# Computer Security

*Reagan Shirk*

*September 1, 2020*

## Quiz

- There'll be a quiz sometime soon, he'll mention it in the lecture before the quiz
- We'll have a quiz on Thursday (same day as Algo quiz for those in both classes)
- All eligible content will be every lecture up until that quiz
- Q: what will the format of the quiz be?
    - He said it'd be diverse…?
    - Written, not on canvas unless you're a student who can't come to in person classes
    - Open book, computer, everything. Can't talk to others though (tests are not but quizzes are)

## Lab

- We'll have enough information to start on the first lab after today
- I think he said it should be pretty easy?
- He'll let us know if we need to install any extra software

## Cryptography

- Cryptography is the art of secret writing
- Takes a string and makes it look random
    - the catch: it has to be reversible (i.e. you have to be able to get the original message from the encrypted one)
- Cryptography and compression: do you encrypt or compress first?
    - Normally we compress first, then encrypt

### Cryptography vs Steganography

- Cryptography requires encryption, steganography is just hiding the message (like with invisible ink, or making every second letter of a word spell something)
- Cryptography hides the message itself, not the fact that the message exists. Steganography hides the fact that the message exists, not the message itself
- Formal definition: cryptograhy conceals the contents of communication between two parties

### Encryption/Decryption

- Plaintext: a text in its original form
- Ciphertext: a text after encryption
- Encryption: the process of transforming plaintext into ciphertext
- Decryption: the process of transforming ciphertext into plaintext
- Key: the value used to control encryption/decryption (you have an encryption/decryption key)

- When the encryption key = the decryption key, it is private key cryptography and the key needs to remain secret
- When the encryption key ≠ the decryption key, it is public key cryptography and only one key is secret

## Cryptanalysis

- The opposite of cryptography- cryptanalysis is the art of revealing the secret
  - The goal is to defeat cryptographic security systems and gain access to the real content of encrypted messages
  - Cryptographic keys can be unknown
- The difficulty depends on the sophistication of the encryption/decryption and the amount of information available to the cryptanalyst

### Ciphertext Only Attacks

- Attacks when only the attacker only knows a set of ciphertexts
- Breaking the cipher requires analysis of patterns in the ciphertext
  - patterns provide clues about the plaintext and the key

### Known Plaintext Attacks

- The attacker has both the plaintext and the ciphertext- you can find the key with this information

### Chosen Plaintext Attacks

- An attacker has the ability to choose arbitrary plaintexts to be encrypted and is able to get the associated ciphertexts
  - how tf is this possible?
  - I missed the explination - I'll try to catch the recording

## Example

- Alice wants to send "sell the business" to Bob
- She encrypts it by replacing each letter with the one that is 3 letters later in the alphabet (i.e. a → d, b → e)
- What is the plaintext?
  - sell the business
- What is the ciphertext?
  - vhoo wkh exvlqhvv
- How to encrypt?
  - replace the plaintext character with the character in the alphabet that comes three letters later
- How to decrypt?
  - do the opposite of encryption, replace each letter with the letter in the alphabet that is 3 before it
- What is the key?
  - 3
- Cryptanalysis attacks?
  - you could use all three to break this system

## Perfectly Secure Ciphers

- Ciphertext that does not reveal any information about which plaintexts are likely to have produced it
  - i.e. hiding any patterns in the words
  - This cipher is robust against ciphertext only attacks
- Plaintext does not reveal any information about which ciphertexts are more likely to be produced

## Computationally Secure Ciphers

- The cost of breaking cipher quickly exceeds the value of the encrypted information, and/or
  - i.e. breaking the cipher takes too much time/many than what the information is worth
- Missed the other thing, I'll catch it in the recording

## Secret Keys vs Secret Algorithms

- Keeping algorithms a secret:
  - Can acheive better security
  - Hard to keep secret if its used widely though
- Public the algorithms
  - Security depends on the secrecy of the keys
  - Less unknown vulnerability if all of the good people in the world examine the algorithms
- The military has both secret keys and secret algorithms

## Caesar Cipher

- Replace each letter with one 3 letters later in the alphabet
  - cat → fdw
- This cipher is trivial to break - it takes 26 tries at most to break

## A variant of Caesar Cipher

- Replace each letter by one that is any number of positions later
- Trivial to break with modern computers - something about them only needing 5 tries?

## Mono-Alphabetic Ciphers

- A generalized substitution cipher- randomly map one letter to another
- How many possibilities does this create?
  - $26! \approx 2^{88}$
- The key must specifiy which permutation- how many bits does that take?
  - $26 = 5$ bits
  - $26! = 88$ bits