CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

September 11, 1996
Revision 0

LECTURE 18

LEDGE'S INTRODUCTION TO CRYPTARITHMS III

SUMMARY

It is again my distinct pleasure to present our guest lecturer LEDGE's (Dr. Gerhard D. Linz) third and final lecture on the interesting topic of Cryptarithms. In this lecture, he covers Multiplication, Multiplicative Structures, Base 11 and Base 12 calculations. LEDGE natural writing style, and talent for making understandable some difficult concepts, makes this lecture strong indeed. LEDGE has already produced one of our better references on novice cryptography, and I sincerely appreciate his assistance in our course. Enjoy. [LEDG]

NOMENCLATURE AND SYMBOLS

Lecture 15 included addition and multiplication tables as well as digital squares and cubes for bases 10 through 16. For the additional numerical symbols required for these bases above ten, it used A to represent ten, B for eleven, C for twelve, D for thirteen, E for fourteen and F for fifteen as needed. In lecture 14 we used t for ten and e or E for eleven, the t for bases 11 and 12 and e for base 12. That has been the custom in the Cryptarithm column in The Cryptogram. We will continue the latter usage in this lecture. The usage in lecture 15 has the virtue of consistency as, for instance, A is used for ten in all the higher bases. Once understood, the tables should occasion no difficulty. Furthermore, base 16 was called "Sexdecimal." Those of you knowing some computer programming recognize it as "Hexadecimal."

As we are restricted to ASCII symbols, we will be using "*" as the symbol for multiplying and "**" for exponentiation. Thus 3 * 4 is three times four and 4**3 is four raised to the third power or four cubed.

INTRODUCTION

In this lecture we will be looking at some more complex cryptarithms: those involving roots of 2 and higher in bases higher than 10, exponentiation, and base 10 problems that give minimal clues and require more of what is called brute force methods. To aid our understanding of cube roots we will first revisit square root arithmetic to gain a deeper understanding of what that procedure involves.

SQUARE ROOTS

First, let's look at the extraction of a square root using numbers rather than letters but presented in the same form as a cryptarithm problem.

```
          1  9  4  1
        ____________
      V 3'76'85'04
       -1
        ----
        2 76
       -2 61
        -------
          15 85
         -15 36
          --------
             49 04
            -38 81
             -----
             10 23
```

The difference in this presentation as compared with that in the first cryptarithm lecture is that we do not have the numbers at each level that were multiplied by their respective digits in the answer. Thus after the first level we see that 261 is to be subtracted from 276, but we do not know that it resulted from the product of 9 times (20 * 1) + 9 or as we pointed out before, b * ((20 * a) + b).

If you look closely at the process of extracting this square root, you will see that it is a process of continual refinement of the trial square root by subtracting the increment added to the square of the trial root successively from the original number. Having marked off every two digits starting at the decimal point, the process starts off with an approximation using only the leftmost or highest order digits of the original number and subtracts the highest number that could be the square root of that digit or digits. In this case the highest order digit(s) in the number is the digit 3. It's square root is between 1 and 2. Because the square of the root should not exceed the 3, we choose the number 1 as the first digit of the root and subtract it's square from 3. Then we pull down the next pair of digits, 76. Now we need to estimate the root of 376. For that we need a second digit to the left of the 1. If we call the first digit "a" and the second digit "b", we want the highest possible number such that (a + b)**2 does not exceed 376.

Unless you are aware of it, you may not have recognized that the number 1 in the quotient is no longer just itself. It has become the highest order digit of a two digit number. That means that it has become a ten. The square that we are looking for has become:

(10a + b)**2

If you remember your algebra, you will remember that when we expand this expression we get:

100a**2 + 20a*b + b**2

But 100a**2 is the square of the first number in the trial root. We have already subtracted it from the number for which we computing the square root and we don't want to subtract it again. Hence we need the number (10a + b)**2 - 10a**2 the incremental difference b makes. In this case since b = 9, we would need to compute 19**2 - 10**2 giving us 361 - 100 = 261, and that is just the number below the 276. If you have a calculator you can use (no, it isn't cheating), you can perform that arithmetic process quickly and painlessly.

Having subtracted the 261 from 276, we bring down the next pair of digits, the 85. Now we need the highest root of 37685. It's at least 190 and no more than 199. The example suggests 4 as the next trial digit. Now a = 190 and b = 4. We have to calculate the value of 194**2 - 190**2. You can see the value of having a calculator here. It computes to 1536 which we can subtract from 1585 nicely. It's not too large or too small.

Now look what's happened from this viewpoint. We have subtracted successively 10,000, 26,100, and 1,536 from 37,685. Those first three subtractions total 37,636 which, when subtracted from 37,685, leaves a remainder of 49. You might also have noticed that 37,636 is the square of 194.

