

AP Exam Review #3: Copyright, AI, Privacy, Security, Safe Computing, Encryption & The Internet

Copyright

AP EXAM VOCABULARY

- **Copyright law** makes it illegal for anyone to make copies of someone else's work (a book, a painting, a song, etc.) without the permission of the author. **Copyright violation** is very different from **plagiarism**, which means pretending that you wrote someone else's work. You can illegally copy someone's work but say it's theirs (**copyright violation**), or you can copy something that isn't protected by copyright because it was written a long time ago, and pretend it's yours (plagiarism). Copyright is complicated, *but it's easy to avoid plagiarism*: Just give credit to whoever wrote the stuff you want to use ("cite your sources")
- Authors of work can use **Creative Commons** to license their material to make it widely available. **Creative Commons** is a popular site for licensing creative work for general use and has truly enabled broad access to digital information. [Here is their website.](#)

Additionally, authors of various types of work can also make their work available through:

- **Free software** means *software* that anyone can copy, use, modify, and redistribute.
- **Open source software** is a more general term that means that you put the program's code online. You may still restrict how people can use the program.
- **Open access** scholarly research reports are available for free download, rather than requiring the permission of a journal publisher.

AP Exam Practice Question

Which of the following actions is most likely to raise legal or ethical concerns?

- A An analyst writes a program that scans through a database of open-access scientific journals and creates a document with links to articles written on a particular topic.
- B A computer scientist adds several features to an open-source software program that was designed by another individual.
- C A musician creates a song using samples of a copyrighted work and then uses a Creative Commons license to publish the song.
- D A public interest group alerts people to a scam that involves charging them for a program that is available for free under a Creative Commons license.

My answer:

[Check!](#)

AP Exam Practice Question

A researcher wants to publish the results of a study in an open access journal. Which of the following is a direct benefit of publishing the results in this type of publication?

A

The researcher can allow the results to be easily obtained by other researchers and members of the general public.

B

The researcher can better anticipate the effect of the results and ensure that they are used responsibly.

C

The researcher can ensure that any personal information contained in the journal is kept private and secure.

D

The researcher can prevent copies of the research from being accessed by academic rivals.

My answer:

[Check!](#)

AP Exam Practice Question

An author is considering publishing an e-book using a Creative Commons license. In which of the following situations would it be better for the author to use a Creative Commons license instead of a traditional copyright?

I. The author wants to make the e-book available as a free download.

II. The author wants to prevent people from sharing copies of the e-book on peer-to-peer networks.

III. The author wants to allow people permission to use and modify the e-book.

A

I only

B

II only

C

I and III

D

II and III

My answer:

[Check!](#)

AP Exam Practice Question

A programmer created a piece of software and wants to publish it using a Creative Commons license. Which of the following is a direct benefit of publishing the software with this type of license?

A

The programmer can ensure that the algorithms used in the software are free from bias.

B

The programmer can ensure that the source code for the software is backed up for archival purposes.

C

The programmer can include code that was written by other people in the software without needing to obtain permission.

D

The programmer can specify the ways that other people are legally allowed to use and distribute the software.

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following is considered an **unethical** use of computer resources?

A

Downloading freeware or shareware onto your home computer

B

Purchasing a game from an app store and downloading it directly to a mobile device

C

Purchasing a single-user copy of photo editing software and installing it on all the computers in a computer lab

D

Searching online for an electronic version of a school textbook

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following actions is most likely to raise legal or ethical concerns?

- A An analyst writes a program that scans through a database of open-access scientific journals and creates a document with links to articles written on a particular topic.
- B A computer scientist adds several features to an open-source software program that was designed by another individual.
- C A musician creates a song using samples of a copyrighted work and then uses a Creative Commons license to publish the song.
- D A public interest group alerts people to a scam that involves charging them for a program that is available for free under a Creative Commons license.

My answer:	Check!
------------	------------------------

AI, Ethical Implications & Bias

AP EXAM VOCABULARY

Artificial intelligence (AI) is a field of computer science loosely defined as "getting computers to do things that, when done by human beings, are said to involve intelligence."

Interestingly, tasks that *humans* generally consider to be *hard* to do (like mastering chess) have turned out to be *easier* for computers than tasks that humans think of as being so easy that we do them "without thinking," like walking.

Another example is *seeing*, or recognizing images. Getting computers to understand images is called **computer vision**, a big field of research in AI which requires computers to be able to actually *learn*, a.k.a. **machine learning**. As you will see in the video below, people don't actually program a computer to distinguish between a honeybee and the number "three" in a picture -- but instead design computers to be able to *learn and improve themselves!* It's crazy, scary, and awesome all at the same time.

Artificial intelligence -- and the technological innovations that use AI in some form -- can raise **ethical concerns** and create ethical dilemmas.

Consider the following ethical questions:

- What about a self-driving car that has to make a choice between the life of its passenger and the life of a pedestrian? How does that choice get made? Who should decide how that choice gets made?
- What about those people whose jobs are being replaced by artificially intelligent robots and automation? They tend to be disproportionately lower-income. How can we make sure that everyone benefits from developments in AI?
- What about video surveillance or other systems that use facial recognition software? The data used to train facial recognition data can result in racial and ethnic biases in the software.
- What laws apply to AI? What happens if a robot commits a crime? Who should be punished and how?

These questions don't have easy or obvious answers, but it's important for the creators of these AI applications -- and you -- to consider them.

In addition to these dilemmas is the issue of **bias**. Because machine learning algorithms use **existing data** to "learn" from and develop an "understanding" of the world, they are influenced by existing **biases** in the data. And as a result, machine learning applications can result in discrimination -- whether intentionally or unintentionally -- against groups of individuals.

AP Exam Practice Question

The developers of a music-streaming application are updating the algorithm they use to recommend music to listeners. Which of the following strategies is LEAST likely to introduce bias into the application?

A

Making recommendations based on listening data gathered from a random sample of users of the application

B

Making recommendations based on the most frequently played songs on a local radio station

C

Making recommendations based on the music tastes of the developers of the application

D

Making recommendations based on a survey that is sent out to the 1,000 most active users of the application

My answer:

[Check!](#)

AP Exam Practice Question

This question is about a beneficial effect for the USER of the program!

MeeReader is an e-reading application that allows users to download and read books and articles on a device. Each user creates a profile with the following personal preferences.

- Screen brightness and contrast
- Choice of typeface and font size
- Amount of spacing between lines of text
- Activation of a text-to-speech feature that reads the text out loud

When the user launches the application, the application scans the user's face and uses facial recognition software to determine the user's identity. Once the user has been identified, the user's personal preferences are applied to whatever book or article the user chooses to read.

The application stores all user information in a database, including personal preferences and a record of previously read books and articles.

Which of the following is most likely to be a beneficial effect of using MeeReader?

