CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

February 22, 1996
Revision 0

LECTURE 8
INTRODUCTION TO CRYPTARITHMS
AND
HILL CIPHER

SUMMARY

In Lecture 8, we depart from the schedule for a real treat. In the first part of this Lecture, we introduce Cryptarithms by our guest lecturer LEDGE (Dr. Gerhard D. Linz). LEDGE has already produced one of our better references on beginning cryptography [LEDG], and I appreciate his assistance in our course. The cryptarithms portion of this course will be presented in three lectures and for the final book labelled Lectures 20 - 23.

Following the Cryptarithms section we introduce the Hill Cipher.

Our second guest lecturer is NORTH DECODER. Dr. Jerry Metzger and his team are presenting you with the Crypto Drop Box and the ACA-L Listserver. The Hill cipher has six GIF files associated with it and can be found at the CDB.

Waiting in wings patiently for my resource materials is TATTERS to present Cipher Exchange problems.

INTRODUCTION TO CRYPTARITHMS (by LEDGE)

Here's the first of the Cryptarithm lectures. It consists of a general introduction to the genre including how to read the problems. That's followed by an explanation of modulo arithmetic. Then we look at how to identify the letters that represent 0, 1 and 9, called digital characteristics. Then there are two sections on making inferences, each demonstrating a problem solution. Finally, there's a section on extracting square roots.

Next lecture LEDGE will give some aids for solving multiplication problems and then go into base 11 and base 12 arithmetic. Perhaps after that I can go to the more complicated problems such as double key division.

PART I

DEFINITION: A cryptarithm is a mathematical problem, generally in arithmetic, in which the numerical digits have been replaced systematically by letters. The challenge of the problem is to identify the digit for each letter and the key, if any.

Rules: 1. Each digit is replaced by one and only one letter throughout the problem.
2. All digits appear at least once in the problem.
3. No letter represents more than one digit.
4. The numerical base, if other than ten (decimal), is named.
5. The highest order digit of a number cannot be zero.

KEYS: A table consisting of each of the letters used in the cryptarithm paired with its numerical equivalent constitutes the key to the cryptarithm. When the digits are arranged in numerical order, either from smallest to largest or largest to smallest or other logical order, the letter portion of the key may spell out one or more words. The word or words are then known as the keyword or keywords. Generally, the constructor of the problem indicates the number of words or the fact that the letters do not spell out words.

When the letter portion of the key consists of a word or several words with no repeated letters (rule 3, above), the digits are assigned in one of four ways:

```
1. From 0 to 9 (0-9). Ex. L O G A R I T H M S
                          0 1 2 3 4 5 6 7 8 9

2. From 9 to 0 (9-0)      9 8 7 6 5 4 3 2 1 0

3. From 1 to 0 (1-0)      1 2 3 4 5 6 7 8 9 0

4. From 0 to 1 (0-1)      0 9 8 7 6 5 4 3 2 1
```

In the first and fourth case L represents 0; in the second it represents 9; and in the third it represents 1, etc. Higher base arithmetic systems require additional digits according to the size of the base. Undecimal is based on 11 digits rather than 10. Generally the letter X or A is used to represent the 11th digit, or ten. Thus instead of a key for 0-9 we would have a key for 0-X or 0-A.

```
Ex. B I G N U M E R A L S
    0 1 2 3 4 5 6 7 8 9 X
```

Here the digit X (ten) will be replaced by S when it occurs. In undecimal, 10 means eleven. If you do not understand the concept of higher base arithmetic systems now, you will get an extended treatment of this topic later in the course.

If no word is used, that fact will be stated as well as the order in which letter equivalents are to be reported, e.g., No word, (0-9), indicating that the letters for reporting purposes are to be arranged starting with the letter representing 0, followed by the letter for 1, then 2, etc., with the letter for 9 last. The letters will then appear in random order, generally not alphabetical order.

ARITHMETIC: Knowledge of addition, subtraction, multiplication and division of whole numbers in base 10 (decimal) system will be assumed. Extraction of square and cube roots will be explained later. While base 13 problems sometimes appear among the numbered problems in the Cryptarithms section, they and higher base problems are generally offered as specials. More esoteric operations, such as powers, magic squares, Pythagorean equations, etc. are also offered as specials for those who like extra challenges.

PROBLEM STATEMENT: In order to conserve space in the journal, the problems in the Cryptarithms section are written sequentially on one or more lines. I recommend rewriting the problems in normal arithmetic format on every other line, so as to have room for trial numbers. The process, without skipping lines, will be illustrated with each of the normal type of problems presented for solution.

The following sample problems to be rewritten are taken from the September-October, 1993, issue of The Cryptogram:

C-1. Square root. (Two words, 1-0) by EDNASANDE.

```
VO'TI'NG gives root VTO; - IN = NNTI; - NNNT = HONG; -UIGG =
NUFE
```

```
             _V__T__O
Rewritten:  {VO'TI'NG
             IN___
             NN TI
             NN_NT
                HO NG
                UI_GG
                NU FE
```

C-3. Division. (Three words, 9-0) by LI'L GAMIN.

AUSSIE v SHEEP = UE; - SHEEP = SUMAIE; - SPIBHP = LUHE

```
                        UE
   Rewritten:  SHEEP/AUSSIE
                     SHEEP
                     SUMAIE
                     SPIBHP
                       LUHE
```

C-6. Subtractions. (Two words, (0-9) by CAGEY KIWI.

LADIES - GENTS = GNSDGS.   DAMES - MALES = NDGSS

```
   Rewritten:  LADIES     DAMES
               -GENTS    -MALES
               GNSDGS     NDGSS
```

Additions and equations (mixed additions and subtractions) are rearranged the same way.

C-8. Multiplication. (Three words, 0-9) by APEX DX.

OTTAWA x ON = HNNTLIL + IIIEHE = TOOINRL

```
   Rewritten:     OTTAWA
                     xON
                 HNNTLIL
                 IIIEHE
                 TOOINRL
```

At this point you should understand the mechanics of the presentation of the problems. You should also be ready to construct cryptarithms of your own, although they may not be suitable as yet for publication. To be suitable for publication, the problem must conform to the rules listed on page 1, and have a unique numerical solution. There must be one and only one key that will solve the problem. If you have understood the material thus far, you are ready to consider ways of analyzing a problem to obtain the solution.

MODULO ARITHMETIC: Since we will be dealing with the ten digits, 0 - 9, but sometimes adding or subtracting them to get numbers that are either greater than 9 or less than 0 (in other words negative numbers), we need a way of reducing those results back to the digits mathematically. Modulo arithmetic is that way. If you add 8 + 5, you get 13. If you want to talk about only the units digit of the result, you could subtract 10 from the 13 and get that units digit, 3. We say, then, that 13 = 3 (modulo 10). The 10 comes from the fact that there are ten digits in the decimal system. When we learned addition, we learned to carry the 10 to the next column on the left, thus avoiding having to write a two digit number in a space where there is room for only one:

```
 28
 +5
 33 or 20 + 13 (8 + 5).
```

In subtraction, 5 - 8 = -3, but -3 is not in the range of the positive digits. Here we could add 10 to -3: -3 + 10 = 7, or -3 = 7 (modulo 10). In a subtraction problem we get the 10 by borrowing it from the next highest order digit in the subtrahend:

```
     25
     -8
   = 17 or 20 - 3 or 10 + (10 - 3)
```

The way we learned to subtract eliminates the negative numbers by borrowing 10 from the 20 in 25. Modulo arithmetic is another way of talking about the same process.

DIGITAL CHARACTERISTICS: Gaining an entry into a problem is often expedited by being able to identify one or more of the digits. Those most commonly identifiable with a little bit of study of the problem are 0, 9, and 1. Zero in particular has a number of recognizable characteristics. Add zero to a number and the sum is that number, i.e., A + 0 = A. Similarly, subtracting zero from a number yields that number, i.e., A -0 = A. Multiply a number by zero and you get zero. Subtract a number from itself and you get zero, i.e., A - A = 0. Once zero is identified, you will have the first or last letter of a keyword, if any.

If 0 cannot be identified through any of the characteristics enumerated above, it may yet be possible to discover the candidates for it through a process of elimination. Given a number, we know that the highest order digit of that number cannot be zero. So if we have a number, ABC, then A is not zero. Let's use that fact and any other inferences we can make on the example multiplication problem, C-8, from page 3.

```
 OTTAWA
    xON
-------
HNNTLIL
IIIEHE
-------
TOOINRL
```

This problem has five different numbers with four different beginning letters: O, H, I, and T. None of those can be zero. The multiplier, ON, contains the digit N which, when multiplying OTTAWA, produces a product not equal to zero. Hence, N does not equal zero. When adding the two partial products, E + I yields R not either E or I. Hence neither E nor I = zero. We have eliminated seven letters as candidates for zero. So far, at least, L, W, or R could be zero. It will take more detailed analysis to determine which one is actually zero.

The number 9 has some interesting characteristics, one of which mimics zero. When subtracting 9 from a number, you must borrow from the next higher digit. The difference between 9 and the number is then one more than that number, i.e., 24 - 9 = 15 contains 4 -9 yielding 4 + 1 or 5. The 2 in the original number has been reduced by 1 because of the borrowing.

Let's look at another subtracting operation involving 9.:

```
247 - 48 = 199 or 247
                  -48
                = 199
```

That example includes a digit that is subtracted from itself.

That operation normally would produce zero. Here it produces 9 because of a borrowing necessitated by a previous subtraction, namely 7 - 8. 4 - 4 becomes 3 -4 yielding 9 and reducing the 2 to 1. That sort of effect is not possible in the units place of a number because there is no previous borrowing when dealing with whole numbers. Thus, when given a problem that includes:

```
ABCDE
-DCFE
 GHIJ
```

H could equal 0 or 9. More information is needed to resolve the ambiguity. We have it here in the units place where E -E = J. There is no ambiguity in that fact since there cannot have been any previous borrowing. So J = 0 and H = 9.

The number one can often be recognized as the highest order digit of a number particularly when, in a subtraction problem, it is not carried down to the answer line. Note that in the previous example, A is the highest order of the subtrahend, the number from which another number is to be subtracted. It does not appear in GHIJ, the difference between the two numbers. Clearly, it must have disappeared in the process of borrowing. D must be greater than B, thus B - D yields G, a number that is greater than B and necessitating borrowing one from A, reducing it to zero. Notice than when subtracting a larger digit from a smaller one, the resulting difference is larger than the subtrahend digit, e.g., 5 - 8 yields 7 or 15 - 8 = 7 > 5. If you now understand subtracting using modulo arithmetic, you will recognize that 5 - 8 = -3 which = 7 (modulo 10). In modulo arithmetic we can add or subtract the base, here 10, as many times as necessary to produce a number in the desired range, here 0 to 9. (See page 3, "Modulo arithmetic," 1st sentence.)

The number one can also be spotted in multiplication since one times a number equals that number, i.e. A x 1 = A. One times one also yields one, making it one of three digits that when squared or multiplied by itself yields a number whose unit digit is the same as the number squared: 1 x 1 = 1, 5 x 5 = 25, and 6 x 6 = 36. Once again, modulo arithmetic lets us know that 25 = 5 (modulo 10) and 36 = 6 (modulo 10).

MAKING INFERENCES: (Example 1). Once you have done what you can to spot 0, 1 and 9, you will have to rely on your knowledge of arithmetic to determine the possibilities of the other letters and to make decisions about their values. To see how that works, let's work on a simple problem, the division problem C-3 at the bottom of page 2. It's reproduced below:

```
      ____UE
SHEEP/AUSSIE
      SHEEP
      SUMAIE
      SPIBHP
        LUHE
```

Before reading on, see what you can do with this problem. Remember, the key is three words, 9-0. When you are ready, read on for the solution.