There is one more detail to notice. In each subtraction the units digit of the subtracter is the same as the units digit of the square of the trial root digit b with which we are working. 9**2 = 81 or 1 mod 10, the units digit of 251. 4**2 = 16 or 6 mod 10, the units digit of 1536. If you are puzzled by that, look at how we came to those subtracters. Except for the square of the trial digit, all other products involve "a" which ends with zero!

A DUODECIMAL SQUARE ROOT

Now let's solve the duodecimal square root problem, C-6, in the May-June, 1996, issue of The Cryptogram. It's by ARIES and has a key that is two words, 0 - E.

Here is the problem:

```
            N  N  C
           _______
         VON'LY'IF
          CT
          -----
          IA LY
          IB TT
          --------
           I SL IF
           I RB OT
             -----
             II SC
```

1) Try to spot zero. Failing that, list all the letters that cannot represent zero. The highest order digits of the numbers cannot be zero. Numbers in the quotient that produce non-zero subtracters cannot be zero. So far, then, N, C, O and I are not zero. Next look for numbers. either units digits that are not zero or differences of zero. That adds T, L and A to the list. Finally, add S from the last subtrahend, ISLIF, since R is subtracted from it and does not (cannot produce a carry to the next higher digit. That leaves B, F, R and Y as the only candidates for zero. Although the letter representing zero has not been identified conclusively, the information so far recovered will prove useful.

2) Next notice the units digit of the squares in the root, The units digits of N**2 and C**2 are both T. None of digits are zero. None of the squares unit digits are N or C. Finally, both squares have the same units digit. We know that N**2 is a two digit number. Considering the length of the last of the last subtracter, five digits, it is reasonable to hypothesize that C**2 is also a two digit number. Now look at the table of duodecimal squares given in Lecture 15 with special attention to the two-digit ones:

```
N     5    6    7    8    9    t    e
n**2 21   30   41   54   69   84   t1
```

The squares of 6 and 9 do not meet the conditions - T is not zero and a square cannot end with the digit that is its root.

3) Now the subtracter, IBTT, can be calculated.

```
N(12) NN(12) NN(10) NN**2(10) NO**2(10)diff(10) diff(12)
  5      55      65      4225        3600     625 441
...
  8      88     104     10816        9216    1600 e14
  t      tt     130     16900       14400    2500 1544
```

The first column is the estimated value of the digit N. The number in the parentheses is in each instance the base, here 12. The next column is the entire trial root base 12, NN, here 55. That's converted to base 10 in the next column (5*12 + 5). In the next column that last number is squared. The fifth column reports the base 10 square of a, 50 base 12 or 60 base 10. The next column reports the difference of the two squares base 10. The final column is the base 12 equivalent of the difference. We compute the base 12 equivalent by successive division of the base 10 number by 12 as follows:

```
12/625
   ***
 12/52 r1          625 = 52*12 + 1
    **
     4 r4          625 = 4*12**2 + 4*12 + 1
```

Starting with the last quotient and appending each remainder from the last in turn to the first produces 441 as the proposed base 12 value of IBTT. As can be seen, that value is much too small by one digit. When N is 8, the value is still too small. N = 9 was eliminated (remember why?). When t is used as the value for N, the number IBTT becomes 1544. The repeated 4 clinches it as it matches the repeated T. Now I = 1, B = 5, T = 4, N = t, and C = 8. As a check, N**2 = CT or 84. That's consistent with our result.

4) To find the value of F, we note that F - T = C base 12. substituting known values F - 8 = 4; hence F = 12 (base 10!!!) or F = 10 base 12 or 0 mod 12.

5) Knowing the value of the root, NC, the value of the last subtracter, IRBOT, is determined by computing NNC**2 -NN0**2 as in the above tabular method. Do it. You should get 12594 (1568**2-1560**2 base 10). Remember tt8 base 12 converts to base 10 as 10*144 + 10 * 12 + 8.

6) From the last subtraction the values of S and L can be found. From the other subtractions the values of A and Y can now be identified. Putting all known values in a key table produces ???.

CUBE ROOTS

The square root process can be extended to the extraction of any higher order root, in the present instance to cube roots. The process is again extending trial cube roots one digit at a time for a closer and closer approximation to the root. Since cube roots are involved, the number whose root is to be extracted is marked after every third digit from the decimal point. The digit or digits before the last mark (the highest order digits) provide the means of estimating a single digit root. That digit should produce the highest cube possible without exceeding the number made by the highest digit(s). The cube of that digit, a, is then subtracted from the number, and the next group of letters is brought down. A second digit, b, is then selected such that the cube of ab (not a * b) is as high as possible without exceeding the number. That process is continued until the units digit of the original number has been brought down and the last increment subtracted.