- A Users may have a reduced risk of the application being used in unintended ways.
- B Users may have a reduced risk of their biometric data being misused.
- C Users with limited Internet access may be able to more easily obtain books and articles.
- D Users with visual impairments may be able to more easily read or listen to books and articles.

My answer:	
------------	--

[Check!](#)

AP Exam Practice Question

This question is about a beneficial effect for the COMPANY that designed and sells the program!

MeeReader is an e-reading application that allows users to download and read books and articles on a device. Each user creates a profile with the following personal preferences.

- Screen brightness and contrast
- Choice of typeface and font size
- Amount of spacing between lines of text
- Activation of a text-to-speech feature that reads the text out loud

When the user launches the application, the application scans the user's face and uses facial recognition software to determine the user's identity. Once the user has been identified, the user's personal preferences are applied to whatever book or article the user chooses to read.

The application stores all user information in a database, including personal preferences and a record of previously read books and articles.

From the perspective of the application's developers, which of the following is most likely to be a benefit of storing all user data in a database?

- A The developers can analyze the data to make improvements to the application based on user behavior.
- B The developers can analyze the data to ensure that no patterns emerge in the data.
- C The developers can reduce the amount of data storage required to support the application.
- D The developers can reduce the need for data encryption.

My answer:	
------------	--

[Check!](#)

AP Exam Practice Question

A mobile game tracks players' locations using GPS. The game offers special in-game items to players when they visit real-world points of interest. Which of the following best explains how bias could occur in the game?

A

Points of interest may be more densely located in cities, favoring players in urban areas over players in rural areas.

B

Some players may engage in trespassing, favoring players in urban areas over players in rural areas.

C

Special items may not be useful to all players, favoring players in urban areas over players in rural areas.

D

Weather conditions may be unpredictable, favoring players in urban areas over players in rural areas.

My answer:

[Check!](#)

AP Exam Practice Question

A software development company has created an application called FileCleanUp. When the application is run on a user device, it searches for all files (including pictures, videos, and documents) that have not been accessed in the past month, stores them on the company's Web server, and deletes them from the user device. The application runs once each day. Users have the ability to manually retrieve files from the server if they are needed.

Which of the following is most likely to be a harmful effect of using FileCleanUp?

A

It prevents users from accessing frequently used files when there is no Internet connectivity.

B

It prevents users from accessing infrequently used files when there is no Internet connectivity.

C

It prevents users from accessing frequently used files when there is reliable Internet connectivity.

D

It prevents users from accessing infrequently used files when there is reliable Internet connectivity.

My answer:

[Check!](#)

AP Exam Practice Question

A software company is designing a mobile game system that should be able to recognize the faces of people who are playing the game and automatically load their profiles. Which of the following actions is most likely to reduce the possibility of bias in the system?

- A Testing the system with members of the software company's staff
- B Testing the system with people of different ages, genders, and ethnicities
- C Testing the system to make sure that the rules of the game are clearly explained
- D Testing the system to make sure that players cannot create multiple profiles

My answer:

[Check!](#)

Privacy Risks

VOCABULARY & BIG IDEAS

- **Personally identifiable information (PII)** is information that can let others figure out who you are and possibly get more information like your Social Security number, age, race, phone number(s), medical information, financial information, or biometric data (such as your thumbprint or face scan).

In addition to the above **PII**, there are many **other types of personal data** that can be used to identify information about you, such as your location, your online search or browsing habits, etc.

OTHER PERSONAL DATA INCLUDE:

- Location data, or "GPS" data (*described below*)
- Your search engine history (terms you have searched for) Yes, Google knows your search history!
- Your browser history (sites you have visited, clicked)
- Browser "cookies" (*described below*)
- Your computer's IP address

Sharing personal data online can have benefits. For example, it can be used to show you personalized movie recommendations or simplify online purchasing by suggesting things you are likely to buy based on previous purchases. Shared personal data also has risks; it can be used for identity theft, fraud, harassment, kidnapping, etc.

The **search engine** you use (Google, Bing, etc.) knows what questions you ask it. It also knows

which links you click on. Less obviously, it knows which *links you hover your mouse over, and for how long*. Crazy! Similarly, various websites you visit record and maintain a history of individuals who have viewed their pages.

What does Google do with the search information it collects about you? One thing is to display *targeted ads* that they think you're likely to click on. It also uses that information to decide which search results to show you -- those that it believes will be most interesting or relevant to you.

Targeted advertising and search results are based on *your personal data* -- specifically, what you search for and what pages you visit.

Your phone can track your location using **geolocation**, enabled through **GPS** ("global positioning system") Your location is a piece of personal data that you may or may not want shared! Additionally, your web browser uses little files called "**cookies**" to store pieces of information for each website you visit.

Cookies make it possible for websites to "remember" your passwords (or auto-log you in) and save payment information (like credit cards) for quick purchase and checkout, like on Amazon. Many people find this use of cookies to be helpful and useful. But credit card numbers and passwords are among the personal data that you most want to keep protected against thieves. You're relying on the seller or the company that makes your browser not to have any security bugs, and you're also relying on them not to misuse this information themselves! **Cookies** also make it possible for websites to target ads to you and help target search results. Maybe you like this, maybe you don't!

Your cell phone carrier is also a potential privacy risk because it knows your physical location at all times through **geolocation**. You can turn off sharing your location with apps on your phone, but you can't block your carrier from knowing your location; it needs to know which cell tower you're using and where that tower is. The information it has isn't just your location right now, but everywhere you've been since you got that phone.

Digital footprint or **digital shadow** refers to one's unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or digital devices.

The use of a digital footprint has both positive and negative consequences. On one side, it is the subject of many privacy issues. For example, without an individual's authorization, strangers can piece together information about that individual by only using search engines. Corporations are also able to produce customized ads based on browsing history. On the other hand, others can reap the benefits by profiting off their digital footprint as social media influencers. Furthermore, employers use a candidate's digital footprint for online vetting and assessing fit due to its reduced cost and accessibility. Between two equal candidates, a candidate with a positive digital footprint may have an advantage. As technology usage becomes more widespread, even children generate larger digital footprints with potential positive and negative consequences such as college admissions.

AP Exam Practice Question

A city's police department has installed cameras throughout city streets. The cameras capture and store license plate data from cars driven and parked throughout the city. The authorities use recorded license plate data to identify stolen cars and to enforce parking regulations.

Which of the following best describes a privacy risk that could occur if this method of data collection is misused?

- A The cameras may not be able to read license plates in poor weather conditions.
- B Local business owners could lose customers who are unwilling to park in the city.
- C Traffic personnel who work for the city could lose their jobs if their services are no longer needed.
- D The vehicle location data could be used to monitor the movements of city residents.

My answer:

[Check!](#)

AP Exam Practice Question

Many Web browsers allow users to open anonymous windows. During a browsing session in an anonymous window, the browser does not record a browsing history or a list of downloaded files. When the anonymous window is exited, cookies created during the session are deleted. Which of the following statements about browsing sessions in an anonymous window is true?