In the above problem, we are helped by being able to find all three of the digits, 0, 1, and 9. In the first subtraction, I - P = I. In the second subtraction, E - P = E. Both facts make 0 = P. Note also that U x P = P and E x P = P, both consistent with P = 0, but not sufficient to prove that P is zero, since both of those equations, modulo 10, could be true for P = 5, e.g., 3 x 5 = 15 and 7 x 5 = 35, both ending in 5. Next for the letter that represents one. U x SHEEP = SHEEP. Hence, U must be 1. Note also in the second subtraction, U -P = blank or zero. Since we know P to be zero, U must be 1. These chains of reasoning are typical in the solution of cryptarithms.

Now let's find the letter for 9. In the first subtraction, note that U - H = U. That could make H be zero or nine. In the absence of other information, you could not be sure which of those is true. Here you already know that zero is represented by P. Thus, H = 9.

You now have a lot of useful information. Let's look at the multiplications for more. U x SHEEP is 1 x SHEEP = SHEEP, not much help there. E x SHEEP = SPIBHP. You can replace the identified letters with their digital equivalents and get: E x S9EE0 = S0IB90. E x 0 = 0, so far so good. E x E = 9 (modulo 10). What are the possible values of E. E could be 3, as 3 x 3 = 9, or 7, since 7 x 7 = 49 or 9 (modulo 10). Let's try out each possibility. 3 x S9330 = ??7990 or ??IHHP, not consistent with SPIBHP. So E is not 3. E must then be 7. Let's check that and see what else you can uncover. 7 x S9770 = ??8390 making I = 8 and B = 3. Now SPIBHP is S08390. 8 is preceded by 0 so 7 x S must end in 4 since we are carrying a 6 from the multiplication of 7 x 9 and 6 + 4 = 0 (modulo 10). Hence, S must be 2 as 7 x 2 = 14. SPIBHP becomes 208390. To bring order out of all this in-formation, we need to reconstruct as much of the key as we can.

```
9 8 7 6 5 4 3 2 1 0
H I E       B S U P
```

The missing letters are A, L, and M, all found in the second subtraction. Entering what is known now makes that subtraction

```
 21MA87
-208390
   L197
```

Remember, you can check a subtraction by adding the subtracter and the difference to get the subtrahend. Here, 0 + 7 = 7; 9 + 9 = 18, carrying 1 to the next addition; 1 + 3 + 1(carried) = 5, so A = 5. Since L and M are both less than 8, representing as they do the two remaining unidentified digits, 6 and 4. L + 8 = M (modulo 10), or 6 + 8 = 14 or 4 (modulo 10). So L = 6 and M = 4. The key becomes HIELAMBSUP.

You could also have worked with the first subtraction, as it contains the letters M and A. Try that now using the partially reconstructed key above. The results should be the same.

MAKING INFERENCES: (Example 2). The multiplication example, C-8, given on page 3 presents somewhat more difficulties than the previous one, as none of 0, 1, or 9 can be initially identified. There are enough other clues, however, to make the solution come through a straightforward series of inferences. Before reading on, see what you can recover from that problem on your own. When you are in a thoroughly stuck place, read on for some help, or the complete solution.

Here is the problem:

```
 OTTAWA
    xON
HNNTLIL
IIIEHE
TOOINRL
```

It was determined that zero is represented by L, W, or R. On page 3 the key is stated to be three words, 0-9. First, notice that N time OTTAWA results in a 7-digit number and that O time OTTAWA results in a 6-digit number, the same length as OTTAWA. Examine the second product carefully. O x OTTAWA = IIIEHE. The highest order I (first digit of IIIEHE) results from the product O x O. O cannot = 1 for 1 x OTTAWA = OTTAWA. O cannot be as large as 4, for 4 x 4 = 16, which would add a seventh digit to the product. So O = 2 or 3. 3 x 3 = 9, which would make I at least 9. Looking at the problem again, the first I is added to H giving T, a digit, but adding anything other than zero to 9 produces a two digit number. So I cannot be 9 and O cannot be 3. So O = 2.

With O = 2, I must be 4 or 5 since O x O is 4 or could be 5 if a 1 is carried from the previous multiplication (2 x T). So we have the following multiplication: 2 x 2TTAWA = 444EHE or 555EHE. We can divide each of those products by the multiplier, 2, getting respectively 222??? and 277???. The first quotient gives 222??? to represent OTTAWA - not possible (it would be OOO???). The second quotient is consistent in making T = 7 and I = 5. OTTAWA becomes 277AWA. IIIEHE = 555EHE.

Now let's look at the first product, N x 277AWA = HNN7LIL. The product must be less than 10 x OTTAWA and that makes its first digit less than O. There is only one such digit, so H = 1. You could now divide 1NN7LIL by various values of N to find a quotient that begins 277. It's easier, however, to look at the addition of the two partial products as they contain N's.

```
1NN7LIL
555EHE
7225NRL
```

Since 1 + 5 = 7 (highest order pair), N + 5 must be > 10. That would allow a carried 1 to be added to 1 + 5.
N + 5 + 1(carried from the previous N + 5) = 2 (modulo 10). That makes N = 6. Let's pause to construct a partial key using the information so far identified.

The key table becomes:

```
0 1 2 3 4 5 6 7 8 9
  H O     I N T
```

It's also possible to rewrite the problem substituting digits for the identified letters:

```
 277AWA
    x26
1667L5L
555E1E
72256RL
```

The sums produce the following modulo 10 equation: E + 7 = 5; L + 1 = 6; E + 5 = R. The equations ignore possible carries of 1 which you may have to supply. Accepting that contingency, the first equation produces 8 as the only possible value of E. The third equation then makes R = 3 since there is no carry possible. The second equation makes 4 and

5 possible values of L, but 4 is the only available digit. Of the three letters that could be zero only W is left unidentified. Only 9 is left for A. As a check, 9 x 6 = 4 or L and 9 x 2 = 8 or E, checking out. The key has become WHORLINTEA as the solution.

EXTRACTING SQUARE ROOTS: Not understanding the following algebraic analysis of the process of extracting a square root is no barrier to understanding how to follow the method. It is included here for those who are interested in understanding how it is that the method works.

When squaring a number, one doubles the number of digits of the original number. If you square 9, you get 81, 2 digits. Squaring 3 you get 09. Square 35 and you get 1225, 4 digits. Square 12 and you get 0144. When extracting the square root of a number, you take cognizance of this fact by making a mark after every two numbers beginning from the decimal point in both directions. So 45678.96 becomes 4'56'78.96' with the initial 4 being understood as 04. As many pairs 00 can be added after the last mark without changing the value of the number.

The first trial root is the largest number whose square is equal to or less than the initial pair of numbers. We'll call that trial root x. (One could use the largest number whose square is equal to or less than the initial two or more pairs of numbers. That makes no theoretical difference although in practice that's more difficult.) The square of x is then subtracted from the first pair of numbers. The next pair of numbers is appended to the difference as in a long division problem.

Now there is room for a 2-digit root whose first digit is x. If we call its second digit y, the root becomes 10x+y. Multiplying that number by itself produces 100x} + 20xy +y}. That can be factored to produce 100x} + y(20x + y). As x} has already been subtracted from the highest order two digit number of the original number it remains to subtract y(20x + y) from the current remainder to make sure that y is not too large and to determine a new remainder.

Now let's extract the square root of 45678. First mark after every second number starting at the decimal point.

```
 _______
{4'56'78
```

The first pair of numbers is 04. The square root of 4 is 2, a number we'll place above the 4. We'll then square 2 getting 4 and placing it under the 4 in the number and subtracting. Since the remainder is zero we'll merely pull down the next pair, 56, and produce our trial divisor. The work looks like:

```
 2______
{4'56'78
 4___
   56
```

The trial divisor is produced by multiplying the root we have, 2, by 20 making 40. 40 divides into 56 one time (trial y) which is added to 40 making 41. The trial y, 1, is placed over the second digit of the new pair, 6. 41 is multiplied by y (1) and subtracted from 56. Then 78 is pulled down at the end of the difference. The work looks like:

```
     2__1___
    {4'56'78
     4___
41     56
       41___
       15 78
```

Again the root, now 21 is multiplied by 20 giving 420. 1578 divided by 420 gives 3, our new y which is added to 420 giving 423. 3 x 423 or 1269 is then subtracted from 1578 giving a remaider of 309. The 3 is put above the 8 of 78 making the new root 213 with a remainder. If it were desired to extend the calculation to the right of the decimal point, a pair of zeroes could be appended to the remainder and the process repeated with a decimal point placed in the root after the 3. The work without going past the decimal point becomes:

```
     2__1__3
    {4'56'78
     4___
 41    56
       41___
423    15 78
       12_69
        3 09
```

You can check that by squaring 213 (213 x 213) and adding 309. You should get 45,678. Practice by taking the square root of another 5 or 6-digit number and checking your outcome. Solve C-1 on page 2 for homework.

If you want more practice work, find divisions, square roots, and multiplication problems in the two current issues of The Cryptogram. Do the subtraction problem, C-6 on page 3 if you wish. Discuss problems you may have with your mentor. If you have suggestions, questions, or other reactions you wish to share with me, my address is

Dr. Gerhard D. Linz

I hope your pleasure in solving Cryptarithms is enhanced by this presentation. Next time I'll respond to any concerns you have. I also plan to give you some more tools for multiplication and introduce counting systems based on 11 and above.

LEDGE
January 2, 1996

OBSERVATIONS ON SQUARES (LANAKI)

Dr. Andree gives us some hints on squares and square roots. [OKLA]

S-1 Squares end only in 0, 1, 4, 5, 6, or 9.

S-2 If (...S)**2 ends in ...S, then S=0,1, 5 or 6.

S-3 If (...S)**2 ends in B n.e. S, then S= 2,3,4,7,8 or 9
B= 1, 4, 6 or 9

S-4 If (..X)**2 ends in	0	1	4	5	6	9
then (...X) ends in	0	1,9	2,8	5	4,6	3,7

S-5 If N contains k digits, then N**2 contains either 2k-1 or 2k digits.

HILL CIPHER SYSTEM (by NORTH DECODER)

There are two basic ways to prevent the tell-tale behavior of plaintext letters from showing through in ciphertext. One method is to vary the ciphertext letter that replaces a given plaintext letter. That is the solution offered by the Vigenere and other polyalphabetic systems. A second technique is to encipher the plaintext in chunks of several letters at a time. The Playfair system provides a compact method for enciphering digraphs, that is, pairs of letters. While the Playfair does disguise the behavior of individual letters, even better would be a system that operated on letters in groups of three letter (or four or five or ...). It seems that no convenient pencil-and-paper method for handling such trigraphic (or quadgraphic or ...) encipherment has been devised.

In 1929, Lester Hill [HIL1, HIL2] described an algebraic procedure that allows encipherment of plaintext letters n at a time (that is, in n-graphs), where n can be any positive integer 1,2,3,.... Hill's Cipher could be carried out by hand probably without too much hardship for groups of letters up to five. After that, it would become a challenge to keep the computations accurate. However, on a computer it would be feasible to work with large groups of letters, and it seems that plaintext enciphered in such a system using say 10-graphs would be difficult to crack.