Since a is the first digit and b the second we need the difference of (10*a + b)**3 - a**3. (Remember that the 10 in this instance represents the value of the base, not decimal 10. 10 base 12 = 12 base 10.) Expanding the above expression yields a longer expression to evaluate: 1000*(a**3) + (300a**2)*b + (300a) *b**2 + b**3 - 1000*(a**3). "b" can be factored from the result giving: b*(300a**2 + 300a*b + b**2). Knowing a and b, the value of that expression can be computed and then subtracted. But it's easier to compute the unexpanded form as was done with square roots.

A UNIDECIMAL CUBE ROOT

Now let's tackle an undecimal cube root presented in the May-June issue of The Cryptogram by FIBBER. It has a key of two words, 1-0. Here's the problem:

```
   E   L   I
3_____________
VWIE'LDI'EST
 WYT
 -------
  IW LDI
  WS DEE
  ----------
   W AYA EST
   W TIL PLA
     -------
     LNT NDP
```

1) Following the same steps as before try to identify the letter representing zero, or at least the non-zero letters. Here we are more fortunate than before. I - Y = I. If Y were = t, borrowing from W of WIE would be necessary. The evidence indicates no such borrowing could have taken place; thus Y = 0. Along the way we might notice that W - S = W. Since Y = 0 and we're working in base 11, S = t.

2) Now to identify the value for E. E**3 = WYT, a three digit number whose second digit is zero and ends in a digit different from E. In the table of unidecimal cubes from lecture 15 we get:

```
N      5    9
N**3 104  603
```

These two are the only ones that meet all the discovered criteria. Can we find other evidence to be able to decide between them? It turns out we can.

When the T of WYT is subtracted from the E above it, the remainder is W, i.e., E - T = W mod 11. We can make a table.

```
E  T  E-T  W
5  4   1   1
9  3   6   6
```

Both values are consistent with the evidence. Hence E = 5 or 9. Since I - W -1 = 0 on the next subtraction, I = W + 1. If E =5, W = 1 and I = 2. If E = 9, then W = 6 and I = 7. We'll carry both possibilities to the next step.

3) The next task is to identify L, if we can. L**3 ends in E as we can determine from the second subtracter, WSDEE. If E = 5, L**3 ends in 5. We look in the table of cubes again and find only one cube that ends in 5, namely 25, the cube of 3. So L = 3. If E = 9 the cube of L must end in 9. There is again only one such cube: 4**3 = 59, thus L = 4. So if E = 9, then L = 4. There is no conflict.

4) Now it's possible to calculate WSDEE. It is EL**3 - E0**3.

```
EL(11) EL(10) E0(11) E0(10) EL**3(10) E0**3(10) diff(10) diff(11)
  53     50     58     55    195,112   166,375    28737   1t655
  94    103     90     99    970,299   729,000   241,299 too big
```

You probably know the process involved for each step, but here's the explanation if you don't understand it all. Since E = 5 and L = 3, EL is 53 base 11. That's converted to base 10 by computing 5*11 + 3 = 55 + 3 or 58 base 10. Similarly

for E0 base 11 becomes 5 * 11 + 0 = 55. The cubes and the difference should be self-explanatory. To compute the base 11 value of 28737 base 10 repeated division by 11 is necessary as follows:

```
11/28737
   -----
 11/2612 r5   28,737 = 2612*11 + 5
    ----
  11/237 r5   28,737 = 237*11**2 + 5*11 + 5
      --
   11/21 r6   28,737 = 21*11**3 + 6*11**2 + 5*11 + 5
       -
       1 rt   28,727 = 1*11**4 + t*11**3 + 6*11**2 +
       5*11 + 5 or 1t655
```

Hence, WSDEE = (starting with the last quotient and going up the remainders) 1t655. Since W, S and E have already been identified, D = 6 can be added to the list.

5) Now the remaining letters can be identified. They are A, P and N and can be computed in that order from the subtractions. It remains only to write out the key table.

6) Could we now compute the last subtracter even without knowing the values of S, D, P, A, or N. The answer is yes, of course, as we need only the values of the digits in the root, 532. The subtracter is 532**3 - 530**3 base 11

```
ELI(11) ELI(10) ELO(10) ELI**3(10) ELO**3(10) diff(10) diff(11)
  532     640     638    262144000  259694072   2449928 1423738
```

1423738 checks out with the numerical equivalent of WTILPLA. Remember to use successive division by the base or 11 on the base 10 difference to recover the base 11 equivalent.