- A The activities of a user browsing in an anonymous window will not be visible to people who monitor the user's network, such as the system administrator.
- B Items placed in a Web store's shopping cart for future purchase during the anonymous browsing session will not be saved on the user's computer.
- C A user will not be able to log in to e-mail or social media accounts during the anonymous browsing session.
- D A user browsing in an anonymous window will be protected from viruses launched from any Web sites visited or files downloaded.

My answer:

[Check!](#)

AP Exam Practice Question

StreamPal is an audio-streaming application for mobile devices that allows users to listen to streaming music and connect with other users who have similar taste in music. After downloading the application, each user creates a username, personal profile, and contact list of friends who also use the application.

The application uses the device's GPS unit to track a user's location. Each time a user listens to a song, the user can give it a rating from 0 to 5 stars. The user can access the following features for each song that the user has rated.

- A list of users on the contact list who have given the song the same rating, with links to those users' profiles
- A map showing all other users in the area who have given the song the same rating, with links to those users' profiles

A basic StreamPal account is free, but it displays advertisements that are based on data collected by the application. For example, if a user listens to a particular artist, the application may display an advertisement for concert tickets the next time the artist comes to the user's city. Users have the ability to pay a monthly fee for a premium account, which removes advertisements from the application.

Which of the following is most likely to be a data privacy concern for StreamPal users?

- A** Users of the application are required to rate songs in order to enable all of the application's features.
- B** Users of the application may have the ability to determine information about the locations of users that are not on their contact list.
- C** Users of the application may not be able to use the application if they are located in an area with a poor Internet connection.
- D** Users of the application may not have similar music taste to any other users on their contact list.

My answer:

[Check!](#)

AP Exam Practice Question

This question deals with the same StreamPal situation as the previous question.

StreamPal is an audio-streaming application for mobile devices that allows users to listen to streaming music and connect with other users who have similar taste in music. After downloading the application, each user creates a username, personal profile, and contact list of friends who also use the application.

The application uses the device's GPS unit to track a user's location. Each time a user listens to a song, the user can give it a rating from 0 to 5 stars. The user can access the following features for each song that the user has rated.

- A list of users on the contact list who have given the song the same rating, with links to those users' profiles
- A map showing all other users in the area who have given the song the same rating, with links to those users' profiles

A basic StreamPal account is free, but it displays advertisements that are based on data collected by the application. For example, if a user listens to a particular artist, the application may display an advertisement for concert tickets the next time the artist comes to the user's city. Users have the ability to pay a monthly fee for a premium account, which removes advertisements from the application.

Which of the following statements is most likely true about the differences between the basic version and the premium version of StreamPal?

- A Users of the basic version of StreamPal are more likely to give songs higher ratings than are users of the premium version of StreamPal.
- B Users of the basic version of StreamPal indirectly support StreamPal by allowing themselves to receive advertisements.
- C Users of the basic version of StreamPal spend more on monthly fees than do users of the premium version of StreamPal.
- D Users of the basic version of StreamPal use less data storage space on their devices than do users of the premium version of StreamPal.

My answer:	
------------	--

[Check!](#)

Security Risks

AP EXAM VOCABULARY

Software has **bugs** (even published software written by professionals). Software developers try to prevent security bugs and fix them, but not every software developer distributes fixes promptly (and not every computer user keeps up with software updates perfectly!). Bad people can use those bugs for bad purposes, such as implanting **keylogging software**, which is software designed to capture what you type, including passwords and other confidential information.

- **Keylogging** is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.

The general name for programs that try to affect your computer badly is **malware**. Your computer can end up with malware if you or someone using your computer downloads untrustworthy software (such as from freeware or shareware sites; not everything on those sites is bad, but if you aren't careful, you might install something that is). **Keyloggers** are one type of **malware**.

- **Malware** stands for **malicious software**, and is any software intended to damage a computing system or to take partial control over its operation.

Another common kind of **malware** is called a **virus**.

- A **computer virus** is a malicious program that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer. Viruses make copies of themselves (just as biological viruses do) and try to spread themselves over the network to other computers
- You can use **antivirus software** and **malware scanning programs** to detect and remove viruses or other malware that may inadvertently get installed on a computer.

Any type of malware, including viruses, and keyloggers, requires a person to perform an action (clicking a link, opening a file, etc), and in order to get you to do that, the attackers try to trick you into it. A common attack strategy is called **phishing**.

- **Phishing:** a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive data, such as bank accounts and emails. Generally, an attacker sends you an email that appears to be from some official organization (such as your bank) and tricks you into giving information to the attackers (such as your bank password). The attacker can then use your personal information to gain access to sensitive online resources, such as your bank accounts or emails.

Below is an example of an email that is part of a **phishing scheme**; the embedded link goes to a *fake website* that the attacker owns, and when the user types in their login information and hits submit, they have actually transmitted that login data to an attacker! Phishing emails often have grammatical or spelling errors or have weird email addresses in the FROM field.



Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

Even though cyberattacks most often occur through an action of the victim (such as actively clicking a link in a phishing email), real-world systems have errors or design flaws that can be exploited to compromise them, which means malware can get onto a computer *without* the victim actually needing to do anything! When such “security backdoors” (security bugs) get discovered, a company will quickly release a security update to fix the issue.

- Regular **software updates** help fix errors that could compromise a computing system!

When you are connecting to a wireless network, you will be sending and receiving data -- and *unless your data is encrypted*, your data could potentially be read or modified as it's being sent over that network. One way that this can happen is through a **rogue access point**, which is a “wireless access point” that gives unauthorized access to a secure network, like the wifi used at a company.

- Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a **rogue access point**, which is a wireless access point that gives unauthorized access to secure networks.

AP Exam Practice Question

A user purchased a new smart home device with embedded software and connected the device to a home network. The user then registered the device with the manufacturer, setting up an account using a personal e-mail and password. Which of the following explains how a phishing attack could occur against the user of the smart home device?

A

A vulnerability in the device's software is exploited to gain unauthorized access to other devices on the user's home network.

B

A vulnerability in the device's software is exploited to install software that reveals the user's password to an unauthorized individual.

C

The user is sent an e-mail appearing to be from the manufacturer, asking the user to confirm the account password by clicking on a link in the e-mail and entering the password on the resulting page.

D

The user's account is sent an overwhelming number of messages in an attempt to disrupt service on the user's home network.

My answer:[Check!](#)**AP Exam Practice Question**

A user unintentionally installs keylogging software on a computer. Which of the following is an example of how the keylogging software can be used by an unauthorized individual to gain access to computing resources?

A

The software gives an unauthorized individual remote access to the computer, allowing the individual to search the computer for personal information.

B

The software installs a virus on the computer and prompts the user to make a payment to the unauthorized individual to remove the virus.

C

The software prompts the user to enter personal information to verify the user's identity. This personal information is recorded and transmitted to an unauthorized individual.