The first step in using Hill's system is to assign numerical values to the 26 letters of the alphabet. There is nothing sacred about 26 in the system. The ideas work just as well for alphabets of any size. So it would be possible to add a few punctuation marks to the usual alphabet to get say 29 symbols, or to work entirely with data in binary form with an alphabet of just two symbols. Also the numerical equivalents of the letters of the alphabet could be assigned in some arbitrary way, which would probably add to the security of the system. For these notes, the 26 letter alphabet will be used, and letters will be given their standard numerical equivalents, namely a = 00, b = 01, ..., z = 26. The encipherment of plaintext is most neatly described using matrix multiplication. A matrix is a rectangular array of numbers such as:

$$M = \begin{vmatrix} 1 & 5 & 3 \\ 0 & 2 & 1 \end{vmatrix}$$

That particular matrix has 2 rows and 3 columns. More briefly, it is a 2 x 3 matrix. In certain cases, the product of two matrices can be computed. The rule for multiplication requires that the number of columns in the lefthand factor match the number of rows in the righthand factor. For example, if

$$N = \begin{vmatrix} 2 & 5 & 0 & 1 \\ 7 & 6 & 1 & 3 \\ 3 & 3 & 0 & 1 \end{vmatrix}$$

Then the product MN can be formed since M has three columns and N has three rows. On the other hand, the product NM is not defined. For these two matrices the product is

$$MN = \begin{vmatrix} 1 & 5 & 3 \\ 0 & 2 & 1 \end{vmatrix} \text{ X } \begin{vmatrix} 2 & 5 & 0 & 1 \\ 7 & 6 & 1 & 3 \\ 3 & 3 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 46 & 44 & 5 & 19 \\ 17 & 15 & 2 & 7 \end{vmatrix}$$

The upper lefthand entry in the product matrix is produced by multiplying each number in the first row of M by the corresponding number in the first column of N, and adding the results:(1)(2)+(5)(7)+(3)(3)=46. That explains why the number of columns in M must match the number of rows in N. The second number in the first row of the product is produced in the same way by multiplying the first row of M times the second column of N: (1)(5)+(5)(6)+(3)(3)=44. And so on, the third number in the first row of the product is produced by multiplying the first row of M by the third column of N, and finally, the fourth number in the first row of the product comes from multiplying the first row of M by the fourth column of N. To produce the second row of the product, the second row of M is used in place of the first row of M in the preceding computations. So, for example,(0)(2)+(2)(7)+(3)(3)=17 gives the first number in the second row of the product matrix. If M had more rows, each would be used in turn in the same way to produce one more row in the product matrix.

If you think about the multiplication process described above, you will see that the result of multiplying an r x s matrix and an s x t matrix will be an r x t matrix.

In the application of matrix multiplication to the Hill Cipher system, all arithmetic will be carried out modulo 26. In other words, any time a number appears which is 26 or larger, it is divided by 26, and the number is replaced by the remainder of the division. In the example above, the computation of the top left number in the product of M and N could be written as (1)(2)+(5)(7)+(3)(3) = 2 +35 + 9 = 2 + 9 + 9 = 20 (mod 26). The symbol (mod 26) is added here just to indicate there is funny arithmetic being used, namely that arithmetic is being done modulo 26. If the alphabet had 29 symbols instead of 26, operations would be carried out modulo 29. Since all the examples here will be done modulo 26, the indicator (mod 26) will be omitted from now on. So we will write the example above as:

$$MN = \begin{vmatrix} 1 & 5 & 3 \\ 0 & 2 & 1 \end{vmatrix} \text{ X } \begin{vmatrix} 2 & 5 & 0 & 1 \\ 7 & 6 & 1 & 3 \\ 3 & 3 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 20 & 18 & 5 & 19 \\ 17 & 15 & 2 & 7 \end{vmatrix}$$

To encipher the plaintext message "send more money", first the message is rewritten in groups of letters of the selected length. For this example, length three will be used, so the message becomes "sen dmo rem one ykz", where two nulls have been added to fill out the last group. Next an enciphering matrix, or key, is selected. If letter groups of size n are being used, an n x n enciphering matrix will be needed. For this example, the 3 x 3 matrix

$$E = \begin{vmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{vmatrix}$$

will be used. Notice that the numbers in the matrix might as well be selected between 0 and 25 since all arithmetic will be done modulo 26 anyway. To encipher the first three letter group of plaintext, it is written as a 3 x 1 matrix, say P, the letters are replaced by their numerical equivalents, and the matrix product EP is computed.

The product is a 3 x 1 matrix, say C. Its entries are converted to letters, and these give the ciphertext for the first group. Here are the details.

$$EP = \begin{vmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{vmatrix} \text{ X } \begin{vmatrix} s \\ e \\ n \end{vmatrix} = \begin{vmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{vmatrix} \text{ X } \begin{vmatrix} 18 \\ 4 \\ 13 \end{vmatrix} = \begin{vmatrix} 20 \\ 4 \\ 13 \end{vmatrix} = \begin{vmatrix} U \\ E \\ N \end{vmatrix}$$

So the first three letters of ciphertext are UEN. The second trigraph is enciphered as

$$EP = \begin{vmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{vmatrix} \text{ X } \begin{vmatrix} d \\ m \\ o \end{vmatrix} = \begin{vmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{vmatrix} \text{ X } \begin{vmatrix} 3 \\ 12 \\ 17 \end{vmatrix} = \begin{vmatrix} 5 \\ 18 \\ 19 \end{vmatrix} = \begin{vmatrix} F \\ S \\ T \end{vmatrix}$$

Continuing in this way, the ciphertext is found to be UEN FST XYH LZI UCN, or, in traditional five letter groups, UENFS TXYHL ZIUCN. Notice that in this example, repeated plaintext letters are replaced by different ciphertext letters, and repeated ciphertext letters represent different plaintext letters.

Deciphering requires a second matrix that undoes the effects of the enciphering matrix. For the enciphering matrix given above, the deciphering matrix, or deciphering key, is

$$D = \begin{vmatrix} 21 & 23 & 18 \\ 6 & 23 & 6 \\ 9 & 7 & 15 \end{vmatrix}$$

and operating on the first ciphertext trigram UEN gives

$$D \begin{vmatrix} U \\ E \\ N \end{vmatrix} = \begin{vmatrix} 21 & 23 & 18 \\ 6 & 23 & 6 \\ 9 & 7 & 15 \end{vmatrix} \text{ X } \begin{vmatrix} 20 \\ 4 \\ 13 \end{vmatrix} = \begin{vmatrix} 18 \\ 4 \\ 13 \end{vmatrix} = \begin{vmatrix} s \\ e \\ n \end{vmatrix}$$

Operating on the remaining ciphertext trigram produces the rest of the plaintext message.

The enciphering key matrix cannot be selected arbitrarily. For example, the matrix

$$Z = \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix}$$

would convert every plaintext message into the ciphertext AAAAAAAA. To allow unique decipherment, an n x n enciphering key matrix should convert different plaintext n-grams into different ciphertext n-grams. An n x n matrix that behaves that way is called nonsingular.

There are a number of more or less efficient tests for nonsingularity. Here is one test that involves the determinant of an n x n matrix. The determinant of a square matrix is a number computed from the entries in the matrix. The definition builds up from small matrices to larger ones. First the determinant of any 1 x 1 matrix is defined to be the number that is the entry in that matrix. Thus det |7| = 7. To compute the determinant of a 2 x 2 matrix, step across the entries in the first row of the matrix, multiply each entry by the determinant of the 1 x 1 matrix that appears when the row and the column the entry appears in are eliminated from the matrix. The numbers produced in this way are alternately added and subtracted to produce the determinant of the matrix. Here's an example.

$$\det \begin{vmatrix} 4 & 3 \\ 8 & 2 \end{vmatrix} = (4)\ (\det |2|\ ) - (3)\ (\ \det |8|\ ) =$$

$$4 \times 2 - 3 \times 8 = 8 - 24 = -16.$$

The determinant of a 3 x 3 matrix is produced in the same way: step across the first row, multiply each entry by the determinant of the 2 x 2 matrix that appears when the entry's row and column are crossed out, and alternately add and subtract the resulting numbers. For the matrix of the earlier example, the computations, carried out modulo 26 this time, look like

$$\det \begin{vmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{vmatrix} = 1 \times \det \begin{vmatrix} 9 & 2 \\ 2 & 5 \end{vmatrix} - 7 \times \det \begin{vmatrix} 4 & 2 \\ 1 & 5 \end{vmatrix}$$

$$+\ 22 \times \det \begin{vmatrix} 4 & 9 \\ 1 & 2 \end{vmatrix} = 1 \times 41 - 7 \times 18 + 22 \times (-1) = 23$$

The computation of the determinant is extended to larger square matrices in the same pattern. More efficient ways to compute determinants are discussed in textbooks on Linear Algebra.

The importance of the determinant is that a matrix is nonsingular (and so usable as an enciphering key matrix in Hill's cipher) if and only if its determinant is relatively prime to 26. The matrix above has determinant 23 which is relatively prime to 26, so it is a legal enciphering key. More generally, if the alphabet used for the plaintext is made up of m symbols, then the usable enciphering matrices are those with determinant relatively prime to m. In the case of an alphabet of 26 symbols, the determinant of a usable matrix must be odd but not 13. Notice that if the size of the alphabet is increased to 29 by adding a few punctuation symbols, many more legal enciphering matrices will be available, both because operations will now be carried out modulo 29, and also because every number from 1 to 28 would be an acceptable value for the determinant of an enciphering key matrix.

Once an enciphering key matrix has been selected, the companion deciphering matrix needs to be computed. There are some reasonably efficient methods for finding the deciphering matrix. The method given here is easy to describe, but not very efficient. Check out a Linear Algebra text for better methods to handle matrices larger than say 4 x 4.

The first step is the computation of the determinant of the enciphering key E. If det E = e, then a number d is needed such that ed= 1 (mod 26). For a relatively small modulus such as 26, the d can be found by trial and error. Simply compute e times 1,3,5,7 ,9,11,15,17,19,21,23, and 25 until a product equivalent to 1 modulo 26 appears.

For larger alphabets with say m letters, solving ed =1 (mod m) can be carried out in a more sophisticated way using the Euclidean Algorithm, for example.

Check a Number Theory text for details. Set the number d aside for a minute.

Second, each number in the enciphering key matrix is replaced by the determinant of the matrix obtained when the element's row and column are erased from the matrix.

Third, plus and minus signs are prefixed to each entry in the new matrix in a checkerboard pattern starting with a plus sign in the upper lefthand corner.

Next, the matrix is flipped over the diagonal from the upper left corner to the lower right corner so that the first row be comes the first column, the second rows becomes the second column, and so on.

Finally, each entry in the matrix is multiplied by the d computed in the first step.

The resulting matrix is D, the deciphering key matrix.

Here are the computations that produce the deciphering key D of the example above. The determinant of the enciphering key E has already been computed: det E = 23. Since (17)(23) = 1 (mod26), it follows that d = 17. Next, the 1 in the upper left handcorner of E is replaced by

$$\det \begin{vmatrix} 9 & 2 \\ 2 & 5 \end{vmatrix} = (9)(5)-(2)(2) = 45 - 4 = 41 = 15 \pmod{26}.$$

where, in the last step, 41 has been reduced modulo 26.

