clues to number of alphabets involved. Analysis of frequency tables prepared upon basis of the number of alphabets.

3. Summary of reasons for the simpicity of the solution. Short key vs. a long or a continuous key. Known alphabets (direct or rversed normal) vs. mixed or unknown alphabets.

4. Correction of errors. Errors in enciphering. Errors in telegraphic transmission. Errors in deciphering. Errors in copying.

5. Examples of deiphered German messages taken from one day's activity. The study of time factor in these solutions.

6. The requirements of a cipher for miltary field use. Form- suitable for telegraphy. Must not be longer than original text. Enemy can be in possession of all details of the system. Only thing kept secret is the key applying to particular messages. If instrument used, must admit possession by enemy. Method of encipherment and decipherment must be simple, demand no strain. Complex processes impossible on field. System must admit of speedy correction of errors. Conforming to all preceding, system must be such that solution of 50 to 200 messages all in same key is a difficult matter--sufficient to delay solution for such length of time that information is valueless when solved.

7. Explanation of the new U.S.Army Multiple Disk Cipher Device. Derving a numerical key from a key word or a key phrase.

Third Lecture, July 8.

1. Code. Review definition and distinction between code and cipher.

2. The various types of codes. Commercial. Governemental. Economy. Secrecy. Alphabetical or one-part codes. Randomized, or two-part codes. Advantages and disadvantages of each. Necessity of furthersencipherment for secret alphabetical codes. Necessity of careful attention to randomized codes. Security in latter consists in rearrangement of code equivalents from time to time. Meaning of "new edition, or change in code".

3. The Army Field Codes. General description of contents and type of groups. Phrases, words, numbers, syllables, letters, time groups, nulls, blanks.

4. The limitations of the field codes. Reduced size, and consequent small vocabulary. Necessity of becoming familiar with contents. Make code message fit the code book, not vice versa.

5. Safeguarding the code. Reasons for precautions to be found in past experiences and study of the analysis of code.

6. General rules. Necessity for preserving complete secrecy of the book itself against unauthorized sight, photographs, etc. Compromise of a single copy necessitates complete withdrawal of all copies and issue of new edition. Very expensive, time lost, danger, etc.
All code messages of equal importance to the enemy code solving section. Solutions in non-important messages great aid in solution of important. Hence, in actual warfare, restrict traffic to lowest possible limit. The amount of material intercepted is usually the deciding factor in solution.

7. Specific rules. Message once transmitted in one form of cipher or code must never be repeated in any other form whatsoever. Demonstration of case in actual solution of new German code from three messages intercepted. If absolutely necessary to repeat in another form, message must be paraphrased. Explanation--changing about the words, phrases, sentences. Make new message bear least resemblance to original. 2. Message once sent in code or cipher must never be sent in clear; and vice versa. 3. Never insert plain text of any kind in code or cipher message, nor punctuation, abbreviations, etc. in clear. 4. Plain text and equivalent code text must never appear on same sheet of paper for file. Work sheets must be destroyed by burning. Plain text sheets must never be filed attached to cipher or code sheets.

8. Brief description of principles of analysis of code. Reconstruction of the code book. Breaking up the unknown text into a series of sets of groups. Study of the behaviour of the various types of elements going to make up intelligible text. Words- various natures. Prepositions, nouns, adjectives, verbs, etc. all behave differently.

9. Solution by comparison or analogy. Danger of stereotyped messages or reports of any kinds. Must be avoided because easiest solved. Solution by first principles.

10. The proper use of the code to make solution by first principles more difficult. Danger of addresses and signatures. Use of Spelling groups to be limited so far as possible. They are weakest part of the code. Use of the variants and nulls or non-significant groups.

11. General summary.