A FOURTH ROOT PROBLEM, BASE 15

The methods used on the square root and cube root problems will work quite as well on higher order roots and higher bases. To demonstrate the truth of that let's look at the C-Sp-1 in the March-April, 1996, issue of The Cryptogram by CROTALUS, the capable editor of the Cryptarithm column. It's a fourth root problem in base 15 with a key consisting of three words, 1-0. You will remember that base 15 requires 15 different numerical symbols. The first ten are the digits from 0 to 9. The other five are A, B, C, D, and E representing respectively 10, 11, 12, 13, and 14. 10 base 15 = 15 base 10. Addition and multiplication tables for base 15 are contained in Lecture 15 as are the squares and cubes of each of the digits. The digits to the fourth power are not presented and will have to be calculated. That's a little chore but not intrinsically difficult. The simplest method is to raise the base 10 equivalent of the digit to the 4th power and convert the result to base 15 using successive division by 15 as was done for bases 11 and 12. The resulting table is as follows:

```
N    1  2  3   4   5   6   7    8    9    A    B    C    D    E
N**4 1 11 56 121 2BA 5B6 AA1 1331 1E26 2E6A 4511 68C6 86E1 B5B1
```

Here's the problem:

```
       S    L    B
     4______________
     VNA'STYS'HIPS
      WH
      -------
      WB STYS
      YR POPB
       -----------
       B'WBAU'HIPS
         GGGN ALUB
        ----------
         LYNA RBNU
```

1) The non-zero letters are S, L, B, N, W, H, Y, G, and U.

2) We can spot the letter representing 1. It has to be the B as the highest order digit of BWBAUHIPS.

3) When S is raised to the fourth power, the result is a two-digit number, WH. Looking at the table above, there is only one such two-digit number with two different letters, namely 56. 3**4 = 56. Hence S = 3, W = 5, and H = 6.

4) Since W - Y = zero, there must have been a borrowing in the previous column's subtraction and Y = W - 1 = 5 - 1 = 4.

5) B - R = B. R cannot = 0 else there would be no necessary borrowing from the W in the next column. So R = (base -1) or 14 or E.

6) In the first subtraction A - H = B or A - 6 = 1; hence A = 7.

7) in the units place of the last subtraction S - B = U or 3 - 1 = U; therefore U = 2.

8) We still have not identified the digit for L. The subtracter associated with it is YRPOPB. It's unit digit is B or 1. Hence L**4 end in 1. Looking at the table, there are eight digits whose 4th power ends in 1. We have to look more deeply to determine the correct one. We know the values of the first two digits and the last digit of the subtracter, YRPOPB Substituting their values we obtain 4EPOP1. We can approximate the base 10 value of that number by expanding it: 4*15**5 + 14*15**4 + P*15**3 + O*15**2 + P*15 + 1. The two highest terms of that expansion are the most significant. They become 3,037,500 + 708,750 = 3,746,250. Following the model used previously we know that the subtracter can be calculate as SL**4 - S0**4. Since we do not know the value of L we must assume one and try it out. Let's take a number from the middle of the pack whose 4th power ends in 1 as does the subtracter. L = 7 will do as a first approximation.

9) Now for the calculation:

SL(15)	SL(10)	SL**4(10)	S0(10)	S0**4(10)	diff(10)	diff(15)
37	52	7311616	45	4100625	3210991	too small
38	53	7890481	45	4100625	3789856	4ECDC1

The first trial difference (base 10) was much below 3,746,250. The second trial difference, with L = 8, is slightly more than the estimated subtracter as can be expected since the less significant digits were ignored in the estimation. Notice also the pattern of the result. The C repeats as expected to match the repeat of the P. P = C and O = D.

10) The key table has become

1	2	3	4	5	6	7	8	9	A	B	C	D	E	O
B	U	S	Y	W	H	A	L				P	O	R	

The value of the rest of the letters can be computed from the various subtractions in the problem. That's left for you to finish.

EXPONENTIATION

Raising a number to a higher power, such as squaring (2nd power), cubing (3rd power) or more has some facets that can be helpful to a solution of a problem involving integer exponents. Generally, such problems are relegated to specials in the Cryptarithm section, although problems involving the extraction of a root are generally not unless they involve other complications.

JE SAURAIS contributed an exponentiation problem that was published as a special in the March-April issue of The Cryptogram. It was a base 10 problem. It's key was one word, 0-1. At worst it could be solved by anagraming, but that is a non-mathematical approach. Here is the problem:

(ELT)**I = SLENTSGNI. (PRA)**N = NPARIA,

Problems like this can involve considerable amounts of trial and error. A calculator (or a computer) can be very helpful. The calculator need not be fancy. One that can handle normal arithmetic operations of addition, subtraction, multiplication and division is adequate. Having one memory to store numbers can make the process simpler. Such calculators are very inexpensive.