The replacement for the 7 in the first row and second column is

$$\det \begin{vmatrix} 4 & 2 \\ 1 & 5 \end{vmatrix} = (4)(5)-(2)(1) = 18 \pmod{26}.$$

The replacement for the 9 in the second row and second column is

$$\det \begin{vmatrix} 1 & 22 \\ 1 & 5 \end{vmatrix} = (1)(5) - (22)(1) = - 17 = 9 \pmod{26}.$$

When all nine entries in E have been replaced, the matrix looks like

$$\begin{vmatrix} 15 & 18 & 25 \\ 17 & 9 & 21 \\ 24 & 18 & 7 \end{vmatrix}$$

Adding the plus and minus signs in a checkerboard pattern produces and replacing negative numbers by equivalent positive numbers modulo 26 gives

$$\begin{vmatrix} 15 & -18 & 25 \\ -17 & 9 & -21 \\ 24 & -18 & 7 \end{vmatrix} = \begin{vmatrix} 15 & 8 & 25 \\ 9 & 9 & 5 \\ 24 & 8 & 7 \end{vmatrix}$$

Flipping over the diagonal gives

$$\begin{vmatrix} 15 & 9 & 24 \\ 8 & 9 & 8 \\ 25 & 5 & 7 \end{vmatrix}$$

Finally, multiplying every entry of the last matrix by the d=17 computed earlier, and reducing the entries modulo 26, the result is

$$D = \begin{vmatrix} (17)(15) & (17)(9) & (17)(24) \\ (17)(\ 8) & (17)(9) & (17)(\ 8) \\ (17)(25) & (17)(5) & (17)(\ 7) \end{vmatrix} = \begin{vmatrix} 21 & 23 & 18 \\ 6 & 23 & 6 \\ 9 & 7 & 15 \end{vmatrix}$$

Arithmetic done with matrices has a lot in common with arithmetic done with ordinary numbers. The n x n matrix whose entries are all 0 except for 1's down the diagonal from the upper left to the lower right is called the identity matrix. It plays a role in matrix multiplication similar to the role 1 plays in multiplication of numbers. That is, for any number m, (1)(m) = m, while for any n x k matrix M, it is easily checked that IM= M. Moreover, for each number r (provided r is not equal to 0), it is possible to find a number s so that sr=1. The number s is called the multiplicative inverse of r, and is written as r^(-1) (that is, r to the -1 power). Likewise, for each n x n matrix M (provided it is nonsingular), there is an n x n matrix N for which MN=I. The matrix N is called the inverse of M, and is written as M^(-1).

The Hill Cipher system can be expressed compactly using some algebraic notation. To encipher a plaintext n-gram using the Hill Cipher, a nonsingular n x n matrix M is selected. The n-gram is written as an n x 1 matrix P, and the ciphertext is the n x 1 matrix C determined by the equation

$$C = MP.$$

The deciphering matrix is the inverse of M. When the ciphertext C is multiplied by M^(-1), the plaintext is recovered.

M^(-1) C = M^(-1) MP = IP = P.

Hill suggested that a good choice for an enciphering key matrix M is one that turns out to be its own inverse. If M = M^(-1), Mi s called an involuntary matrix. The advantage gained is that it is not necessary to compute the deciphering key. There are a number of methods that will automatically produce involuntary matrices, so the process of finding involuntary matrices does not have to proceed by trial-and-error. In any case, almost all papers written about the Hill Cipher system following Hill's time down to the present day assume the key is involuntary.

It seems that Hill and a partner (Weisner) filed a patent (Message Protector, patent number 1,854,947) for a mechanical version of the Hill Cipher in 1929, which, according to Kahn [KAHN], used an involuntary matrix enciphering key so that the same machine could be used to both encipher and decipher.

The Message Protector patented by Weisner and Hill provides a mechanical means of doing matrix multiplication. The device illustrated in the patent application is more accurately described as authentication indicator rather than a cryptographic mechanism. The principle of operation is very simple. The active component consists of three gears on an axle which are connected to three accumulator gears by chains. The three accumulator gears all have the same number of teeth (101 in the patent), and they can rotate independently. The three gears on the axle have 101, 202 and 303 teeth. As the axle is turned through a certain amount, the accumulator gears turn one, two and three times as far respectively. The teeth on the accumulator gears are numbered from 0 to 100, and small gear on the axle also has its teeth numbered from 0 to 100.

Now suppose the three accumulator gears start in position 0,0,0. If the axle turned through an amount that rotates its small gear through 43 teeth, then accumulator gear one will read 43, accumulator two will show 86 and accumulator three will show 28. The last value occurs since the third accumulator wheel will have made more than one revolution. If the starting position of the accumulator wheels had been 11,91,4, then the axle rotation through 43 teeth would leave the accumulators showing 53,76,32. In essence, the accumulators are modulo 101.

On the actual devise, there are six axles, and their gears can be moved to engage the accumulator drive chain one axle at a time. The placement of the gears on the axles vary from one axle to the next. On the illustrated machine in the patent, the sequence is:

axle 1: 101,202,303
axle 2: 202,303,101
axle 3: 303,101,202
axle 4: 101,303,202
axle 5: 202,101,303
axle 6: 303,202,101

Suppose the accumulators begin showing 0,0,0. Keeping track for now of only the total on the accumulator that connects to first gear on each axle, here is what happens as the axles are turned as follows:

axle 1: 23,
axle 2: 10,
axle 3: 88,
axle 4: 17,
axle 5: 41, and
axle 6: 51.

Initially, all the axles are disengaged from the accumulator drive chain. (Keeping in mind the number of teeth on the first gear on each axle.) axle 1 is engaged, turned 23, and the accumulator shows 23. Axle 1 is disengaged, axle 2 is engaged, turned 10, and the accumulator shows 43. Axle 2 is disengaged, axle 3 is engaged, turned 88 , and the accumulator shows 4. Axle 4 is disengaged, axle 4 is engaged, turned 17, and the accumulator shows 21. Axle 4 is disengaged, axle 5 is engaged, turned 41, and the accumulator shows 18. Axle 5 is disengaged, axle 6 is engaged, turned 51, and the accumulator shows 70. The final total on the on that accumulator represents the computation

(1)(23)+(2)(10)+(3)(88)+(1)(17)+(2)(41)+(3)(51) = 70 (mod 101).

Likewise the value on the accumulator connected to the second gear on each axle shows the result of the operation

(2)(23)+(3)(10)+(1)(88)+(3)(17)+(1)(41)+(2)(51) = 2 (mod 101).

Matrix notation can be used to express to whole operation compactly as

$$\left|\begin{matrix} 1 & 2 & 3 & 1 & 2 & 3 \\ 2 & 3 & 1 & 3 & 1 & 2 \\ 3 & 1 & 2 & 2 & 3 & 1 \end{matrix}\right| \;.\; \left|\begin{matrix} 23 \\ 10 \\ 88 \\ 17 \\ 41 \\ 51 \end{matrix}\right| = \left|\begin{matrix} 59 \\ 55 \\ 54 \end{matrix}\right|$$

where arithmetic has been carried out modulo 101.

To use the machine to authenticate a check for example, six numbers, between 0 and 101, are selected from the check. Perhaps the dollar amount of $1230.45 could be split up as 12 and 30 and the cents could be ignored. The check number of say 22131 might contribute three more numbers, 2, 21, and 31. Finally, the date of the check, maybe January 25, 1996 might contribute a sixth number, say 25. Of course, people must agree on how these numbers are selected. The check writer runs the six values through the Message Protector as described above, and the resulting triple of values is stamped on the check. The bank, before cashing the check, operates on the same six numbers with its Message Protector, and makes sure that the numbers produced on the accumulators matches the ones stamped on the check, thus being sure that none of the important figures on the check have been changed.

Although the Message Protector is a clever engineering construction, there are certainly many obvious mechanical shortcomings as well as weaknesses in the cryptographic system which probably explains why the machine never became popular. In fact, it's not clear if any were actually constructed. It would take a good salesman to get people to spend money on a machine to multiple 3 x 6 and 6 x 1 matrices. There did not seem to be and reasonable way to change the gear sizes. If a key matrix with entries besides 1, 2, and 3 were wanted, the number of teeth on the gears would soon become so large that the structure would have to be made pretty large, instead of the shoebox size Weisner and Hill diagrammed.

Weisner and Hill also explain how the Message Protector could be modified to act as a cryptographic devise. First of all, the numbers on the various gears would be replaced by letters, and the number of teeth on the accumulator gears would be 26 so that the arithmetic operations would be carried out modulo 26. Next, the axles would now carry six gears each, with the number of teeth on each gear being a multiple of 26. There would be six accumulators, so that six plaintext are converted to six ciphertext letters. They say that the number of teeth on the various gears "have to be selected according to certain mathematical principles". What they mean, of course, is the 6 x 6 matrix, each entry of which gives the multiple of 26 that gives the number of teeth on the corresponding gear, has to be non-singular modulo 26. It is suggested that the matrix may be, but does not have to be, selected to be involuntary.

The gearing in the devise cannot be changed easily, and certainly cannot be changed arbitrarily, so it seems the gearing set was intended to be selected once and for all. Since that pretty much makes the device cryptographically pointless, the inventors proposed that a plaintext message first be converted to a preliminary ciphertext according to so system left unspecified, but they probably had something like a Playfair in mind. The resulting ciphertext is then passed through the 6 x 6 Message Protector, to yield an intermediate ciphertext which is then passed through a third and final encipherment using another unspecified cipher system. The final ciphertext is transmitted, and the authorized recipient reverses each of the three encipherments to recover the original plaintext. It's not very clear how much additional security has been introduced passing the text through the Message Protector.

Nearly all discussions of cryptanalysis of Hill enciphered messages begin with the fairly generous assumptions that the cryptanalyst knows that an involuntary key matrix of known size has been used, and also knows the numerical values assigned to the alphabet letters. The only unknown is the particular key matrix used to encipher the message. For a key matrix of size 2 x 2, a brute force attack is feasible since there are only 736 2 x 2 involuntary matrices. As the size of the key grows, a brute force attack is no longer practical. For larger key sizes, no specific cryptanalytic approaches have been published. But, several authors given more or less detailed descriptions of cryptanalysis, with examples for small key size (2 x 2, 3 x 3) using the classic probable word or crib technique. That is, a piece of plaintext is assumed to appear in the message, and it is tried in each possible position. At each test location, a number of equations must be true if the crib is to generate the ciphertext at that spot. It turns out that even with a relatively modest crib (3 letters for a 2 x 2 key, and 4 for a 3 x 3 key), most positions can be eliminated as impossible by applying a few principles of linear algebra. Each possible crib location will produce a candidate matrix key. A trial decipherment of the ciphertext is made. If recognizable plaintext results, the cryptogram is broken. If not, the crib is moved along to the next possible spot, and the process is repeated. For details on see on cryptanalysis of the Hill Cipher, see [LEV1], [LEV2], [LEV3], [SINK], [MELL].

NORTH DECODER advises that the Hill cipher patent diagrams (GIF format) scanned in reasonable well into the CDB. If you would like to look at them, the files they are at the CDB in

/lanaki.crypt.class/docs/hill-gifs

There is a freeware gif file viewer at the CDB in

/msdos/gif-viewers

HOMEWORK SOLUTIONS FROM LECTURE 7

FRE-2. K2. (105) Another species. {sauvage,fp=ST]   MELODE

```
P Q   N X B M H Q I   Q A B   C I Q   D K E X Q B Q   O Q

P' W M R R Q;  D K E X Q B Q   O Q U Q I Q E Q Q   M C

T E X R X B X D Q ,   X P   Q A B   K  P' W M R R Q   N Q

V C Q   N W K B   O Q   U M C B B X Q E Q   Q A B   K C

N W K B   A K C D K U Q.
```

Solution reads: (PRIMITIVE) Le citoyen est une variete de 'homme; vavariete degeneree ou primitive, il est a l'homme ce que chat de gouttiere est au chat sauvage.

