AP CSP VOCAB LIST (not in alphabetical order)

CTRL-F is your friend.

Updates, comments, additions: Email melodyc.lam[at]cms.k12.nc.us!

Vocab Word	**Definition/Examples**
Sequencing	One of the three building blocks of programming. Sequencing refers to just sequential steps in a program. Example: area = length * width print(“The area is: “, area)
Selection	One of the three building blocks of programming. Selection is just another word for **conditional**, which are if/if-else/if-elseif-else/switch statements. Example: if (x != 5) return false; else return true;
Iteration	One of the three building blocks of programming. Iteration is another way of saying **loops**, or while/repeat until/for loops. Example For each x in item: print(x)
Phishing	~~What all the kool leet haxors are doing right now.~~ Phishing is any attempt (usually through email) to get your personal information, which can be used to gain unauthorized access to important accounts. Examples: ● “I’m a Nigerian prince and I have lots of money that I want to give to you instead of some charity that is more deserving” emails ● “Hey, your account is compromised, confirm your identity” and you haven’t done anything with that account in like 2 years ● Terribly misspelled emails that try to ask for things (like Amozon instead of Amazon, etc) ● Your boss is too busy to buy (insert gift card here) and they’ll pay you back once you buy the cards for them **(this actually happened at my school, no joke)**
Binary	Anything that has 2 choices.

	Examples: Binary number system (0 & 1) Booleans (True, False)
High Level Programming Language	Pretty much any language that has a high level of abstraction. -- These languages are either object oriented, or have things like list comprehensions, etc. Examples: Scratch, Snap, Python, Java, JavaScript, C++, C#
Low Level Programming Language	Languages that have a low level of abstraction. Basically, these languages are very terse. However, a program can be written in any language, whether high or low. Examples: Assembly, C, actual machine code.
Lossless Compression	Compression that allows one to uncompress and get the original item back. Examples: ZIP/RAR/tarballs, PNG, OGG
Lossy Compression	Compression where data is lost in order to compress the item. Uncompression to the original item is impossible. Examples: JPG, MP3
Cloud Computing	Cloud computing refers to services that normally would be confined to a computer that are now served through the Internet. Examples: Google Drive, Dropbox, Amazon Web Services, Microsoft Office Online/Google Docs
Creative Commons	A license that allows users to freely use, remix, and share items. There are different ones but you don't need to know all of them -- the only thing you should know is that it's used for "open source" items and that you still need to credit the creator of the item.
Heuristic	A problem for which there is no best general algorithm to solve the problem or no best solution to the problem. We can have approximate solutions but they're not good for certain inputs (like compressing text is easy, but compressing video not so much) For example: ● mapping a route from point A to point B. ● Encryption. ● Compression.
IP Address	A numerical address to identify users & devices on the Internet. (This is different from the MAC address, which is a hardware encoded address that cannot be changed.

	An IP number will change every time a device reconnects to the Internet.) ● IPV4 is 4 sets of 8 bits (so the max address is 255.255.255.255) -- 32 bits total. ● IPV6 uses hexadecimal and is 128 bits, so you have 2^{128} possible addresses
Client	The device/user sending information TO another device. Usually it's referring to the person sending requests to a website (like a user requesting the Amazon homepage.)
Server	The device/user/computer serving (or providing) information to users connecting to a server.
Cookies	Files that are used to keep track of a user's interaction with a webpage. This is how sites know that you are logged in after you've closed a tab/window.
Reasonable Time	Any algorithm that runs in polynomial time/log time as the number of elements **n** increases. (By polynomial time, we mean n^x, where x is constant as n increases.) If you want more details, lookup "Big O notation". Examples: ● Linear search -- O(n) ● Binary search -- O(log n) ● Calculating area -- O(1) (doesn't depend on inputs at all.)
Unreasonable Time	Any algorithm that runs in exponential time as the number of elements **n** increases. Examples: ● Find all subsets of a set of n numbers that satisfy a condition -- 2^n ● Decrypting a message encoded with RSA/SHA-256 -- it would take longer than the life of the universe to decrypt such a message.
Unsolvable problems	Some problems are impossible to solve using a computer -- aka, there's no algorithm for which the problem can be solved with a clear yes or no answer (or any answer, for that matter.) Examples: ● The halting problem (given an input, will this program stop?) ● The mortality problem (given a program, will this program stop for ALL inputs)
Private Key Encryption (Asymmetric Encryption)	Encryption that relies on a public key that is given out

	to everybody and a private key that is kept only by the receiver of the message. How it works: Alice wants to send Bob a message, but Eve is nosy and wants to eavesdrop on their communications. Alice knows that Bob has a public key, and uses the key, her message M, and a known algorithm to make a new message (let's just call this R). (**This is encrypting the message.**) Bob receives R, and uses his private key + the known algorithm to unscramble the message (**decrypt the message)** and get M. Eve somehow intercepts the message R that Alice sends to Bob, but unless she has Bob's private key, it's going to take her forever and a day to decrypt the message. (This is an unreasonable time problem.)
Symmetric Encryption	Encryption that relies on a known key that is shared between two parties. Examples: Substitution ciphers (such as Caesar cipher, alphanumerical substitution, Vigenère cipher)
Overflow	The condition in which a variable can't properly hold the exact value of a number. For example, in 8 bit systems, because the registers were 8 bits, the max number that could be stored in an 8 bit processor was 255. If you added 1 to 255, the variable would roll back to 0. By the way, the range of integers that one can express with n bits is always $[0, 2^n-1]$, so if you have 5 bits, the range is [0, 31]. If you tried to put the number 32 into this range, there would be overflow.
Moore's Law	Generally speaking, every 2.5 years the processing speed of a computer doubles & the processor size is cut in half. Because Moore's Law is generally correct in the long run, companies can prepare funds or personnel to upgrade to the latest and greatest when the new processors come out (if needed.) However, Moore's Law has not been true in the past few years since there's a quantum limit on how small a processor is before quantum effects kick in (see quantum tunneling effects if you want to learn more about this!)

