MATH 314 Spring 2018 - Class Notes

1/29/2018

Scribe: Jordan Puglisi

Summary: Today's class covered the brief history of many different encryption methods. These methods went back in time to be as simple as a message on a piece of leather that would be wrapped around a stick to the Caesar Cipher which would encrypt a message using a key with the key being the number of alphabet letters shifted. Eventually the Vigenre Cipher was created and was seen as "unbreakable" due to the fact that one letter was not encoded the same every time it occurred. Enigma machines were then created and began to be used in WWII to encrypt messages. These encryption methods rapidly advanced and were always seen as "unbreakable" until they were broken and a better system had to be created up until today's use where our encryption algorithms have become very advanced.

Caesar Cipher : Take plain text shift it by some fixed amount

Modular Arithmetic : Convert letters to numbers

$A \equiv 0, B \equiv 1, ., ., ., Z \equiv 25$
$BAT \equiv B(1)A(0)T(20)$

Encryption in the Caesar cipher is addition by a key:

- Fix the key $k = 7$
- BAT $\rightarrow$ B(1) A(0) T(20) (based on the index of the letter in the alphabet with $A = 0$)
- 8 7 27 (values obtained by shifting or adding the key to the values we established in the step above)
- I H B (the letters corresponding to the new indexes we found)

To make the letters wrap around we use modular arithmetic:

- Fix a modulus 26
- Instead of writing down a number we write down the remainder we get when we divide by 26.
- Notation: $27 \equiv 1 \pmod{26}$ meaning that 27 is a B because the remainder found from doing a modulus operation becomes the new index for that value.

How do we decrypt a Caesar cipher? Subtraction!
Encryption Function: $E(x) \equiv x + k \pmod{26}$
Decryption Function: $D(x) \equiv x - k \pmod{26}$

How many keys are there for the Caesar cipher?

- The key is only important mod(26)
- Only 26 possibilities for k (0-25)
- Normally k is between 1 and 25.