FRE-3. K2. (87) (jamais, A=b) It's fun trying.   GUNG HO

```
D G   X   Z   Q N J D P   M C J P U P   L S U   E' Z D

Z D H U   Q J S E J S N P   U Q   E Z H Z D P   M J H -

K N D P:   G Z   K U D I Q S N U ,   G Z   H S P D L S U,

U Q   G U P   O Z H U P .   * R J I Q U I U G G U
```

Solution reads: (AMOUR) Il y a trois choses que j'ai aime toujours et jamais compris: La peinture, la musique, et les dames. Fontenelle.

FRE-4. PAT from [GIVI] page 13.and ff.   (130)

Solve and recover key(s).

```
YJXMG   XBXUF   JGECU   JEBZD   XAMNM   ZDFLG   FAFNJ   OFNDJ

GVJXE   FNNME   VRJZJ   KAFNB   FNZAG   NCUJE   BNRUX   OFNJG

NNXKX   FELGF   BJRVF   NOFUI   FXAAF   GTFVR   FAFKU   FNBJE

NADXN   VMXUF
```

PAT format reads: JAIOU IDIRE AUNGR ANDPH ILOSO PHEQU ELESA MESHA UTAIN ESSON TCAPA BLESD ESPLU SGRAN DSCRI MESAU SSIBI ENQUE DACTE SMERV EILLE UXETC ELEBR ESDAN SLHIS TOIRE.

ITA-2. K2. (88) (ne, han, con) Thirty days hath September. LABRONICUS

IDSAIK QW PLAIK ALBSCMDS PLA

KEDWZS, UWOUAL S RSIISCMDS. QW

BSAILIIL PS A'S OAL. IOIIW UZW

KZIDW AS VKA IDSAUIOAL.

Solution reads: (CALANDRIO) Trenta di contra Novembre con Aprile, giugno e Settembre. Di ventotto ce n'e uno. Tutti gli altri ne han trentuno.

ITA-3. K2. (117) (sulla, f=I). La frode necessaria. MICROPOD

GZQKE AFSZL TKFQA QSFNF QKGKQ

TGGZP ZQFRA TJZEF NSZMT ZJSAS

ZRAPT DAFFQ KGKZL ZSSKE OFJFQ

QTJKR AEZFQ ZSSZH FJSFM TFGGK

EOFLF JQZGA JXTSZ JD.

Solution reads: (PERFIDO) La sicieta puoesister esolo sulla basediunacerta quantitadibugie esolo apatto che nessunodicaesattamente quello che pensalinyutang.

SPA-1. BARKER

ZKEPC UKY TCYDMSR VCTPER A

ZPZNDZK GCTYRZK R NTDGR YC VK

KSTPQDPER MK TCYGRZYPQPMPEKE

ECM KSCZSKER GRT CM URUCZSR.

Partial solution: no key. TADI MAS RESULTO HERIDO Y

SPA-2. K2. (96) (deseo, f=R) Musica.   D. STRASSE

TIZ QBJNAZ KJKTFZN BP LTB BF

KNAGBN AGKTFPJ GTPAOZF MBF

SJGHNB RTB TI KTNZGBIQB

BPKJIQZIBJ MPBBJ NAQGAOJ MB

MZIYZN.

Partial solution: (HOMBRES) UNA TEORIA POPULAR ES QUE

SPA-3. (122) (-ulado, MZ=qk) Flight?   LIFER

NSPYK IXPUA KPZDX PSPEX KRLKO

KAXTS PQKDX RKRRS SINKY KRLAR

SDKTQ LDLPX KTASQ XSPXP RSOSP

RXJKR KTOAS TSPQX LSDOA XISAE

CSDLR SCPVD LNLBA XOCDK RL.

Partial solution: (DIPLOMAT) BENJAMIN FRANKLIN ENVIADO

POR-2. K2 (96) (tenta; gj=NQ) Machine Age?   YO TAMBIEN

EPEJTXD URTC JZXGC VRJ DJ

XINRSOC HCD TCVRPUCD VRJ

ZJUDCT J HJDGXUMPC HJ AXHX

OXTJT VRJ AJUAC MCBJSX.

*O. *TRTMXIH *QXUJD

Solution reads: (VIDAREL) Vivemos numa epoca que se orgulha das maquinas que pensam e desconfia de todo homen que tenta fazelo. H. Mumford Jones.

POR-3. K1. (nossos va-) Letter to horseman? ZYZZ

UCUCG VCJFD EFWEO CBGCV SIHCL

ITIWF YCVFU HFWFT LFRFB CHWFC

ESHIL FGICD EGTIJ HCVGR PCVCJ

FVDEF WFHCV LFVFH JISKI XJIZU

IGVTI VVIVB CDEFG HIVVC IFYKF

RFTWF V.

Partial Solution reads: (VAQUEIRO): Papai sabe que tu.

NEW PROBLEMS

C-1 Give two solutions to: (BE)**2 = ARE

C-2 Square root: [OKLA] [OKLI]

```
       R, A, T, S
      -----------
     |Q  UA  RT  ET
     -A
      -----
      T  UA
     -T  SI
      -----
         U  RT
        -A  UT
         -----
         E  AO  ET
        -E  ES  UB
         ---------
              R  AR
```

>From Sinkov [SINK] two Hill system problems:

Hill-1

Decipher the message: YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC PQTYJ

Use the deciphering matrix

```
| 5  1 |
| 2  7 |
```

Hill-2

Decipher the message: MWALO LIAIW WTGBH JNTAK QZJKA ADAWS SKQKU AYARN CSODN IIAES OQKJY B

Use the deciphering matrix

```
| 2  23 |
| 21  7 |
```

REFERENCES / RESOURCES [updated 22 February 1996]

[ACA] ACA and You, "Handbook For Members of the American Cryptogram Association," ACA publications, 1995.

[ACA1] Anonymous, "The ACA and You - Handbook For Secure Communications", American Cryptogram Association, 1994.

[ACM] Association For Computing Machinery, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," Report of a Special Panel of ACM U. S. Public Policy Committee (USACM), June 1994.

[AFM] AFM - 100-80, Traffic Analysis, Department of the Air Force, 1946.

[ALAN] Turing, Alan, "The Enigma", by A. Hodges. Simon and Schuster, 1983.

[ALBA] Alberti, "Treatise De Cifris," Meister Papstlichen, Princeton University Press, Princeton, N.J., 1963.

[ALKA] al-Kadi, Ibrahim A., Origins of Cryptology: The Arab Contributions, Cryptologia, Vol XVI, No. 2, April 1992, pp 97-127.

[AND1] Andree, Josephine, "Chips from the Math Log," Mu Alpha Theta, 1966.

[AND2] Andree, Josephine, "More Chips from the Math Log," Mu Alpha Theta, 1970.

[AND3] Andree, Josephine, "Lines from the O.U. Mathematics Letter," Vols I,II,III, Mu Alpha Theta, 1971,1971,1971.

[AND4] Andree, Josephine and Richard V., "RAJA Books: a Puzzle Potpourri," RAJA, 1976.

[ANDR] Andrew, Christopher, 'Secret Service', Heinemann, London 1985.

[ANNA] Anonymous., "The History of the International Code.", Proceedings of the United States Naval Institute, 1934.

[AS] Anonymous, Enigma and Other Machines, Air Scientific Institute Report, 1976.

[AUG1] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part I:The Encoding Problem", Cryptologia, Vol XIII, No. 4, October 1989.

[AUG2] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part II:The Encrypting Problem", Cryptologia, Vol XIV, No. 1, August 1990.

[BADE] Badeau, J. S. et. al., The Genius of Arab Civilization: Source of Renaissance. Second Edition. Cambridge: MIT Press. 1983.

[BAMF] Bamford, James, "The Puzzle Palace: A Report on America's Most Secret Agency," Boston, Houghton Mifflin, 1982.

[BARB] Barber, F. J. W., "Archaeological Decipherment: A Handbook," Princeton University Press, 1974.

[B201] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Course #201, Aegean Park Press, Laguna Hills, CA. 1982.

[BALL] Ball, W. W. R., Mathematical Recreations and Essays, London, 1928.

[BAR1] Barker, Wayne G., "Course No 201, Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1975.

[BAR2] Barker, W., ed., History of Codes and Ciphers in the U.S. During the Period between World Wars, Part II, 1930 - 1939., Aegean Park Press, 1990.

[BAR3] Barker, Wayne G., "Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, 1977.

[BARK] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1973.

[BARR] Barron, John, '"KGB: The Secret Work Of Soviet Agents," Bantom Books, New York, 1981.

[BAUD] Baudouin, Captain Roger, "Elements de Cryptographie," Paris, 1939.

[BAZE] Bazeries, M. le Capitaine, " Cryptograph a 20 rondelles-alphabets," Compte rendu de la 20e session de l' Association Francaise pour l'Advancement des Scienses, Paris: Au secretariat de l' Association, 1892.

[BEES] Beesley, P., "Very Special Intelligence", Doubleday, New York, 1977.

[BLK] Blackstock, Paul W. and Frank L Schaf, Jr., "Intelligence, Espionage, Counterespionage and Covert Operations," Gale Research Co., Detroit, MI., 1978.

[BLOC] Bloch, Gilbert and Ralph Erskine, "Exploit the Double Encipherment Flaw in Enigma", Cryptologia, vol 10, #3, July 1986, p134 ff. (29)

[BLUE] Bearden, Bill, "The Bluejacket's Manual, 20th ed., Annapolis: U.S. Naval Institute, 1978.

[BODY] Brown, Anthony - Cave, "Bodyguard of Lies", Harper and Row, New York, 1975.

[BOLI] Bolinger, D. and Sears, D., "Aspects of Language," 3rd ed., Harcourt Brace Jovanovich,Inc., New York, 1981.

[BOSW] Bosworth, Bruce, "Codes, Ciphers and Computers: An Introduction to Information Security," Hayden Books, Rochelle Park, NJ, 1990.

[BOWE] Bowers, William Maxwell, "The Bifid Cipher, Practical Cryptanalysis, II, ACA, 1960.

[BP82] Beker, H., and Piper, F., " Cipher Systems, The Protection of Communications", John Wiley and Sons, NY, 1982.

[BRAS] Brasspounder, "Language Data - German," MA89, The Cryptogram, American Cryptogram Association, 1989.

[BROO] Brook, Maxey, "150 Puzzles in Cryptarithmetic," Dover, 1963.

[BRIT] Anonymous, "British Army Manual of Cryptography", HMF, 1914.

[BROG] Broglie, Duc de, Le Secret du roi: Correspondance secrete de Louis XV avec ses agents diplomatiques 1752-1774, 3rd ed. Paris, Calmann Levy, 1879.

[BRYA] Bryan, William G., "Practical Cryptanalysis - Periodic Ciphers -Miscellaneous", Vol 5, American Cryptogram Association, 1967.

[BURL] Burling, R., "Man's Many Voices: Language in Its Cultural Context," Holt, Rinehart & Winston, New York, 1970.

[CAND] Candela, Rosario, "Isomorphism and its Application in Cryptanalytics, Cardanus Press, NYC 1946.

[CAR1] Carlisle, Sheila. Pattern Words: Three to Eight Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CAR2] Carlisle, Sheila. Pattern Words: Nine Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CASE] Casey, William, 'The Secret War Against Hitler', Simon & Schuster, London 1989.

[CAVE] Cave Brown, Anthony, 'Bodyguard of Lies', Harper & Row, New York 1975.

[CCF] Foster, C. C., "Cryptanalysis for Microcomputers", Hayden Books, Rochelle Park, NJ, 1990.

[CHOI] Interview with Grand Master Sin Il Choi.,9th DAN, June 25, 1995.

[CHOM] Chomsky, Norm, "Syntactic Structures," The Hague: Mouton, 1957.