DNS	Domain name system. Translates IP addresses of servers to names.
HTTP	Hypertext Transfer Protocol. Allows webpages to be sent to and responded to.
DDoS (attack)	Distributed Denial of Service attack. This is when someone **intentionally** floods a server with requests, overloading the server and preventing legitimate requests from getting through (because servers can handle only so many requests at a time.) Oftentimes, we say DDoS when the server flooding is not a DDoS in question. (Same thing goes with hacking.) When a server is flooded because there's a new Supreme drop and you can't get your items because of it, it's just because the server is busy.
TCP/IP	Transmission Control Protocol/Internet Protocol. Denotes how data should be sent to servers (as packets) and reassembles packets at the destination.
Hacking	We use "hacking" in the wrong way, usually speaking. When a scammer calls and gains unauthorized account access knowing some basic personal information, this is **social engineering**, not hacking. When a student gains access to a teacher's gradebook account because their teacher wrote their password on a sticky note on their computer, this is just **bad security practice. (And if your teacher does this, please gently remind them not to do this.)** Hacking is usually when you gain unauthorized access through a backdoor exploit or security exploit. For example, just recently a casino was robbed of millions of dollars because their IoT thermometer in their fish tank was insecure and they could access the network from that entry point.
Citizen Science/Crowdsourcing	The phenomenon where because of the ubiquity of the Internet, users online can be harnessed to perform tasks to produce results for experiments or share results to public repositories. Scientists use these results in their papers. Distributed computing is an offshoot of citizen science where personal computers that are idle are harnessed to produce results.

	Examples: Zooniverse, SETI @ Home, World Community Grid, amateur astronomy
Internet Engineering Task Force	The organization responsible for creating and maintaining standards and protocols for Internet communication, such as defining HTTP/s, FTP, domain names, etc. For April Fools, they often make documentation for fake protocols: see the HyperText Coffee Pot Protocol (For something that was written in 1998 as a joke, it was a pretty good prediction of our Internet of Things world. And I think the IETF really appreciates companies making Internet enabled coffee makers ;))
Metadata	Data about data. Meta, eh? Examples of metadata: ● File name itself ● Date file was created/accessed ● Where the file was created (especially for photos) ● Version number of file
Program development	It's important that you know the "conventions" for program development. ● **ABD -- Always. Be. Documenting.** Documenting code makes it easier for other programmers (especially those not familiar with the language) to read and understand code. Also, it helps **you** out because sometimes, when you come back to some code, you may not know what you wrote there and why you wrote it. ● **Variable names should be tied to what data they hold.** Not that you should make a variable name called student_id_and_birth_date… but saying **studentID** is better than **x**. Conventions for variable names: the exam uses CamelCase, which means words are separated by capitals (like CamelCase, studentID, birthDate) Some people adhere to underscores and that's OK too. ● **Modularize your program.** That means build your program, then test, and once everything works, build the next part. This is why

	functions & abstractions are so crucial in modern programming. You can write a function, test the function, and then write another function for the next part of your program. Then, if the program fails, you know that the new function was the culprit and can debug from there.
Digital Millennium Copyright Act (DMCA)	US laws that govern the copyright and digital rights of users on the Internet. This law is why Youtubers can have “strikes” on their account -- if a company claims parts of the video as their own, Youtube must bring the video down. Other laws that come from the DMCA -- users were not allowed to “jailbreak” their phones until the Supreme Court ruled otherwise. Reverse engineering is (mostly) illegal. There are severe penalties with distributing copyrighted materials on the Internet.
Digital Divide	The gap between populations that have Internet/technology access and those who do not. (By the way, this is not an income thing (although income plays a role) -- rural areas have a hard time getting Internet access because of the fact that telecos will not run fiber lines to those areas.) Another issue that causes a digital divide is how older populations may not be able to navigate the digital world -- changing modes from paper-based information like tax forms to more digital forms has confused a lot of the older generation. One way to close the digital divide is to provide programs that teach people how to use computing resources such as computers, search engines, or providing them help to complete government forms. Another way to close the digital divide is to provide more forms of access to the digital world, such as free/low-cost laptops & internet service.
Logic gates https://en.wikipedia.org/wiki/Logic_gate	Basically the digital electronics/engineering equivalent of the compound Boolean operators AND, OR, and NOT. This is what processors use to do a lot of the stuff we take for granted. You don’t really NEED to know this for the exam, but there are certain logic gates that they might put on the exam:

	P NAND Q -> NOT (P AND Q) P NOR Q -> NOT (P OR Q) P XOR Q -> True if P & Q have differing truth values, False if P & Q have the same truth value.