HW #1

Travis Collins
traviscollins@wpi.edu
ECE 578 Crytography and Data Security

September 3, 2012

1 Ciphertext 1

Methodology:
The first process was to determine what cipher was used, which was done by utilizing the attacks demonstrated in class. Starting with the easy attacks and working my way upward the attack that produced results was the Affine cipher. This was discovered by the brute force method, which is quite reasonable since there are only

$$26 * 12 = 312$$

possible permutations. This was done by loading the text into MATLAB for visual inspection and

Translated:
This is time for all good men to come to the aid of their party!

2 Ciphertext 2

Methodology:
I used the same process as before to determine the cipher type for the encrypted text. It reduced quickly to a Vigenere Cipher, which was quite evident by inspection of the text itself. The first step in deciphering a Vigenere Cipher is to determine the keyword length. This was done by finding the longest repeated words in the text, determining their distance apart, and

finally taking the "GCD" of that distance. The keyword then was determined to be 5. The next step was to determine the shift distances or the keyword itself. This was done by assume original words for encrypted text, measuring the distance of the ciphered text letter to the plaintext letter for repeated or assumed repeated words. These shifts were determined to be:

7169211

or the keyword "krypt". **Translated:**

Matlab Code

$$-$$

$$-$$

$$\not\approx$$

$$> \not\approx$$

$$-$$

$$\not\approx$$

$$-$$

$$-$$

$$\not\approx$$

$>$

$\not\asymp$

$-$

$\not\asymp$

$-$

$-$

$\not\asymp$

$>$

$\not\asymp$

$-$

$\not\asymp$

$-$

$$
\begin{aligned}
&- \\
&\not\asymp \\
&> \\
&\not\asymp \\
&- \\
&\not\asymp \\
&-
\end{aligned}
$$