[CHUN] Chungkuo Ti-erh Lishih Tangankuan, ed "K'ang-Jih chengmien chanch'ang," Chiangsu Kuchi Ch'upansheh, 1987., pp993-1026.

[CI] FM 34-60, Counterintelligence, Department of the Army, February 1990.

[COUR] Courville, Joseph B., "Manual For Cryptanalysis Of The Columnar Double Transposition Cipher, by Courville Assoc., South Gate, CA, 1986.

[CLAR] Clark, Ronald W., 'The Man who broke Purple', Weidenfeld and Nicolson, London 1977.

[COLF] Collins Gem Dictionary, "French," Collins Clear Type Press, 1979.

[COLG] Collins Gem Dictionary, "German," Collins Clear Type Press, 1984.

[COLI] Collins Gem Dictionary, "Italian," Collins Clear Type Press, 1954.

[COLL] Collins Gem Dictionary, "Latin," Collins Clear Type Press, 1980.

[COLP] Collins Gem Dictionary, "Portuguese," Collins Clear Type Press, 1981.

[COLR] Collins Gem Dictionary, "Russian," Collins Clear Type Press, 1958.

[COLS] Collins Gem Dictionary, "Spanish," Collins Clear Type Press, 1980.

[COPP] Coppersmith, Don.,"IBM Journal of Research and Development 38, 1994.

[COVT] Anonymous, "Covert Intelligence Techniques Of the Soviet Union, Aegean Park Press, Laguna Hills, Ca. 1980.

[CULL] Cullen, Charles G., "Matrices and Linear Transformations," 2nd Ed., Dover Advanced Mathematics Books, NY, 1972.

[DAGA] D'agapeyeff, Alexander, "Codes and Ciphers," Oxford University Press, London, 1974.

[DALT] Dalton, Leroy, "Topics for Math Clubs," National Council of Teachers and Mu Alpha Theta, 1973.

[DAN] Daniel, Robert E., "Elementary Cryptanalysis: Cryptography For Fun," Cryptiquotes, Seattle, WA., 1979.

[DAVI] Da Vinci, "Solving Russian Cryptograms", The Cryptogram, September-October, Vol XLII, No 5. 1976.

[DEAC] Deacon, R., "The Chinese Secret Service," Taplinger, New York, 1974.

[DEAU] Bacon, Sir Francis, "De Augmentis Scientiarum," tr. by Gilbert Watts, (1640) or tr. by Ellis, Spedding, and Heath (1857,1870).

[DELA] Delastelle, F., Cryptographie nouvelle, Maire of Saint- Malo, P. Dubreuil, Paris, 1893.

[DENN] Denning, Dorothy E. R.," Cryptography and Data Security," Reading: Addison Wesley, 1983.

[DEVO] Devours, Cipher A. and Louis Kruh, Machine Cryptography and Modern Cryptanalysis, Artech, New York, 1985.

[DIFF] Diffie, Whitfield," The First Ten Years of Public Key Cryptography," Proceedings of the IEEE 76 (1988): 560- 76.

[DIFE] Diffie, Whitfield and M.E. Hellman,"New Directions in Cryptography, IEEE Transactions on Information Theory IT-22, 1976.

[DOW] Dow, Don. L., "Crypto-Mania, Version 3.0", Box 1111, Nashua, NH. 03061-1111, (603) 880-6472, Cost $15 for registered version and available as shareware under CRYPTM.zip on CIS or zipnet.

[EIIC] Ei'ichi Hirose, ",Finland ni okeru tsushin joho," in Showa gunji hiwa: Dodai kurabu koenshu, Vol 1, Dodai kurabu koenshu henshu iinkai, ed., (Toyko: Dodai keizai konwakai, 1987), pp 59-60.

[ELCY] Gaines, Helen Fouche, Cryptanalysis, Dover, New York, 1956.

[ENIG] Tyner, Clarence E. Jr., and Randall K. Nichols, "ENIGMA95 - A Simulation of Enhanced Enigma Cipher Machine on A Standard Personal Computer," for publication, November, 1995.

[EPST] Epstein, Sam and Beryl, "The First Book of Codes and Ciphers," Ambassador Books, Toronto, Canada, 1956.

[EYRA] Eyraud, Charles, "Precis de Cryptographie Moderne"' Paris, 1953.

[FL] Anonymous, The Friedman Legacy: A Tribute to William and Elizabeth Friedman, National Security Agency, Central Security Service, Center for Cryptological History,1995.

[FREB] Friedman, William F., "Cryptology," The Encyclopedia Britannica, all editions since 1929. A classic article by the greatest cryptanalyst.

[FR1] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 1, Aegean Park Press, Laguna Hills, CA, 1985.

[FR2] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 2, Aegean Park Press, Laguna Hills, CA, 1985.

[FR3] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part III, Aegean Park Press, Laguna Hills, CA, 1995.

[FR4] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part IV, Aegean Park Press, Laguna Hills, CA, 1995.

[FR5] Friedman, William F. Military Cryptanalysis - Part I, Aegean Park Press, Laguna Hills, CA, 1980.

[FR6] Friedman, William F. Military Cryptanalysis - Part II, Aegean Park Press, Laguna Hills, CA, 1980.

[FRE] Friedman, William F. , "Elements of Cryptanalysis," Aegean Park Press, Laguna Hills, CA, 1976.

[FREA] Friedman, William F. , "Advanced Military Cryptography," Aegean Park Press, Laguna Hills, CA, 1976.

[FRAA] Friedman, William F. , "American Army Field Codes in The American Expeditionary Forces During the First World War, USA 1939.

[FRAB] Friedman, W. F., Field Codes used by the German Army During World War. 1919.

[FR22] Friedman, William F., The Index of Coincidence and Its Applications In Cryptography, Publication 22, The Riverbank Publications, Aegean Park Press, Laguna Hills, CA, 1979.

[FROM] Fromkin, V and Rodman, R., "Introduction to Language," 4th ed.,Holt Reinhart & Winston, New York, 1988.

[FRS] Friedman, William F. and Elizabeth S., "The Shakespearean Ciphers Examined," Cambridge University Press, London, 1957.

[FUMI] Fumio Nakamura, Rikugun ni okeru COMINT no hoga to hatten," The Journal of National Defense, 16-1 (June 1988) pp85 - 87.

[GAR1] Gardner, Martin, "536 Puzzles and Curious Problems," Scribners, 1967.

[GAR2] Gardner, Martin, "Mathematics, Magic, and Mystery ," Dover, 1956.

[GAR3] Gardner, Martin, "New Mathematical Diversions from Scientific American," Simon and Schuster, 1966.

[GAR4] Gardner, Martin, "Sixth Book of Mathematical Games from Scientific American," Simon and Schuster, 1971.

[GARL] Garlinski, Jozef, 'The Swiss Corridor', Dent, London 1981.

[GAR1] Garlinski, Jozef, 'Hitler's Last Weapons', Methuen, London 1978.

[GERM] "German Dictionary," Hippocrene Books, Inc., New York, 1983.

[GIVI] Givierge, General Marcel, " Course In Cryptography," Aegean Park Press, Laguna Hills, CA, 1978. Also, M. Givierge, "Cours de Cryptographie," Berger-Levrault, Paris, 1925.

[GRA1] Grandpre: "Grandpre, A. de--Cryptologist. Part 1 'Cryptographie Pratique - The Origin of the Grandpre', ISHCABIBEL, The Cryptogram, SO60, American Cryptogram Association, 1960.

[GRA2] Grandpre: "Grandpre Ciphers", ROGUE, The Cryptogram, SO63, American Cryptogram Association, 1963.

[GRA3] Grandpre: "Grandpre", Novice Notes, LEDGE, The Cryptogram, MJ75, American Cryptogram Association,1975

[GRAH] Graham, L. A., "Ingenious Mathematical Problems and Methods," Dover, 1959.

[GODD] Goddard, Eldridge and Thelma, "Cryptodyct," Marion, Iowa, 1976

[GORD] Gordon, Cyrus H., " Forgotten Scripts: Their Ongoing Discovery and Decipherment," Basic Books, New York, 1982.

[HA] Hahn, Karl, " Frequency of Letters", English Letter Usage Statistics using as a sample, "A Tale of Two Cities" by Charles Dickens, Usenet SCI.Crypt, 4 Aug 1994.

[HAWA] Hitchcock, H. R., "Hawaiian," Charles E. Tuttle, Co., Toyko, 1968.

[HAWC] Hawcock, David and MacAllister, Patrick, "Puzzle Power! Multidimensional Codes, Illusions, Numbers, and Brainteasers," Little, Brown and Co., New York, 1994.

[HEMP] Hempfner, Philip and Tania, "Pattern Word List For Divided and Undivided Cryptograms," unpublished manuscript, 1984.

[HIDE] Hideo Kubota, " Zai-shi dai-go kokugun tokushu joho senshi." unpublished manuscript, NIDS.

[HILL] Hill, Lester, S., "Cryptography in an Algebraic Alphabet", The American Mathematical Monthly, June-July 1929.

[HIL1] Hill, L. S. 1929. Cryptography in an Algebraic Alphabet. American Mathematical Monthly. 36:306-312.

[HIL2] Hill, L. S. 1931. Concerning the Linear Transformation Apparatus in Cryptography. American Mathematical Monthly. 38:135-154.

[HINS] Hinsley, F. H., "History of British Intelligence in the Second World War", Cambridge University Press, Cambridge, 1979-1988.

[HIN2] Hinsley, F. H. and Alan Strip in "Codebreakers -Story of Bletchley Park", Oxford University Press, 1994.

[HISA] Hisashi Takahashi, "Military Friction, Diplomatic Suasion in China, 1937 - 1938," The Journal of International Studies, Sophia Univ, Vol 19, July, 1987.

[HIS1] Barker, Wayne G., "History of Codes and Ciphers in the U.S. Prior to World War I," Aegean Park Press, Laguna Hills, CA, 1978.

[HITT] Hitt, Parker, Col. " Manual for the Solution of Military Ciphers," Aegean Park Press, Laguna Hills, CA, 1976.

[HODG] Hodges, Andrew, "Alan Turing: The Enigma," New York, Simon and Schuster, 1983.

[HOFF] Hoffman, Lance J., editor, "Building In Big Brother: The Cryptographic Policy Debate," Springer-Verlag, N.Y.C., 1995. (A useful and well balanced book of cryptographic resource materials.)

[HOF1] Hoffman, Lance. J., et. al.," Cryptography Policy," Communications of the ACM 37, 1994, pp. 109-17.

[HOM1] Homophonic: A Multiple Substitution Number Cipher", S- TUCK, The Cryptogram, DJ45, American Cryptogram Association, 1945.

[HOM2] Homophonic: Bilinear Substitution Cipher, Straddling," ISHCABIBEL, The Cryptogram, AS48, American Cryptogram Association, 1948.

[HOM3] Homophonic: Computer Column:"Homophonic Solving," PHOENIX, The Cryptogram, MA84, American Cryptogram Association, 1984.

[HOM4] Homophonic: Hocheck Cipher,", SI SI, The Cryptogram, JA90, American Cryptogram Association, 1990.

[HOM5] Homophonic: "Homophonic Checkerboard," GEMINATOR, The Cryptogram, MA90, American Cryptogram Association, 1990.

[HOM6] Homophonic: "Homophonic Number Cipher," (Novice Notes) LEDGE, The Cryptogram, SO71, American Cryptogram Association, 1971.

[HUNG] Rip Van Winkel, "Hungarian," The Cryptogram, March - April, American Cryptogram Association, 1956.

[IBM1] IBM Research Reports, Vol 7., No 4, IBM Research, Yorktown Heights, N.Y., 1971.

[INDE] PHOENIX, Index to the Cryptogram: 1932-1993, ACA, 1994.