D

The software records all user input on the computer. The recorded information is transmitted to an unauthorized individual, who analyzes it to determine the user's login passwords.

My answer:[Check!](#)

AP Exam Practice Question

An individual receives an e-mail that appears to be from an insurance company. The message offers a low insurance rate, and prompts the recipient to click a link to learn more. Which of the following is most indicative that the e-mail is part of a phishing attempt?

A

After clicking the link, a browser cookie is downloaded to the recipient's computer.

B

After clicking the link, a Web page opens that prompts the recipient for personal information.

C

After clicking the link, the recipient's private network becomes publicly visible via a rogue access point.

D

After clicking the link, software is installed on the recipient's computer that records every keystroke made on the computer.

My answer:

[Check!](#)

Protecting Yourself

AP EXAM VOCABULARY

Here is how to protect yourself:

- Run up-to-date software.
- Use strong passwords (one that is hard to guess).
- Don't use sketchy software; if the advertising says that the program will get you money, free stuff, or cheats for video games, it's very likely to be **malware**.
- Install **antivirus** and **anti-malware software**.
- Don't connect to insecure wifi.
- Don't click links on websites or links sent to you in email, without first double-checking that the actual URL in the link is what you expect; they could be **malicious links**.
 - **Malicious links** can be disguised on a web page or in an email message; unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.

- **Enable multifactor authentication** (such as **two-factor authentication**), which requires at least two steps to unlock protected information. Each step adds a new layer of security that must be broken to gain unauthorized access. Typically one piece of information is a password and the other requires another of your devices (like your cell phone) or uses something that detects your body like a fingerprint reader.
 - **Multifactor authentication** is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in *at least two* of the following categories:
 - **knowledge** (something they know, like a password or mother's maiden name)
 - **possession** (something they have, like a cell phone)
 - **inherence** (something unique about them, like a fingerprint).

Multifactor authentication requires *at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.*

Below is a typical example of **multifactor (two-factor) authentication**:



The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.

AP Exam Practice Question

A Web site uses several strategies to prevent unauthorized individuals from accessing user accounts. Which of the following is NOT an example of multifactor authentication?

A

Each employee for a company is issued a USB device that contains a unique token code. To log into a company computer, an employee must insert the USB device into the computer and provide a correct password.

B

After logging into an account from a new device, a user must enter a code that is sent via e-mail to the e-mail address on file with the account.

C

In order to log into an account, a user must provide both a password and a fingerprint that is captured using the user's device.

D

When a user enters an incorrect password more than two times in a row, the user is locked out of the account for 24 hours.

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following best exemplifies the use of multifactor authentication?

A

A computing device enables users to input information using multiple interfaces, including a keyboard, a mouse, and a touch pad.

B

A user employs a public key encryption method that uses one key to encrypt information and a different key to decrypt information.

C

A Web site requires a user to enter a password as well as a numeric code received via text message before the user can log in to an account.

D

Multiple users share an account to a Web-based software program, and each user has an individual username and password.

My answer:

[Check!](#)

Encryption

VOCABULARY & BIG IDEAS

- **Cryptography**, or cryptology, is the practice and study of techniques for secure communication.
- **Encryption** is the process of encoding data to prevent unauthorized access
- **Decryption** is the process of decoding the data

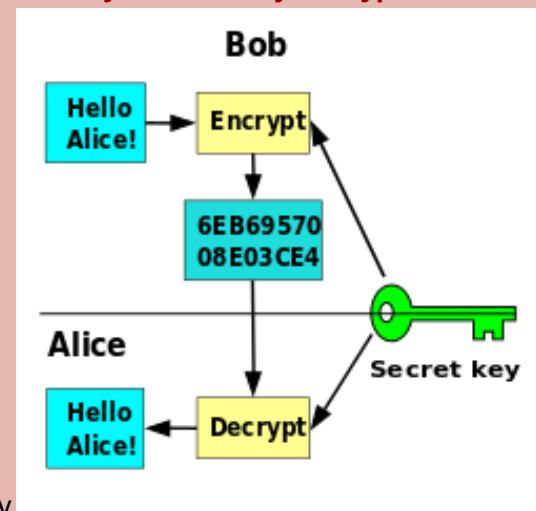
There are two primary techniques for encrypting and decrypting information:

- **Symmetric key encryption** involves **one** key for both encryption and decryption (both the sender and receiver know the key and the same key used to encrypt the message is used to decrypt it).

Symmetric key encryption

An example of **symmetric key encryption** is shown to the right. In this example, Bob is sending Alice a message and uses the “secret key” to encrypt the message, then Alice uses the *same* “secret key” to decrypt the message.

The *problem* with symmetric key encryption is that the sender and receiver both need to know the key ahead of time (since the same key is used for encryption and decryption) -- what if you are trying to send an encrypted message for real to a friend? You would need to email or text them the encrypted message *and the key* to let me know how to decrypt it. But if someone is snooping on your email or text messages, they will be able to see you are sending an encrypted message, but also see the key which, then immediately apply it to the encrypted message.

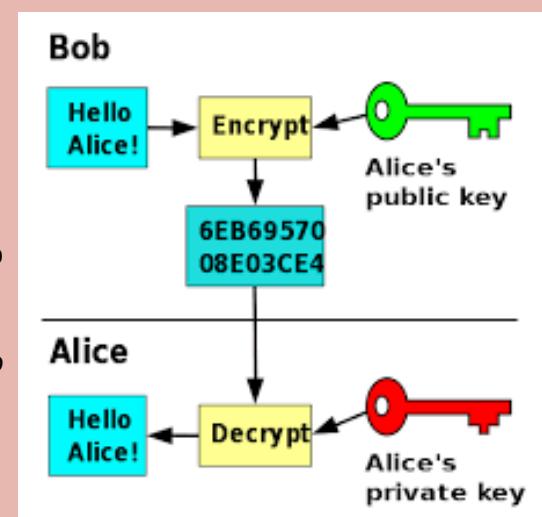


Public key encryption

Because of this problem with symmetric key encryption, which uses a single key for encryption and decryption that *both parties must know ahead of time*, a *more secure* encryption scheme was developed in the 1970's called **public key encryption**.

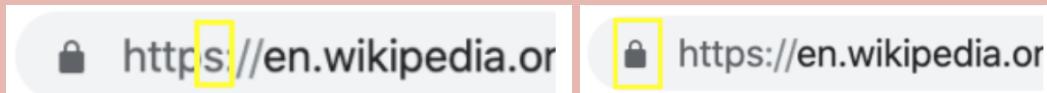
- **Public Key Encryption ("PKE")** is encryption that uses **two different keys** for encrypting and decrypting (it is also called **asymmetric key encryption** because it uses two different keys). It allows for the sender and receiver to communicate using encrypted messages *without having to agree on a shared encryption key ahead of time* (thus solving the fundamental weakness of symmetric encryption).