The problem, while it will involve some trial and error, has much less of it than might be imagined at first glance. There are more clues than initially meet the eye. First we notice that the exponents, I and N, are digits, i.e., integers having a value of 2 to 9. Next we could count the number of digits in each number. In each case the number to be raised to a power has three digits. In the first equation the result is a nine digit number. In the second a six digit one. Let's examine that more closely.

A two digit number can be as small as 10 and as large as 99. When squared (or raised to the 2nd power) they result in 100 and 9801, Either three or four digits. No square of a two digit number can have fewer or more digits. A three digit number can be as small as 100 and as large as 999. Their squares are 10,000 and 998,001, either five or six-digits. Notice that there is no overlap on the number of digits in the length between powers. We find a similar situation with the cube (3rd power) of those four numbers. 10**3 = 1000 and 99**3 = 970,279: from four to six digits long. 100**3 = 1,000,000 and 999**3 = 997,002,999: from seven to nine digits long. Again there is no overlap between powers. A six-digit number must be the square of a three-digit number or the cube of two-digit number. There is in fact a general rule about the number of digits in the result when a number of known length, L, is raised to a power, P. The maximum length of the result, R-max, is P*L. The minimum length, R-min, is L*(P-1) + 1.

We can apply that information to the above problem. In the second equation, L = 3, R = 6, and power = N. Using the equation for R-max, 6 = 3 * N; hence N = 2. For the first equation, L = 3, R = 9 and power = I. Again using the equation for R-max, 9 = 3 * I or I = 3. If we had seven digits in the result of the second equation and ignored the first equation, we would have solved the equation 7 = 3 * N and N would be greater than 2 (2.33) but not more than 3. We could then safely deduce that N = 3. If we wanted to check on the lower bound of N, we could have used the equation for R-min. The above formulas work for any integer power and any length of the original number.

The second equation contains the letters P, R, and A in both numbers and I in the result, a known number (3). PRA is a number that when squared produces a number whose highest order digit is 2. Another way of saying that is it produces a number between 200,000 and 299,999. The square roots of these numbers extend from 447 to 547. That's 101 numbers to try, if we need to. But we don't. We can narrow the search much more than that. The six-digit result starts NP and three digit base stars with P. We have just found out that P must be 4 or 5 (447-547). Hence the range of the six-digit result is from 240,000 to 259,999. The square roots of these two numbers extend from 490 to 509, a range of only twenty numbers, quite a reduction from 101. Yet, we can even do better than that. Both numbers, base and result end in A so that A**2 = A mod 10. If A were zero, the result of squaring the number would have two zeros at the end. It does not. So A = 1, 5 or 6. Now we have only six numbers to try that are in the correct range and end with a possibly correct digit: 491, 501, 495, 505, 496 and 506. We are looking for a number that has the pattern of NPARIA or 24AR3A OR 25AR3A. Here are the results:

```
ELT        491    501    495     505    496    506
ELT**3  241081 251001 245025 illegal 246016 256036
```

Only the last square gives the correct pattern. Now we know that R = 0, P = 5, and A = 6.

Our key table is

```
0 9 8 7 6 5 4 3 2 1
R       A P   I N
```

Now let's look at the cube. T**3 must = I mod 10 since I is the units digit of the result. I = 3; the only digit that when cubed ends in three is 7 (check the unidecimal table in Lecture 15); hence T = 7. The largest eight digit number is 99,999,999. Since the result is a nine digit number, the base that produced it must be larger than the cube root of 99,999,999. That cube root < 465. The highest order digit of the base, E can be 9, 8, or 4. The last digit, T is 7. The second digit of the base is the same as the second digit of result.

Now let's use intelligent trial and error. For ELT, E = 4, 8, or 9: L = 1, 4 ,8 or 9 and must differ from E; and T = 7. The possible values for ELT are as follows:

487 497 817 847 897 917 947 987

That's only 8 numbers to try. 947**3 = 849,278,123. Match that with the pattern of SLE,NTS,GNI. S = 8, L = 4, E = 9, N = 2, T = 7, G = 1, I = 3. Add those which are new to the key table and read the resulting word. If you have followed the reasoning and understand it, congratulations. Perhaps in the future you will say toyourself, "I can probably do that."

The major lesson to have learned is this: when faced with trial and error, try to limit as much as you can the range of the possible. In the last part of this problem we had identified six of the digits, leaving only four to choose among. Further we able to determine that for ELT, E was had only three possible values, L had four and T was identified. Without any clues, ELT could range from 102 to 987, a range of 886 possibilities less those numbers that have a repeated digit. We were able to reduce that number of permissible values to just eight.