[ITAL] Italian - English Dictionary, compiled by Vittore E. Bocchetta, Fawcett Premier, New York, 1965.

[JAPA] Martin, S.E., "Basic Japanese Coversation Dictionary," Charles E. Tuttle Co., Toyko, 1981.

[JOHN] Johnson, Brian, 'The Secret War', Arrow Books, London 1979.

[KADI] al-Kadi, Ibrahim A., Cryptography and Data Security: Cryptographic Properties of Arabic, Proceedings of the Third Saudi Engineering Conference. Riyadh, Saudi Arabia: Nov 24-27, Vol 2:910-921., 1991.

[KAHN] Kahn, David, "The Codebreakers", Macmillian Publishing Co. , 1967.

[KAH1] Kahn, David, "Kahn On Codes - Secrets of the New Cryptology," MacMillan Co., New York, 1983.

[KAH2] Kahn, David, "An Enigma Chronology", Cryptologia Vol XVII,Number 3, July 1993.

[KAH3] Kahn, David, "Seizing The Enigma: The Race to Break the German U-Boat Codes 1939-1943 ", Houghton Mifflin, New York, 1991.

[KERC] Kerckhoffs, "la Cryptographie Militaire, " Journel des Sciences militaires, 9th series, IX, (January and February, 1883, Libraire Militaire de L. Baudoin &Co., Paris. English trans. by Warren T, McCready of the University of Toronto, 1964

[KOBL] Koblitz, Neal, " A Course in Number Theory and Cryptography, 2nd Ed, Springer-Verlag, New York, 1994.

[KONH] Konheim, Alan G., "Cryptography -A Primer" , John Wiley, 1981, pp 212 ff.

[KORD] Kordemsky, B., "The Moscow Puzzles," Schribners, 1972.

[KOTT] Kottack, Phillip Conrad, "Anthropology: The Exploration Of Human Diversity," 6th ed., McGraw-Hill, Inc., New York, N.Y. 1994.

[KOZA] Kozaczuk, Dr. Wladyslaw, "Enigma: How the German Machine Cipher was Broken and How it Was Read by the Allies in WWI", University Pub, 1984.

[KRAI] Kraitchek, "Mathematical Recreations," Norton, 1942, and Dover, 1963.

[KULL] Kullback, Solomon, Statistical Methods in Cryptanalysis, Aegean Park Press, Laguna Hills, Ca. 1976

[LAFF] Laffin, John, "Codes and Ciphers: Secret Writing Through The Ages," Abelard-Schuman, London, 1973.

[LAI] Lai, Xuejia, "On the Design and Security of Block Ciphers," ETH Series in Information Processing 1, 1992. (Article defines the IDEA Cipher)

[LAIM] Lai, Xuejia, and James L. Massey, "A Proposal for a New Block Encryption Standard," Advances in Cryptology - Eurocrypt 90 Proceedings, 1992, pp. 55-70.

[LAKE] Lakoff, R., "Language and the Women's Place," Harper & Row, New York, 1975.

[LANG] Langie, Andre, "Cryptography," translated from French by J.C.H. Macbeth, Constable and Co., London, 1922.

[LATI] BRASSPOUNDER, "Latin Language Data, "The Cryptogram," July-August 1993.

[LAUE] Lauer, Rudolph F., "Computer Simulation of Classical Substitution Cryptographic Systems" Aegean Park Press, 1981, p72 ff.

[LEAU] Leaute, H., "Sur les Mecanismes Cryptographiques de M. de Viaris," Le Genie Civil, XIII, Sept 1, 1888.

[LEDG] LEDGE, "NOVICE NOTES," American Cryptogram Association, 1994. [One of the best introductory texts on ciphers written by an expert in the field. Not only well written, clear to understand but as authoritative as they come!]

[LENS] Lenstra, A.K. et. al. "The Number Field Sieve," Proceedings of the 22 ACM Symposium on the Theory of Computing," Baltimore, ACM Press, 1990, pp 564-72.

[LEN1] Lenstra, A.K. et. al. "The Factorization of the Ninth Fermat Number," Mathematics of Computation 61 1993, pp. 319-50.

[LEWI] Lewin, Ronald, 'Ultra goes to War', Hutchinson, London 1978.

[LEWY] Lewy, Guenter, "America In Vietnam", Oxford University Press, New York, 1978.

[LEVI] Levine, J., U.S. Cryptographic Patents 1861-1981, Cryptologia, Terre Haute, In 1983.

[LEV1] Levine, J. 1961. Some Elementary Cryptanalysis of Algebraic Cryptography. American Mathematical Monthly. 68:411-418

[LEV2] Levine, J. 1961. Some Applications of High-Speed Computers to the Case n =2 of Algebraic Cryptography. Mathematics of Computation. 15:254-260

[LEV3] Levine, J. 1963. Analysis of the Case n =3 in Algebraic Cryptography With Involuntary Key Matrix With Known Alphabet. Journal fuer die Reine und Angewante Mathematik. 213:1-30.

[LISI] Lisicki, Tadeusz, 'Dzialania Enigmy', Orzet Biaty, London July-August, 1975; 'Enigma i Lacida', Przeglad lacznosci, London 1974- 4; 'Pogromcy Enigmy we Francji', Orzet Biaty, London, Sept. 1975.'

[LYNC] Lynch, Frederick D., "Pattern Word List, Vol 1.," Aegean Park Press, Laguna Hills, CA, 1977.

[LYSI] Lysing, Henry, aka John Leonard Nanovic, "Secret Writing," David Kemp Co., NY 1936.

[MADA] Madachy, J. S., "Mathematics on Vacation," Scribners, 1972.

[MAGN] Magne, Emile, Le plaisant Abbe de Boisrobert, Paris, Mecure de France, 1909.

[MANS] Mansfield, Louis C. S., "The Solution of Codes and Ciphers", Alexander Maclehose & Co., London, 1936.

[MARO] Marotta, Michael, E. "The Code Book - All About Unbreakable Codes and How To Use Them," Loompanics Unlimited, 1979. [This is a terrible book. Badly written, without proper authority, unprofessional, and prejudicial to boot. And, it has one of the better illustrations of the Soviet one-time pad with example, with three errors in cipher text, that I have corrected for the author.]

[MARS] Marshall, Alan, "Intelligence and Espionage in the Reign of Charles II," 1660-1665, Cambridge University, New York, N.Y., 1994.

[MART] Martin, James, "Security, Accuracy and Privacy in Computer Systems," Prentice Hall, Englewood Cliffs, N.J., 1973.

[MAVE] Mavenel, Denis L., Lettres, Instructions Diplomatiques et Papiers d' Etat du Cardinal Richelieu, Historie Politique, Paris 1853-1877 Collection.

[MAYA] Coe, M. D., "Breaking The Maya Code," Thames and Hudson, New York, 1992.

[MAZU] Mazur, Barry, "Questions On Decidability and Undecidability in Number Theory," Journal of Symbolic Logic, Volume 54, Number 9, June, 1994.

[MELL] Mellen G. 1981. Graphic Solution of a Linear Transformation Cipher. Cryptologia. 5:1-19.

[MEND] Mendelsohn, Capt. C. J., Studies in German Diplomatic Codes Employed During World War, GPO, 1937.

[MERK] Merkle, Ralph, "Secrecy, Authentication and Public Key Systems," Ann Arbor, UMI Research Press, 1982.

[MER1] Merkle, Ralph, "Secure Communications Over Insecure Channels," Communications of the ACM 21, 1978, pp. 294-99.

[MER2] Merkle, Ralph and Martin E. Hellman, "On the Security of Multiple Encryption ," Communications of the ACM 24, 1981, pp. 465-67.

[MER3] Merkle, Ralph and Martin E. Hellman, "Hiding Information and Signatures in Trap Door Knapsacks," IEEE Transactions on Information Theory 24, 1978, pp. 525-30.

[MILL] Millikin, Donald, " Elementary Cryptography ", NYU Bookstore, NY, 1943.

[MM] Meyer, C. H., and Matyas, S. M., " CRYPTOGRAPHY - A New Dimension in Computer Data Security, " Wiley Interscience, New York, 1982.

[MODE] Modelski, Tadeusz, 'The Polish Contribution to the Ultimate Allied Victory in the Second World War', Worthing (Sussex) 1986.

[MRAY] Mrayati, Mohammad, Yahya Meer Alam and Hassan al- Tayyan., Ilm at-Ta'miyah wa Istikhraj al-Mu,amma Ind al-Arab. Vol 1. Damascus: The Arab Academy of Damascus., 1987.

[MYER] Myer, Albert, "Manual of Signals," Washington, D.C., USGPO, 1879.

[NBS] National Bureau of Standards, "Data Encryption Standard," FIPS PUB 46-1, 1987.

[NIBL] Niblack, A. P., "Proposed Day, Night and Fog Signals for the Navy with Brief Description of the Ardois Hight System," In Proceedings of the United States Naval Institute, Annapolis: U. S. Naval Institute, 1891.

[NIC1] Nichols, Randall K., "Xeno Data on 10 Different Languages," ACA-L, August 18, 1995.

[NIC2] Nichols, Randall K., "Chinese Cryptography Parts 1-3," ACA-L, August 24, 1995.

[NIC3] Nichols, Randall K., "2erman Reduction Ciphers Parts 1-4," ACA-L, September 15, 1995.

[NIC4] Nichols, Randall K., "Russian Cryptography Parts 1-3," ACA-L, September 05, 1995.

[NIC5] Nichols, Randall K., "A Tribute to William F. Friedman", NCSA FORUM, August 20, 1995.

[NIC6] Nichols, Randall K., "Wallis and Rossignol," NCSA FORUM, September 25, 1995.

[NIC7] Nichols, Randall K., "Arabic Contributions to Cryptography,", in The Cryptogram, ND95, ACA, 1995.

[NIC8] Nichols, Randall K., "U.S. Coast Guard Shuts Down Morse Code System," The Cryptogram, SO95, ACA publications, 1995.

[NIC9] Nichols, Randall K., "PCP Cipher," NCSA FORUM, March 10, 1995.

[NICX] Nichols, R. K., Keynote Speech to A.C.A. Convention, "Breaking Ciphers in Other Languages.," New Orleans, La., 1993.

[NICK] Nickels, Hamilton, "Codemaster: Secrets of Making and Breaking Codes," Paladin Press, Boulder, CO., 1990.

[NORM] Norman, Bruce, 'Secret Warfare', David & Charles, Newton Abbot (Devon) 1973.

[NORW] Marm, Ingvald and Sommerfelt, Alf, "Norwegian," Teach Yourself Books, Hodder and Stoughton, London, 1967.

[NSA] NSA's Friedman Legacy - A Tribute to William and Elizabeth Friedman, NSA Center for Cryptological History, 1992, pp 201 ff.

[OKLA] Andre, Josephine and Richard V. Andree, "Cryptarithms," Unit One, Problem Solving and Logical Thinking, University of Oklahoma, Norman, Ok. Copy No: 486, 1976.

[OKLI] Andre, Josephine and Richard V. Andree, " Instructors Manual For Cryptarithms," Unit One, Problem Solving and Logical Thinking, University of Oklahoma, Norman, Ok. Copy No: 486, 1976.

[OP20] "Course in Cryptanalysis," OP-20-G', Navy Department, Office of Chief of Naval Operations, Washington, 1941.

[PERR] Perrault, Charles, Tallement des Reaux, Les Historiettes, Bibliotheque del La Pleiade, Paris 1960, pp 256-258.

[PGP] Garfinkel, Simson, "PGP: Pretty Good Privacy," O'reilly and Associates, Inc. Sebastopol, CA. 1995.

