Math 314 - Spring 2020
Class Notes - 2/10/2020
Scribe: Cody Price

Attacking The Hill Cipher

Ciphertext Only:

1) Brute-Force - Only feasible when the block size m of the key is small. The possible number of combinations can be found using 26^{m^2} So if $m = 2$, then $26^4 = 456976$ possible combinations.

2) Frequency Analysys - Only feasible when the block size m of the key is small. First find the frequency of all letter pairs in the ciphertext, then contrast them with the frequency of common letter pairs like "TH" or "ER" to guess and test out possible keys.

Known Plaintext: Must know the block size m of the key first. For example, if m = 2, then suppose we know "BO OL" $\rightarrow$ "CN DR" and when converted to numbers 1,14 14,11 $\rightarrow$ 2,13 3,17

$$E(<1,14>) = <1,14> * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = <2,13>$$

$$E(<14,11>) = <14,11> * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = <3,17>$$

Combine the two equations: $\begin{bmatrix} 1 & 14 \\ 14 & 11 \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 13 \\ 3 & 17 \end{bmatrix}$ and set $K = \begin{bmatrix} 1 & 14 \\ 14 & 11 \end{bmatrix}$

Find the inverse of K. $K^{-1} = (a*d - b*c)^{-1} * \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (mod 26)$

$$K^{-1} = (1*11 - 14*14)^{-1} * \begin{bmatrix} 11 & -14 \\ -14 & 1 \end{bmatrix} = 23^{-1} \begin{bmatrix} 11 & 12 \\ 12 & 1 \end{bmatrix} (mod 26)$$

Using multiplication table modulo 26. $23 * 17 = 1$ $K = 17 \begin{bmatrix} 11 & 12 \\ 12 & 1 \end{bmatrix} (mod 26)$

$$K = \begin{bmatrix} 17*11 & 17*12 \\ 17*12 & 17*1 \end{bmatrix} = \begin{bmatrix} 187 & 204 \\ 204 & 17 \end{bmatrix} = \begin{bmatrix} 5 & 22 \\ 22 & 17 \end{bmatrix} (mod 26)$$

$$\begin{bmatrix} 5 & 22 \\ 22 & 17 \end{bmatrix} * \begin{bmatrix} 2 & 13 \\ 3 & 17 \end{bmatrix} = \begin{bmatrix} 5*2+22*3 & 5*13+22*17 \\ 22*2+17*3 & 22*13+17*17 \end{bmatrix} = \begin{bmatrix} 76 & 439 \\ 95 & 575 \end{bmatrix}$$

$$= \begin{bmatrix} 24 & 23 \\ 17 & 3 \end{bmatrix} (mod 26) \qquad Key = \begin{bmatrix} 24 & 23 \\ 17 & 3 \end{bmatrix} (mod 26)$$

Chosen Ciphertext: Choose "BA AB" which when converted to numbers is 1,0 0,1

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1*a+0*c & 1*b+0*d \\ 0*a+1*c & 0*b+1*d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = Key$$

Let's say the $Key = \begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix}$ then $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix} = \begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix} = Key$

One Time Pad

This encryption uses the Vigenere cipher, but with the following constraints - key is the same length as the plaintext, the key is completely random letters, and the key is only used a single time. This encryption method has perfect secrecy, meaning that it is mathematically impossible to break. However, it is also considered to be very impractical due to the key needing to be shared beforehand and often being very long.

Euclid's Algorithm

This algorithm uses division with remainder to compute the GCD (greatest common divisor) of two numbers much faster than by trying all possible divisors.

Theorem: Given positive integers a and b, there exists integers q and r, where $a = q * b + r$ when $0 \leq r \leq b$

Proof: Fix a and b, pick $q = \lfloor \frac{a}{b} \rfloor$, pick $r = a - b * q$ and add $b * q$ to both sides to get $a = r + q * b$
now to show $0 \leq r \leq b$, since $\frac{a}{b} - 1 < q < \frac{a}{b}$, multiply through by b getting $a - b < q * b < a$
since $a * b \leq a$, $\quad o \leq a - q * b \leq r$, $\quad$ so $r \geq 0$, $\quad$ since $a - b < q * b$
therefore $a - b * q < b$, $\quad$ so $r < b$

Finding GCD: Take $gcd(a, b) = d$ and use the division with remainder $a = q * b + r$. If $d|a$ and $d|b$ then $d|r$ also if $a|r$ and $d|b$ then $d|a$. So $gcd(a, b) = gcd(b, r)$, since $r < b$. Now if we repeat this process until we get a remainder of 0.

Example: Find $gcd(162, 21)$

$162 = 7(21) + 15$, so then $gcd(162, 21) = gcd(21, 15)$

$21 = 1(15) + 6$, so then $gcd(21, 15) = gcd(15, 6)$

$15 = 2(6) + 3$, so then $gcd(15, 6) = gcd(6, 3)$

$6 = 2(3) + 0$, since $r = 3$, then $gcd(6, 3) = 3$, therefore $gcd(162, 21) = 3$