- In PKE, a **public key** is the key used to **encrypt** information (but not decrypt); this key can be safely shared with anyone publicly.
- In PKE, a **private key** is the key used to **decrypt** information (but not encrypt); this key is known *only to* the individual.



An example of **public key encryption** is shown on the previous page. In this example, Bob wants to send Alice a secret message, so he encrypts it using *Alice's public key*. Everyone has access to Alice's public key, and it can be used by anyone used to *encrypt messages specifically to Alice*. When Alice receives a message, she uses her **private key** to decrypt the message, and only she knows her private key. No other private keys will work -- only hers -- and no one can figure out her private key from her public key because of the "one-way" mathematical relationship that was used to create one from the other.

Public key encryption is the standard encryption scheme used on the internet and web pages for securing communications. You can tell if a website uses public key encryption by looking for the "s" in `https://` and the lock icon:



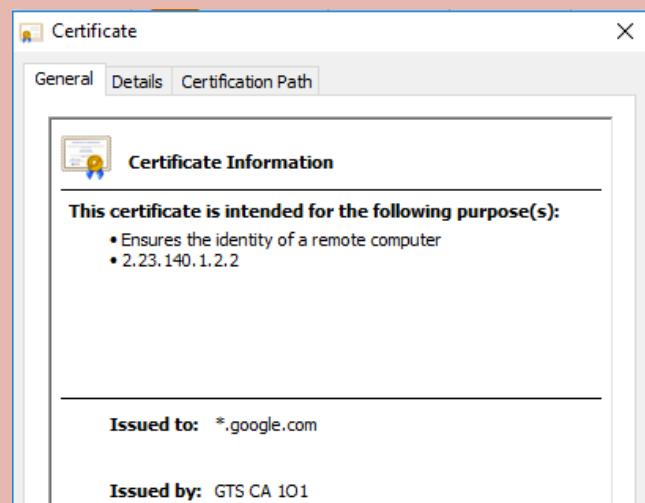
This means communication from that website is **secure**. If a website does *not* use public key encryption, you should be cautious about what information you enter! Secure HTTP connections (those that use `https://` instead of `http://`) use a protocol called **Transport Layer Security (TLS)** or maybe an older version called **Secure Sockets Layer (SSL)**. Both make use of public key encryption. With SSL/TLS, the site you are visiting (such as Amazon) **sends its public key to your browser**, and your browser uses it to encrypt the information you send (such as credit card numbers or passwords). The website owner (e.g. Amazon) has **its private keys stored securely on its servers**, and never reveals them to anyone, but uses them to decrypt messages it receives.

If you click on the lock icon, you can view a website's **digital certificate**.

- In cryptography, a **digital certificate** (also known as a **public key certificate**) is an electronic document used to prove the ownership of a public key.

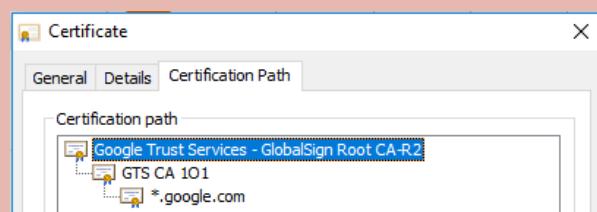
An example of the **digital certificate** for Google's website is shown on the right:

Basically, this certificate guarantees that the website you are visiting is *actually* Google (as opposed to a fake Google website set up by a bad person trying to steal people's info).



These certificates are issued by **certificate authorities** who verify each company's website.

- Certificate authorities** issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.



In the example above, if you click on the "Certification Path" tab, you can see that "GlobalSign" is the **certificate authority** that issued this certificate.

AP Exam Practice Question

Which of the following best illustrates symmetric key encryption?

- A Abe writes a message and seals it in an envelope. She addresses it to his friend, Emily. Abe hands the envelope to Frank, who then delivers it to Emily. Emily opens the envelope and reads the message.
- B Barb writes a message, folds it up, and hides the message behind the trashcan in the cafeteria. She tells her friend Raymond where to find the message. Raymond locates the message, then opens it privately so no one else can read it.
- C Cathy writes a message and slides it through the opening in Jared's locker. Jared is the only one that knows the combination to his locker. At the end of the school day, Jaren unlocks his locker and retrieves the message from Cathy.
- D David writes a message, then encodes each letter of the message with another symbol by using a secret key to map each letter to a new symbol. David hands the message to his friend, Debra, and tells her the secret key. Debra uses that same key to decode the message and read it.

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following best illustrates public key encryption?

- A Abe has a mailbox with a single unlocked door on the front that can be used to deposit and take out the mail.
- B Barbara has a mailbox with a single locked door on the front that can be used to deposit and take out the mail. Barbara has made two copies of the key to the door and hangs one above the mailbox so anyone can unlock an open the door and deposit mail in. She uses her copy of the key to unlock it and take the mail out.
- C Cathy has a mailbox with one locked door on the top and a second locked door on the bottom. Both doors have different keys. Cathy hangs the key to the top door above the mailbox so anyone can unlock the door and drop mail in. Then Cathy can use the key to the bottom door (which only she has) to unlock it and take the mail out (assume people that drop the mail in the top door can't access the lower part of the mailbox).
- D David asks people slide mail under his door. He is the only person with the key to his apartment, and he uses that key to get into his apartment and get his mail.

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following are true statements about digital certificates in Web browsers?

- I. Digital certificates are used to verify the ownership of encrypted keys used in secured communication.
- II. Digital certificates are used to verify that the connection to a Web site is fault tolerant.

 A

I only

 B

II only

 C

I and II

 D

Neither I nor II

My answer:	
-------------------	--

[Check!](#)**AP Exam Practice Question**

Which of the following activities poses the greatest personal cybersecurity risk?

 A

Making a purchase at an online store that uses public key encryption to transmit credit card information

 B

Paying a bill using a secure electronic payment system

 C

Reserving a hotel room by e-mailing a credit card number to a hotel

 D

Withdrawing money from a bank account using an automated teller machine (ATM)

My answer:	
-------------------	--

[Check!](#)

AP Exam Practice Question

Which of the following has the greatest potential for compromising a user's personal privacy?

- A A group of cookies stored by the user's Web browser
- B The Internet Protocol (IP) address of the user's computer
- C The user's e-mail address
- D The user's public key used for encryption

My answer:

[Check!](#)

Crowdsourcing, Crowdfunding & Citizen Science

AP EXAM VOCABULARY

- **Crowdsourcing** is the practice of obtaining input or information from a large number of people via the Internet to gather data, innovate, or complete a task.

