Cryptography 2/24

Reagan Shirk

February 24, 2020

Midterm

- The midterm will be March 4th
- Very similar to the homework, if we can do the homework we should be fine
- We'll have an review session on Monday
- Closed book but we can bring in two front and back letter sized note sheets
  - We can write anything and it doesn't matter if they're handwritten or typed
- No calculator
- Won't get our midterm back
- I think he just implied that he'll change numbers from homework problems but outside of that they'll be the same
- He mumbled something about algorithms and theorems

Encryption

- Looks like we're talking about Alice and Bob
- Alice and Bob share a channel which is assumed to be insecure, how insecure is it?
- The attacker tries a passive attack, we call the attacker Eve (the name comes from eavesdrop lol)
  - She's just listening, not doing anything
  - Recording, I guess that's doing something
- The messages are in a plain text space
  - Sending a message directly over the channel would be dangerous
  - You want an encrypted message
  - We want the cipher text to be in a cipher text space
  - This requires an alphabet? I was guessing my password to MyFitnessPal and missed a second of what he said
- The cipher text can go through the insecure channel
  - you need an encryption key
  - once the message gets to Bob, he'll run a decryption algorithm and use the decryption key

Caesar Cipher

Plain Text	Cipher Text
A	F
B	G
C	H
D	I
E	J
F	K
G	L
H	M
I	N
J	O

Plain Text	Cipher Text
K	P
L	Q
M	R
N	S
O	T
P	U
Q	V
R	W
S	X
T	Y
U	Z
V	A
W	B
X	C
Y	D
Z	E

- OKLAHOMA $\rightarrow$ TPQFMTRF
- The encrytpion key is 5, the decryption key is $-5 = 21$
- Cryptology is the study of the cryptographer, cryptography, and cryptoanalysis