A MORE DIFFICULT ADDITION

Equations and additions can produce more challenges for the solver because often very few if any of the numerical equivalents of the letters can be identified. Algebraic equations involving the digits can be written. These equations are often helpful, but much trial and error is still required. Trial and error is often called brute force, because, while it must be systematically applied, it does not require much deep thinking. Yet is does require some, as we discovered in the previous problem.

Here is an addition problem in base 10 provided by THE RAT as C-11 in the May-June, 1996, issue of The Cryptogram. The key is two words, 9-0.

```
  RATTLE   LO
+ SNAKE  +GO
 ------  ---
 RRKGKK  SGG
```

1) We can identify the following non-zero letters: S, G, L, O, R, E, and probably T. That leaves K, N, and A as the candidates for zero.

2) From the second addition, we can identify S = 1.

3) Also from the second addition, since L cannot be zero (since it's the highest order digit of LO), L = 9.

4) There are two digital sums that could be useful: O + O = G mod 10 and E + E = K mod 10. In each case the sum has to produce a carry of 1 so that L + 1 = 0 mod 10. Hence neither E nor O can be less than 5. G cannot equal zero so O must be 6 or more.

5) Since L + K + 1 = 10 + K, T + A + 1 = G and T + N (+ 1?) = K.

6) We now have enough information to produce a table of known and unknown values to try out, remembering L = 9 and S = 1.

O	G	E	K	(T, A)	N
6	2	5	0		
		7	4		
7	4	5	0		
		6	2		
		8	6		
8	6	5	0		
		7	5		

In case it's not clear, we start each line with a possible value of O: 6, 7, or 8. O cannot be 5, nor 9(L). In each case G = O + O mod 10. Then we start with the smallest possible value for E, 5 and add the resultant value for K which is 0. It turns out that E can be 5 for each value of O. When O is 6, E cannot be 6 but it can = 7. Nor can E be 8 as that would make K = 6. It turns out that E can be 6 or 8 only when O = 7. When O = 8, E can be 5 or 7.

7) Since K occurs four times in the problem, and the value of zero works well for it in each place and occurs in three positions of the table, I have a preference for trying those places first.

8) On the top line where O = 6 and E = 5, T + A + 1 = G: 2 or 12. Because 2 and 0 are assigned to G and K. T + A = 11. Therefore the pair, T, A, can be 8,3; 7,4; or 6,5. We do not know which letter represents which digit. 6,5 is not permissible since O = 6 and E = 5. The two other pairs produce a carry to the next addition: T + N + 1 = K: 10 or T + N = 9. For the 8, 3 pair N = 1 or 6, since 8 + 1 = 9 and 3 + 6 = 9. Nether value of N is permissible. For the 7,4 pair N = 2 or 5, neither of which is permissible. So we abandon O = 6 for the moment. Not permissible means that the results conflict with assignments already made to other letters.

For O = 7, T + A + 1 = 4 mod 10 or T + A = 3, 13. Only 13 is permissible. It is produced by 6, 7; 5, 8; or 4, 9. Since on this line 4, 7, 5, and 9 are already in use, this solution is not permissible. It produced redundancies.

For O = 8. T + A + 1 = 6(G) mod 10 or T + A = 5, 15. 15 can be produced by 8 + 7 but 8 is already assigned. 5 = 2 + 3. No problem. T, A are 2, 3 but maybe not in that order. With T + A = 5 there is no carry to the next addition; hence T + N = 10(K). Since 8 is already assigned, T = 3 and N = 7. A must = 2. No contradictions so far.

9) Let's construct our partial key table and then go back to the problem, if everything looks OK.

```
9 8 7 6 5 4 3 2 1 0
L O N G E   T A S K
```

The only letter left to place is the letter, R, which must be 4.

You can substitute all the digits in the problem and check the answer.

Sometimes it takes courage to tackle a cryptarithm, particularly if it might take you to less well known territory. My best advice is to forge ahead. You cannot lose. Either you will solve the problem and perhaps be surprised by your competence or ingenuity, or you will find yourself stumped, needing to learn something new. Look at a book, or consult with a mathematically inclined friend or a friendly math teacher, someone who can point the way or find a fallacy. That way, you learn and add something you had not known to your armamentarium of mathematical strategies.

You are of course welcome to contact me with a problem, a success, or a new wrinkle you've discovered. If there are problem types you'd like me to write more about, let me know. Phrase any questions as clearly as you can, and I'll see what I can do with them. There's no sin in being stumped - our hobby sees to it that we run into that situation with regularity.

