AP Computer Science Principles
Unit 4 Test Review

Name: Key

1. Vocabulary

- Big Data - a broad term for datasets so large or complex that traditional data processing applications are inadequate
- Moore's Law - a prediction made by Gordon Moore in 1965 that computing power would double every 1.5-2 years, it has remained more or less true ever since
- Caeser Cipher - a technique for encryption that shifts the alphabet by some number of characters
- Cipher - the generic term for a technique (or algorithm) that performs encryption
- Cracking encryption - when you attempt to decode a secret message without knowing all the specifics of the cipher, you are trying to "crack" the encryption.
- Decryption - a process that reverses encryption, taking a secret message and reproducing the original plain text.
- Encryption - a process of encoding messages to keep them secret, so only "authorized" parties can read it.
- Random Substitution Cipher - an encryption technique that maps each letter of the alphabet to a randomly chosen other letter of the alphabet
- Vigenère Cipher - a method of encrypting text by ~~encrypting~~ applying a series of Caesar ciphers based on the letters of a keyword

- Computationally Hard - a "hard" problem for a computer is one in which it cannot arrive at a solution in a reasonable amount of time
- Asymmetric Encryption - used in public key encryption, it is a scheme in which the key to encrypt data is different from the key to decrypt
- Modulo - a mathematical operation that returns the remainder after integer division
  ex: $7 \bmod 4 = 3$
- Public Key Encryption - used prevalently on the web, it allows for secure messages to be sent between parties without having to agree on, or share, a secret key. It uses an asymmetric encryption scheme in which the encryption key is made public, but the decryption key is kept private
- SSL/TLS - an encryption layer of HTTP. When you see the little lock icon and "HTTPS" it means you are visiting a website over HTTP but the data going back & forth between you & the server is encrypted (use PKC)
- DDoS - typically a virus installed on many computers (thousands) activate at the same time & flood a target w/ traffic to the point the server becomes overwhelmed - doing this can render web services like DNS, or routers, or certain websites useless or unresponsive.
- Phishing - typically a thief trying to trick you into sending them sensitive information. Typically these include emails about system updates asking you to send your username and password, SSN or other things.
- Virus - a program that runs on a computer to do something the owner does not intend. Viruses can be used as a Bot Net to trigger a DDoS-style attack, or they can spy on your computer activity
- Two-Factor Authentication - adds extra security by requiring more than just your password. (often a security code sent to your phone.

Please answer the following questions:

2. What is different about Big Data compared to data we have learned in the past and what is an example of it?

- traditional processing applications are inadequate
- there are more challenges with how to analyze and store this data

3. Explain one data innovation and how it directly uses, produces, or consumes data (different from the one you wrote about on the mini-project).

many possible answers...

4. What is meant by the title "The Cost of Free" in lesson 4?

we often ~~trade~~ trade our personal data in order to get services for free, this is part of the business model for many apps/ websites

5. Why is the Vigenere cipher harder to crack than a random substitution cipher?

Vigenere is strong because looking at the cipher text there are no discernable patterns assuming a good key was chosen. We essentially have to guess the key. Even if we know the length of the key, it is still difficult.

6. Why is modulo used in public key cryptography?

PKC is asymmetric. One key can only be used to encrypt data, and a different, (but related) key can only be used to decrypt. That "related key" relies on mathematical properties that make it easy to produce the public/private key pair, but hard to figure out the private one if you can only see the public. The fact that modulo acts as a one-way function is critical to this process.

7. What is 37 mod 10?

7

8. What is 14 mod 7?

0

9. Read through "How to Not Get Hacked" on Code Studio (there is also a link in Google Classroom). Jot down some notes about security on the Internet.

- look at the video
- pay attention to what HTTPS is
- read about Two-factor authentication