[PHIL] Phillips, H., "My Best Puzzles in Logic and Reasoning," Dover, 1961.

[PIER] Pierce, Clayton C., "Cryptoprivacy", 325 Carol Drive, Ventura, Ca. 93003.

[POLY] Polya, G., "Mathematics and Plausible Reasoning," Princeton Press, 1954.

[POL1] Polya, G., "How To Solve It.," Princeton Press, 1948.

[POPE] Pope, Maurice, "The Story of Decipherment: From Egyptian Hieroglyphic to Linear B., Thames and Hudson Ltd., 1975.

[PORT] Barker, Wayne G. "Cryptograms in Portuguese," Aegean Park Press, Laguna Hills, CA., 1986.

[POR1] Aliandro, Hygino, "The Portuguese-English Dictionary," Pocket Books, New York, N.Y., 1960.

[RAJ1] "Pattern and Non Pattern Words of 2 to 6 Letters," G & C. Merriam Co., Norman, OK. 1977.

[RAJ2] "Pattern and Non Pattern Words of 7 to 8 Letters," G & C. Merriam Co., Norman, OK. 1980.

[RAJ3] "Pattern and Non Pattern Words of 9 to 10 Letters," G & C. Merriam Co., Norman, OK. 1981.

[RAJ4] "Non Pattern Words of 3 to 14 Letters," RAJA Books, Norman, OK. 1982.

[RAJ5] "Pattern and Non Pattern Words of 10 Letters," G & C. Merriam Co., Norman, OK. 1982.

[REJE] Rejewski, Marian, "Mathematical Solution of the Enigma Cipher" published in vol 6, #1, Jan 1982 Cryptologia pp 1-37.

[RHEE] Rhee, Man Young, "Cryptography and Secure Communications," McGraw Hill Co, 1994

[RIVE] Rivest, Ron, "Ciphertext: The RSA Newsletter 1, 1993.

[RIV1] Rivest, Ron, Shamir, A and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM 21, 1978.

[ROAC] Roach, T., "Hobbyist's Guide To COMINT Collection and Analysis," 1330 Copper Peak Lane, San Jose, Ca. 95120-4271, 1994.

[ROBO] NYPHO, The Cryptogram, Dec 1940, Feb, 1941.

[ROHE] Jurgen Roher's Comparative Analysis of Allied and Axis Radio-Intelligence in the Battle of the Atlantic, Proceedings of the 13th Military History Symposium, USAF Academy, 1988, pp 77-109.

[ROOM] Hyde, H. Montgomery, "Room 3603, The Story of British Intelligence Center in New York During World War II", New York, Farrar, Straus, 1963.

[ROSE] Budge, E. A. Wallis, "The Rosetta Stone," British Museum Press, London, 1927.

[RSA] RSA Data Security, Inc., "Mailsafe: Public Key Encryption Software Users Manual, Version 5.0, Redwood City, CA, 1994

[RUNY] Runyan, T. J. and Jan M. Copes "To Die Gallently", Westview Press 1994, p85-86 ff.

[RYSK] Norbert Ryska and Siegfried Herda, "Kryptographische Verfahren in der Datenverarbeitung," Gesellschaft fur Informatik, Berlin, Springer-Verlag1980.

[SADL] Sadler, A. L., "The Code of the Samurai," Rutland and Tokyo: Charles E. Tuttle Co., 1969.

[SACC] Sacco, Generale Luigi, " Manuale di Crittografia", 3rd ed., Rome, 1947.

[SANB] Sanbohonbu, ed., "Sanbohonbu kotokan shokuinhyo." NIDS Archives.

[SAPR] Sapir, E., "Conceptual Categories in Primitive Language," Science: 74: 578-584., 1931.

[SASS] Sassoons, George, "Radio Hackers Code Book", Duckworth, London, 1986.

[SCHN] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," John Wiley and Sons, 1994.

[SCH2] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," 2nd ed., John Wiley and Sons, 1995.

[SCHU] Schuh, fred, "Master Book of Mathematical Recreation," Dover, 1968.

[SCHW] Schwab, Charles, "The Equalizer," Charles Schwab, San Francisco, 1994.

[SHAN] Shannon, C. E., "The Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol 28 (October 1949).

[SHIN] Shinsaku Tamura, "Myohin kosaku," San'ei Shuppansha, Toyko, 1953.

[SIG1] "International Code Of Signals For Visual, Sound, and Radio Communications," Defense Mapping Agency, Hydrographic/Topographic Center, United States Ed. Revised 1981

[SIG2] "International Code Of Signals For Visual, Sound, and Radio Communications," U. S. Naval Oceanographic Office, United States Ed., Pub. 102, 1969.

[SIMM] Simmons, G. J., "How To Insure that Data Acquired to Verify Treaty Compliance are Trustworthy, " in "Authentication without secrecy: A secure communications problem uniquely solvable by asymmetric encryption techniques.", IEEE EASCON 79, Washington, 1979, pp. 661- 62.

[SINK] Sinkov, Abraham, "Elementary Cryptanalysis", The Mathematical Association of America, NYU, 1966.

[SISI] Pierce, C.C., "Cryptoprivacy," Author/Publisher, Ventura Ca., 1995. (XOR Logic and SIGTOT teleprinters)

[SMIH] Smith, David E., "John Wallis as Cryptographer", Bulletin of American Mathematical Society, XXIV, 1917.

[SMIT] Smith, Laurence D., "Cryptography, the Science of Secret Writing," Dover, NY, 1943.

[SOLZ] Solzhenitsyn, Aleksandr I. , "The Gulag Archipelago I-III, " Harper and Row, New York, N.Y., 1975.

[SPAN] Barker, Wayne G. "Cryptograms in Spanish," Aegean Park Press, Laguna Hills, CA., 1986.

[STEV] Stevenson, William, 'A Man Called INTREPID', Macmillan, London 1976.

[STIN] Stinson, D. R., "Cryptography, Theory and Practice," CRC Press, London, 1995.

[STIX] Stix, F., Zur Geschicte und Organisation der Wiener Geheimen Ziffernkanzlei, Mitteilungen des Osterreichischen Instituts fir Geschichtsforschung, LI 1937.

[STUR] Sturtevant, E. H. and Bechtel, G., "A Hittite Chrestomathy," Linguistic Society of American and University of Pennsylvania, Philadelphia, 1935.

[SUVO] Suvorov, Viktor "Inside Soviet Military Intelligence," Berkley Press, New York, 1985.

[TERR] Terrett, D., "The Signal Corps: The Emergency (to December 1941); G. R. Thompson, et. al, The Test(December 1941 - July 1943); D. Harris and G. Thompson, The Outcome;(Mid 1943 to 1945), Department of the Army, Office of the Chief of Military History, USGPO, Washington,1956 -1966.

[THEO] Theodore White and Annalee Jacoby, "Thunder Out Of China," William Sloane Assoc., New York, 1946.

[THOM] Thompson, Ken, "Reflections on Trusting Trust," Communications of the ACM 27, 1984.

[TILD] Glover, D. Beaird, Secret Ciphers of The 1876 Presidential Election, Aegean Park Press, Laguna Hills, Ca. 1991.

[TM32] TM 32-250, Fundamentals of Traffic Analysis (Radio Telegraph) Department of the Army, 1948.

[TRAD] U. S. Army Military History Institute, "Traditions of The Signal Corps., Washington, D.C., USGPO, 1959.

[TRAI] Lange, Andre and Soudart, E. A., "Treatise On Cryptography," Aegean Park Press, Laguna Hills, Ca. 1981.

[TRIB] Anonymous, New York Tribune, Extra No. 44, "The Cipher Dispatches, New York, 1879.

[TRIT] Trithemius:Paul Chacornac, "Grandeur et Adversite de Jean Tritheme ,Paris: Editions Traditionelles, 1963.

[TUCK] Harris, Frances A., "Solving Simple Substitution Ciphers," ACA, 1959.

[TUKK] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[TUCM] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[USAA] U. S. Army, Office of Chief Signal Officer, "Instructions for Using the Cipher Device Type M-94, February, 1922," USGPO, Washington, 1922.

[VAIL] Vaille, Euggene, Le Cabinet Noir, Paris Presses Universitaires de Frances, 1950.

[VALE] Valerio, "De La Cryptographie," Journal des Scienses militares, 9th series, Dec 1892 - May 1895, Paris.

[VERN] Vernam, A. S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," J. of the IEEE, Vol 45, 109-115 (1926).

[VIAR] de Viaris in Genie Civil: "Cryptographie", Publications du Journal Le Genie Civil, 1888.

[VIA1] de Viaris, "L'art de chiffre et dechiffre les depeches secretes," Gauthier-Villars, Paris, 1893.

[VOGE] Vogel, Donald S., "Inside a KGB Cipher," Cryptologia, Vol XIV, Number 1, January 1990.

[WALL] Wallis, John, "A Collection of Letters and other Papers in Cipher" , Oxford University, Bodleian Library, 1653.

[WAL1] Wallace, Robert W. Pattern Words: Ten Letters and Eleven Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WAL2] Wallace, Robert W. Pattern Words: Twelve Letters and Greater in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WATS] Watson, R. W. Seton-, ed, "The Abbot Trithemius," in Tudor Studies, Longmans and Green, London, 1924.

[WEBE] Weber, Ralph Edward, "United States Diplomatic Codes and Ciphers, 1175-1938, Chicago, Precedent Publishing, 1979.

[WEL] Welsh, Dominic, "Codes and Cryptography," Oxford Science Publications, New York, 1993.

[WELC] Welchman, Gordon, 'The Hut Six Story', McGraw-Hill, New York 1982.

[WHOR] Whorf, B. L., "A Linguistic Consideration of Thinking In Primitive Communities," In Language, Thought, and Reality: Selected Writings of Benjamin Lee Whorf, ed. J. B. Carroll, Cambridge, MA: MIT Press, pp. 65-86., 1956.

[WINK] Winkle, Rip Van, "Hungarian: The Cryptogram,", March - April 1956.

[WINT] Winterbotham, F.W., 'The Ultra Secret', Weidenfeld and Nicolson, London 1974.

[WOLE] Wolfe, Ramond W., "Secret Writing," McGraw Hill Books, NY, 1970.

[WOLF] Wolfe, Jack M., " A First Course in Cryptanalysis," Brooklin College Press, NY, 1943.

[WRIX] Wrixon, Fred B. "Codes, Ciphers and Secret Languages," Crown Publishers, New York, 1990.

[XEN1] PHOENIX, "Xenocrypt Handbook," American Cryptogram Association, 1 Pidgeon Dr., Wilbraham, MA., 01095-2603, for publication March, 1996.

[YARD] Yardley, Herbert, O., "The American Black Chamber," Bobbs-Merrill, NY, 1931.

[YAR1] Yardley, H. O., "The Chinese Black Chamber," Houghton Mifflin, Boston, 1983.

[YOKO] Yukio Yokoyama, "Tokushu joho kaisoka," unpublished handwritten manuscript.

[YOUS] Youshkevitch, A. P., Geschichte der Mathematik im Mittelatter, Liepzig, Germany: Teubner, 1964.

[YUKI] Yukio Nishihara, "Kantogan tai-So Sakusenshi," Vol 17., unpublished manuscript, National Institute for Defense Studies Military Archives, Tokyo.,(hereafter NIDS Archives)

[ZIM] Zim, Herbert S., "Codes and Secret Writing." William Morrow Co., New York, 1948.

[ZEND] Callimahos, L. D., Traffic Analysis and the Zendian Problem, Agean Park Press, 1984. (also available through NSA Center for Cryptologic History)