DOUBLE KEY DIVISION

>From time to time a division problem is presented which has two sets of substitutes for the digits, one upper case and one lower case. The sets are complete but keyed differently. The problem is often done in base ten, but occasionally in base 11 or twelve. Such a problem was presented as a special in the September - October, 1994, issue of The Cryptogram. A base twelve problem with two words, 0-1, and FOUR WORDS, 0 to E, was propounded by ARIES. It's presented here written in standard arithmetical form.

```
                r h l d b
              **********
i l l a d/G O L D E N A G E
          i l l a d
          **********
          A Y Y G L N
          l y d t i d
          **********
            U M U Y Y A
            r h i b h y
            **********
              U L O N A G
              r l r e h h
              **********
                S N Y L B E
                d r u c u h
                **********
                  S L D O U
```

As in any division problem, we have a series of multiplications, or products, and a series of subtraction (or additions). The subtractions involve both sets of letters, but, interestingly, the multiplications involve only the lower case letters. We cannot do the subtractions without both sets of letters. We can, however, attack the multiplications by considering only the lower case letters. Let's see what can be done to identify the numerical equivalents of the lower case letters.

As usual, the first effort is to find the letters representing 1 and 0. The letter representing 1 is easy to find: r * illad = illad; so r = 1. The letter for zero is hidden a little better. In the third subtraction, A - y = A; so y = 0. Our equivalent table looks like:

```
0 E X 9 8 7 6 5 4 3 2 1
y                     r
```

So the first of the two words starts with y and the second ends with r. A double-key division problem usually has a lot of products. This one is typical. That characteristic allows us to build a partial multiplicative structure to which we can look for the appropriate diagram (see Lecture 14). Since we are interested at this point only in the units digits of the products, we will use modulo 12 multiplication.

h * illad = lyttid or h * d = d or h => d. Likewise l => y; d => h; and b => h. We can combine this information for the following partial structure:

b => h <=> d and l => y. Since we know that y = 0, l * d = 0; or, finally, l => 0.

Having this much information, we can now look at the base 12 structures in lecture 14. Look them over yourself. There are two possible matches. Can you spot them? It could be a good exercise to stop and try this on your own.

The two that match produce the following table:

```
d     h     b         l
3 <=> 9 <= E, 7      4, 8
8 <=> 4 <= 2, 5, E   3, 6, 9
```

In each case there is only one possible value for d and h on each line. To narrow the possibilities, choosing a product with most letter equivalents partially identified will provide the quickest entry. Such a product is the second one: h * illad = lydtid. The inverse of that is lydtid/h = illad. In other words, if the product is divided by the single digit multiplier that produced it, the divisor of the problem which served as the multiplicand should emerge.

Before doing that, there is more useful information in the problem that may result in the elimination of some of the possibilities. Notice that two of the products have r as their highest order digit Since r = 1, the digit multipliers that produced them must be smaller than the other two letters that also produced 6-digit products. So l and d < h and b. In the first group h (9) is always greater l (4, 8) and d(3). On the other hand, if l = 4, b = 7 or e. If l = 8, b can only be E.

In the second set d > h. But d should be < h. Hence the second set cannot be correct. So we will confine our attention to the first set. Back to the proposed division: h = 9; lydtid is l03ti3. l can be 4 or 8. One of those must be correct. It's a 50/50 chance to guess correctly. Let's start with l = 4.

```
  *********    Remember this is base 12. 4 x 12 + 0 is 48.
9 / 403ti3.    9 goes into 48, 5 times, giving 9 * 5 = 45.
    39         base 10 or 39 base 12 (3 * 12 + 9 = 45).
   ***         Hence i = 5. Subtracting 9 from 0 or 12 =
    33         3. 39 divided by 9 = 4. 4 x 9 = 36 or 30
    30         base 12. Hence l = 4. Since we are looking
    **         for illad, we hope the next quotient will
    3?         be 4 also. Though we don't know t's
    **         equivalent, we do know we can subtract 30
               again! 403ti3 has become 403t53. illad is
               544a3. We move to the end of this
               division. 9 * 3 = 27 or 23 base 12. Hence
               the previous subtraction must have produce
               a 2 in its units place.
```

Since the units digit in the dividend is 5, 9 * a = 3 mod 12. The multiplicative structure and the multiplication table both show that the only possible multipliers of 9 that fit are 7 and E. 7 * 9 = 53 base 12, making t = 5, not possible since i = 5. E * 9 = 83, making t = 8 and a = E. The completed partial product is: 9 * 544E3 = 403853. The equivalent table now becomes;

```
0 E X 9 8 7 6 5 4 3 2 1
y a   h t     i l d   r.   Letters without values are b, c, u and e.
```

"b" is the units value of the quotient. b * 544E3 = 31ucu9. 31 base 12 or 37 base 10 divided by 5 = 7; thus b = 7. If you carry out the multiplication, you will discover the values of u and c. That would leave only one place for e. If you can do a little anagraming, you can read the key without those last computations.