There are many reasons for a company, organization, or individual to **crowdsource**:

- To get **ideas, data, or information**: Asking the public for their ideas or to contribute data or information to help them craft better products and services.
- To outsource **tasks or problems**: Breaking massive tasks up into smaller individual tasks, which allows hundreds or thousands of people to work on small jobs that contribute to the overall problem and that they can work on by themselves.
- To **raise money for new projects**: This is known as "**crowdfunding**", a term used to describe the process of crowdsourcing funds (money) from the public; *crowdfunding is an example of crowdsourcing*.
- For **scientific research**: This is known as **citizen science**, *which is another type of crowdsourcing* in which scientific research is conducted in whole or part by many individuals (many of whom may not be scientists). These individuals contribute relevant data to the research using their own computing devices. Other terms for **citizen science** are "**crowdsourced science**" and "**community science**".

AP Exam Practice Question

Which of the following applications is most likely to benefit from the use of crowdsourcing?

A

An application that allows users to convert measurement units (e.g., inches to centimeters, ounces to liters)

B

An application that allows users to purchase tickets for a local museum

C

An application that allows users to compress the pictures on their devices to optimize storage space

D

An application that allows users to view descriptions and photographs of local landmarks

My answer:	
-------------------	--

[Check!](#)**AP Exam Practice Question**

A mobile application is used to display local traffic conditions. Which of the following features of the application best exemplifies the use of crowdsourcing?

A

Users can save an address to be used at a later time.

B

Users can turn on alerts to be notified about traffic accidents.

C

Users can submit updates on local traffic conditions in real time.

D

Users can use the application to avoid heavily congested areas.

My answer:	
-------------------	--

[Check!](#)

Digital Divide

AP EXAM VOCABULARY

- The **digital divide** refers to unequal access to computers and the Internet based on poverty, racism, sexism, isolation in the countryside, age, and other factors. The digital divide affects both individuals within a country and between countries themselves.

AP Exam Practice Question

Which of the following actions is most likely to help reduce the digital divide?

A

Adding a requirement that all users of a popular social media site link their accounts with a phone number.

B

Deploying satellites and other infrastructure to provide inexpensive Internet access to remote areas of Earth

C

Digitizing millions of books from university libraries, making their full text available online

D

Offering improved Internet connections to Internet users who are willing to pay a premium fee for more bandwidth

My answer:

[Check!](#)

AP Exam Practice Question

A city government is attempting to reduce the digital divide between groups with differing access to computing and the Internet. Which of the following activities is LEAST likely to be effective in this purpose?

A

Holding basic computer classes at community centers

B

Providing free wireless Internet connections at locations in low-income neighborhoods

C

Putting all government forms on the city Web site

D

Requiring that every city school has computers that meet a minimum hardware and software standard

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following is LEAST likely to be a contributing factor to the digital divide?

- A Some individuals and groups are economically disadvantaged and cannot afford computing devices or Internet connectivity.
- B Some individuals and groups do not have the necessary experience or education to use computing devices or the Internet effectively.
- C Some parents prefer to limit the amount of time their children spend using computing devices or the Internet.
- D Some residents in remote regions of the world do not have access to the infrastructure necessary to support reliable Internet connectivity.

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following actions is most likely to be effective in reducing the digital divide at a local level?

- A Creating an application that offers coupons and discounts for local businesses
- B Offering a discount to utility customers who pay their bills online instead of by mail
- C Providing free community access to computers at schools, libraries, and community centers
- D Requiring applicants for local government jobs to complete an online application

My answer:

[Check!](#)

AP Exam Practice Question

Which of the following school policies is most likely to have a positive impact on the digital divide?

- A school allows students to bring a graphing calculator from home to complete in-class mathematics assignments.
- B A school allows students to bring a tablet computer to class every day to participate in graded quizzes.
- C A school provides a laptop or tablet computer to all students enrolled at the school.
- D A school recommends that all students purchase a computer with as much processing speed as possible so that projects run faster.

My answer:	
------------	--

[Check!](#)

Beneficial and Harmful Effects

VOCABULARY & BIG IDEAS

- A **computing innovation** is any piece of technology that involves a computer program as an integral part of its function. Computing innovations can be physical (such as a self-driving car, Roomba vacuum cleaners, or Alexa speakers), non-physical (such as phone apps, websites, facial recognition software, or any program that runs on your computer), or conceptual (such as “e-commerce” or “social media”).

Sometimes the impacts of a piece of a **computing innovation** can be both **beneficial and harmful**.

Whatever the intentions of the programmers, they don't always anticipate all the consequences -- good and bad. Here's an oversimplified chart of some of the implications of Facebook:

Facebook Consequences	Intended	Unintended
Good	finding old friends	organizing protests and aid
Bad	privacy violation for targeted advertising	"fake news" to influence elections

Facebook was started as a way for people to stay connected with each other (**intended positive consequences**). But it turned out *also* to be good for organizing group activities, such as political protests and disaster support (**unintended positive consequences**). So computing innovations can have **intended and unintended beneficial** effects!

Of course, there can be harmful effects also. Facebook's ability to make money could have been based on charging a fee for a Facebook account, but instead they chose to make the accounts free and to make money by using people's data to provide advertising targeted to that user's interests. This data gathering is **potentially harmful but it is also intended** (Facebook relies on user data as part of its profit model). But one thing Facebook didn't intend was the ability of political campaigns and foreign countries to post fake content, which is potentially **harmful and is unintended**. So computing innovations can have **intended and unintended harmful** effects!

Interestingly, a single effect *can be viewed as both beneficial and harmful by different people, or even by the same person*. You might not like your personal data being collected and shared with other companies (data collection may be **harmful to you**), but doing so isn't bad for Facebook (data collection is **beneficial** to the company). And you might **appreciate** seeing advertisements that are relevant to you but based on the data collected on you -- so in a way, the effects of data collection on your privacy could be both good and bad from your perspective.

Overall, technological innovations can have both beneficial and harmful effects on society, the economy, or culture, and these effects can be intended or unintended.

“The two sides of the same coin”

Here are two more examples:

- **Targeted advertising** is used to help businesses (beneficial for them; helps make them profits), but the data collected about users to target such advertising can be misused at both individual and aggregate levels (potentially harmful for users).
- **Machine learning and artificial intelligence** has enabled innovation in many areas (positive effects!), but information discovered in this way has also been used to discriminate against groups of individuals, such as facial recognition software models that contain racial bias (harmful, unintended effects)

AP Exam Practice Question

Both online newspapers and social media sites are used to distribute information on the Internet. Which of the following best describes an advantage that online newspapers have over social media sites?

