MATH 314 - Class Notes

09/06/2016

Scribe: Jarrett Booz

Summary: Today's class covered an example decryption of an Affine Cipher, an example of a substitution cipher, and the Vigenere Cipher.

Notes:

Staring with an example decryption of an Affine Cipher:

In order to decrypt an Affine Cipher, we need to know what 2 letters decrypt to. That is, we can perform a known ciphertext attack if we know what 2 letters of the ciphertext decrypt to in the plaintext.

If we know: $C \to j$ and $U \to z$ we can figure out the key.
To determine the key we will use this equation:

$$E(x) = \alpha x + \beta$$

When using this equation to decrypt, $E(x)$ will be exchanged for the value of the plaintext letter and the variable x will be replaced by the value of the ciphertext letter.

So, in this example, we will have 2 equations, which correspond to the letters that we know the decryptions to :

$$\alpha(2) + \beta = 9$$
$$\alpha(20) + \beta = 25$$

We can use algebra to solve for one of the variables, β first in this example.
We can multiply the first equation by 10 and reduce mod 26 to get:

$$10\alpha(2) + 10\beta = 12$$

Subtract this new equation from the second equation which results in:

$$9\beta = -13$$

Since mod 26 does not allow us to use traditional division, the next step must be to multiply by the inverse of 9 (mod 26) on both sides of this equation. This results in :

$$\beta = 13$$

Now that we know that $\beta = 13$ we can substitute this in to the original equations and solve to determine what α is:

1. $2\alpha + 13 = 9$

$$2\alpha = 22$$

$\alpha = 11$, or $\alpha = 24$

2. $20\alpha + 13 = 25$

$$20\alpha = 12$$

$\alpha = 11$, or $\alpha = 24$

We know from the previous class that any value of α does not work out well with mod26 arithmetic. We can determine that the value of α must be 11 because 24 shares factors with 26.

This leaves the decipher equation being :

$$E(x) = 11x + 13$$

The next topic that was discussed was related to Caesar and Affine Ciphers, both of which are **monoalphabetic ciphers**. This means that each letter in the plaintext can only correspond exactly 1 letter in the ciphertext.
The general form of a monoalphabetic cipher is the Arbitrary Substitution Cipher, in which each letter of the plaintext is given an arbitrary corresponding ciphertext letter.
An online example of how easy it is to crack the arbitrary substitution cipher was given after we discovered that the probability of randomly guessing the key is equal to 26!

Next we discussed the Vigenere Cipher. The Vigenere Cipher is a **polyalphabetic cipher**. This means that each letter of the plaintext can have 1 or more corresponding letters in the ciphertext. This makes frequency analysis attacks (like we used to crack the caesar and substitution ciphers). To perform the Vigenere Cipher we must:

- Pick a KEY word/phrase/document
- Convert the letters of the KEY to numbers (mod 26) and treat this as a vector
- Write the plaintext message out as numbers (mod 26)
- Write the KEY vector out below the plaintext vector. The KEY vector should be repeated as many times as it is necessary.
- Add the two vectors (mod 26). This is the encryption function

Example:
KEY = "vector" $=< 21 \quad 4 \quad 2 \quad 19 \quad 14 \quad 17 >$
Message = "here is how it works"

Message	7	4	17	4	8	18	7	14	22	8	19	22	14	17	10	18
KEY	21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19
+(mod 26)	2	8	19	23	22	9	2	18	24	1	7	13	9	21	12	9
C.T.	C	I	T	X	W	J	C	S	Y	B	H	M	J	V	L	J