We were fortunate. Had we chosen l = 8, we would soon have run into contradictions leading to the discarding of that possibility.

We have identified all the lower case letter equivalents and not yet one single upper case equivalent. Now that's just a matter of solving five subtraction problems. That shouldn't prove too difficult and will be fine base 12 practice.

Errata for Lecture 14

a) In the explanatory paragraph below the duodecimal Example 4. Division, after writing down the 32 we must first subtract it from 48, making 16 the difference, and then bring down the next digit of the dividend, t.

b) The final product of the duodecimal multiplication at the end of the lecture, before the Appendix, is 7C8e8t8 not 7C8et8 as written. Unfortunately this typo was not spotted in time before publication.

LECTURE 17 ANSWERS

17-1 Headline Puzzle

Paul Derthick's HEADLINE PUZZLE . by Larry Gray

The following are all headlines from a recent daily newspaper. Each of the five is a different mono -alphabetic substitution, and all five are derived from the same mixed alphabet at different settings against itself.

1. PXYWFXKLJE DFYMJYV VGHKJ `DFYM-US' GF ZYFGJVG PJEJYHW VLXGEFDS;

2. JUBHFGO EUHKEOF HR WEUDBGO, FHSJF DKD RO ZGI YRE FUNROI HUED;

3. NEZZY AEZYVKU AEVP NFUVLKY LR ALVVKU JLBPV ECKU AWGBKV;

4. ZEHCGOL LZCCOMMSS WEMSAQ MZALD AFB AZFMS MZ DZBZA MDZAGS;

5. PTQQU WQRKWCQBSD WQEKLLQUBX BZOKWEQ MKW ENJWSQX JUB BZ

ANS:
   Setting = ANOLE   Key = GECKO   Hat= CHAMELEON

17-2 Playfair. While Rome Burns. BARRISTER: ON44:CE17
      Tip= "ers are"

OCMAF ZDAPZ BYPGY BOKYT BYVMT AVIBY PVGPP RBCFH
XEAPI VTCPV VBKGV MEWCB IEGMQ PPBOL ENRHZ MRFSC
DRNAI ZEITN SUNA.

TWO HINTS: The title is significant and does not follow LANAKI's Red Herring rule and look for naturals such as PO = QP or OPQ. A Natural is a cipher digraph not in the keyword whose letters because of the standard alphabetical relationships stay in the natural alphabetical order in the cipher square.

Key Square:

```
H U C K L
E B R Y F
I N A D G
M O P Q S
T V W X Z
```

Message: Pupil's answers are que(x)er, to wit: Nero was a cruel tyrant who would torture his poor subjects by playing the violin.

17-3 Foursquare 'anasonly' ZEMBIE

UB XB MS SF SQ MS TH DE UB HM GL NL BW GB LW NQ NF UB FM
QH EM BW BI GT LD UQ IG WM CF TQ ET CT NF IP LS UQ FK UH
IZ UQ YF TN XP NS FF UV HV NF HI CE NQ UO UQ GK ET HT ND
PV BI BE ND BD YM DE LX UB GA CX ET XT DE PE NL BF PY IQ
NG QW IS NC CK XB TF GK ED LA EL LE RW MI EX SF MS UP XQ
NF EV FF BI KK NA MX.

Answer in complex Caesar: (ISUPV OMPAY - UGBSK NGKPN)
ZKXJO GGKGN SFXPC DYJKP MRPPJ

hints: run down 10 letters ; Look for thinks 2x, germs 2x, if all fails - square to = i/juxtaposition, square 4 = viewpoints.

17-4 Short Bifid. Clue - DIAMONDS is there somewhere and the text talks about them being HIDDEN. Period = 7.

ETIALIG LDMNITV NFEMISI EEIDGEI
HPCEDUT PINOFLW INDLEEK

ANS: The diamonds are hidden in the side pocket of me bosses car.

LECTURE 18 PROBLEMS

18-1 Unidecimal square root. (Three words 0-E) MARSHEN

LO'SE gives root it; - KF = EKSE; - ERRE = EWH

18-2 Duodecimal division. (Two words, 0-E) CODEX

BRIDGE / CLUBS = CC; - DUHRE = BRHEE; - DUHRE = BOLO

REFERENCES AND CRYPTOGRAPHIC RESOURCES

The CDB (Crypto Drop Box) was updated last week with 140,000 bytes of references. I will update them again after Lecture 19 is complete.