- A The ability to distribute information instantaneously
- B The ability to provide credibility to the information distributed
- C The ability to provide information that is widely accessible
- D The ability to provide media-rich content for low cost

My answer:

[Check!](#)

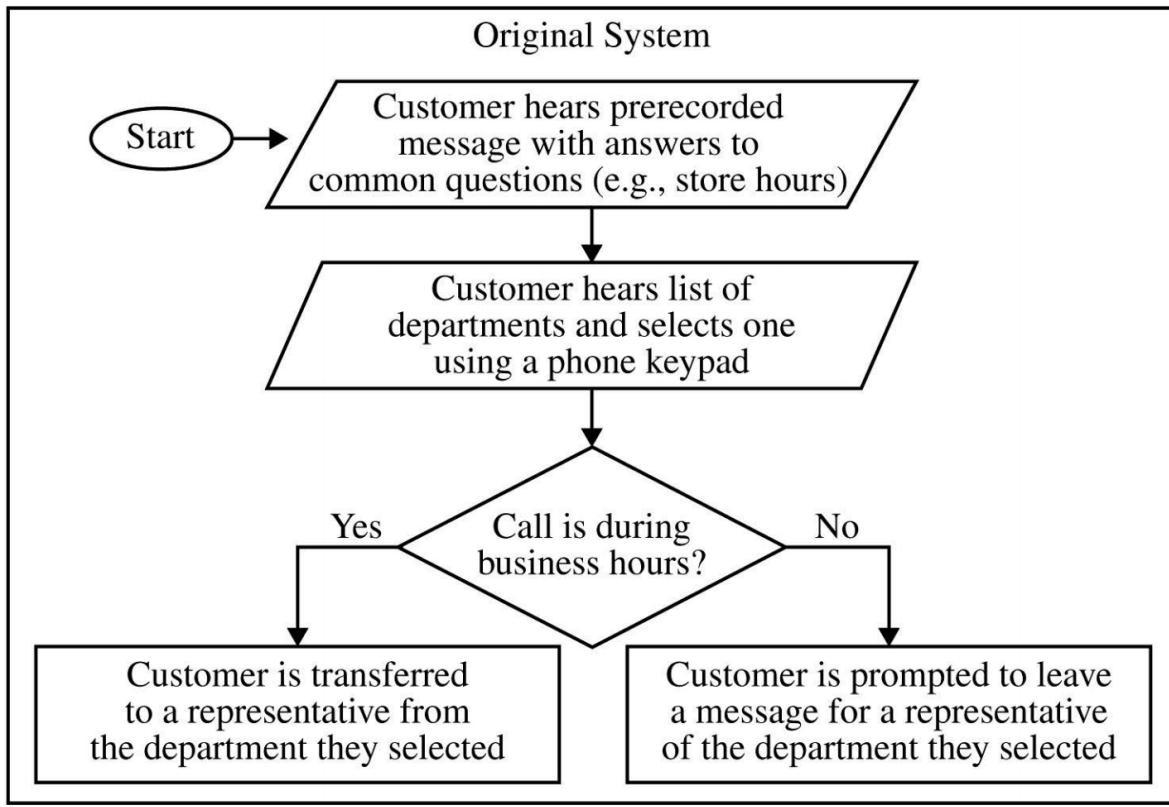
Practice AP Exam Questions Based on a Reading Passage

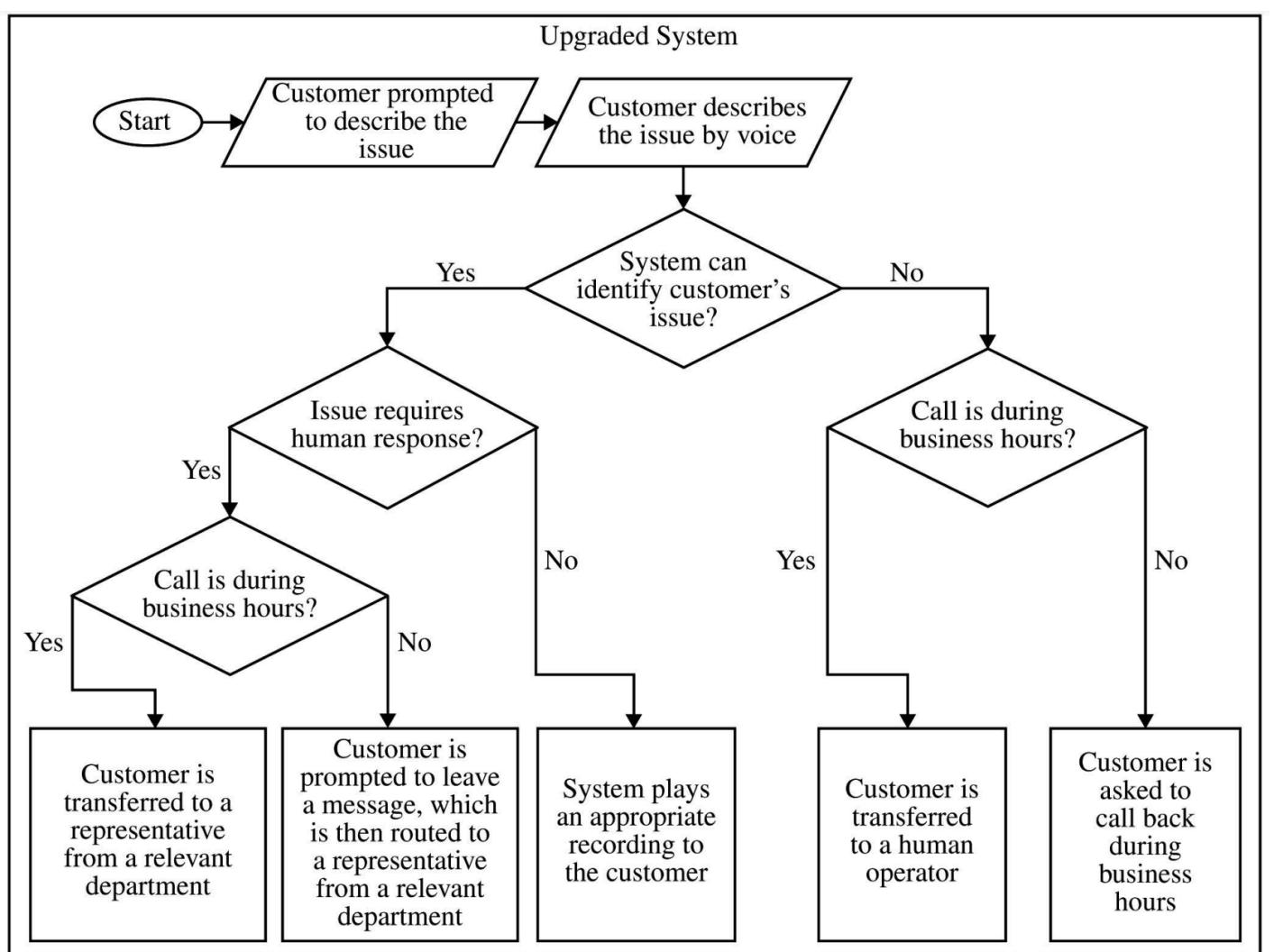
The following three questions refer to the information and reading passage below.

Note: On the AP Exam, there will be *five* single-select multiple-choice questions related to a reading passage.

- A chain of retail stores uses software to manage telephone calls from customers. The system was recently upgraded. Customers interacted with the original system using their phone keypad. Customers interact with the upgraded system using their voice.
- The upgraded system (but not the original system) stores all information from the calling session in a database for future reference. This includes the customer's telephone number and any information provided by the customer (name, address, order number, credit card number, etc.).
- The original system and the upgraded system are described in the following flowcharts. Each flowchart uses the following blocks.

Block	Explanation
Oval	The start of the algorithm
Parallelogram	An input or output step
Diamond	A conditional or decision step, where execution proceeds to the side labeled "Yes" if the answer to the question is yes and to the side labeled "No" if the answer to the question is no
Rectangle	The result of the algorithm





1.

The upgraded system uses a directory containing additional information not supplied by the customer. The directory is used to help direct calls effectively. Which of the following is LEAST likely to be included in the directory?

- (A) A list of common issues and whether each issue requires a human representative
- (B) A list of common keywords or phrases and a corresponding issue for each keyword or phrase
- (C) A list of computers the company owns and the computers' corresponding IP addresses
- (D) A list of human representatives and the corresponding department for each representative

Your answer (A, B, C, D):

[Check your answer!](#)

2. NOTE: For this question, a “benefit” could be **any** benefit: either a benefit to the customer **or** a benefit to the company!

Of the following potential benefits, which is LEAST likely to be provided by the upgraded system?

- (A) Human representatives will not be needed to respond to some inquiries.
- (B) The company will be able to provide a human representative for any incoming call.
- (C) Customers are likely to spend less time listening to information not relevant to their issue.
- (D) Customers will be unable to mistakenly select the incorrect department for their particular issue.

Your answer (A, B, C, D):

[Check your answer!](#)

3.

Which of the following is the most likely data privacy concern of the upgraded system?

- (A) Customers’ personal information could be compromised if an unauthorized individual gains access to the call session database.
- (B) Storing information in the call session database makes it easy for individuals to trick the system using malicious links.
- (C) The system design increases the chance that customers will unknowingly install malware on their devices that will share their data with unauthorized individuals.
- (D) The system design makes it easy for unauthorized individuals to acquire customers’ private encryption keys.

Your answer (A, B, C, D):

[Check your answer!](#)

How The Internet Works

AP EXAM VOCABULARY

- The **Internet** is a network of independent, connected computing devices spread out over the world.
- The **World Wide Web** is the collection of linked pages, programs, and files that you can view with a web browser by typing an address like <https://www.wikipedia.org> or <https://www.youtube.com>. The World Wide Web *uses* the Internet to function (and World Wide Web is where the “www” comes from in front of lots of web pages).
- The Internet is a massive **computing network** of computers that facilitate communication around the globe. It works because it's engineered to be **fault-tolerant** (capable of working even if some of the network breaks down) and uses **protocols** for routing and transmitting data.
- The Internet is **fault-tolerant** because it is a **redundant** network. This means there are multiple pathways among its physical connections to create redundancy. *Even if one pathway is unavailable, there is still another way to transmit a message from sender to receiver.* Software in the various connection points known as **routers** know how to reroute data if one connection fails.
- A **router** is a computer that passes information from one computer network to another.
- The Internet is more technically a *network of networks*. The connection points between networks are called **routers**, networking devices that route traffic between “subnetworks” on the Internet.
- Data is transmitted via **protocols**, “*the rules of the road*” for the Internet that *standardize* communication so all data is sent by the same rules for sending and receiving. These protocols are **open protocols**, which means they are available for use by anyone and not “owned” by any company or government. *Open protocols ensure that any company or person can build systems or devices that connect to the Internet*, and have contributed to the **scalability** of the internet.
- Every device on the Internet has a unique **Internet Protocol (IP) address**, like a postal or email address. The **Internet Protocol** is responsible for assigning IP addresses to devices, as well as specifying how a **router** handles a request for a specific IP address.
- Each router knows the layout of its specific “neighborhood” of the Internet and knows which way to send each message to get it a little bit closer to where it's going. The fact that each router doesn't have to know the complete Internet improves **scalability**.
- Internet **scalability** is the ability of the Internet to keep working even as the size of the network and the amount of traffic increases (which happens every day as new devices get added).
- **Protocols** are “*the rules of the road*” for the Internet and are used to *standardize* communication so all data is sent and received by the same rules. An **open protocol** is one that is not “owned” or regulated by any one particular group or company. For the Internet, **open protocols** are used to ensure that a variety of devices can connect and communicate smoothly with each other.
- **ISPs (Internet Service Providers)** are the companies who sell Internet access to homes and institutions. The computers connected to the Internet and the connections among them don't belong to any one organization. Different ISPs provide the Internet to different communities. And typically within a large organization, the organization itself provides the Internet connections.
- **HTTP (HyperText Transfer Protocol):** A protocol used by the World Wide Web for sending GET and POST requests to obtain website images and data.

- **Internet Protocol (IP)**: A protocol responsible for assigning IP addresses to devices, as well as specifying how a router handles a request for a specific IP address.
- **IP address**: A unique number assigned to each device on a computer network and a *machine-readable* way of locating an Internet site (such as 172.124.54.13).
 - **IPv4** addresses look like this: 172.124.54.13
 - **IPv6** was introduced to support **scalability** and allow many more devices to connect to the internet; IPv6 addresses look like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- **URL (Uniform Resource Locator)**: The human-readable address of a given unique resource on the Web that you type into the browser: e.g. <https://www.google.com>, <https://apclassroom.collegeboard.org>, <https://www.youtube.com/watch?v=AkL2ufOFejl>

AP EXAM PRACTICE QUESTION

Which of the following best describes the relationship between the World Wide Web and the Internet?

- (A) The World Wide Web is a protocol that is accessed using a data stream called the Internet.
- (B) The World Wide Web is a system of linked pages, programs, and files that is accessed using a data stream called the Internet.
- (C) The World Wide Web is a system of linked pages, programs, and files that is accessed via a network called the Internet.
- (D) The World Wide Web is a Web site that is accessed using a protocol called the Internet.

My answer:

[Check my answer!](#)

AP EXAM VOCABULARY

In the early days of the Internet, **bandwidth** was slow, so people couldn't send video (only text and small pictures). Computers used to be huge and very expensive, so people went to a "computer center" to do their computations. As the technology became smaller and more efficient, these centers became less important because people could do computations on personal computing devices, like home laptops or mobile phones.

- A **bit** is the smallest unit of data, which can have only one of two values (such as a 1 or 0). All digital data is represented as bits, specifically 0's and 1's.
- The **bandwidth** of a computer network is the maximum amount of data that can be sent in a fixed amount of time, measured in **bits per second**. *Higher bandwidth is better → more data can travel each second*

- **Latency** is the time between the transmission and the receipt of a message (usually measured in milliseconds). *Lower latency is better* → the data takes *less time* to get to you!

On the internet, you want HIGHER bandwidth and LOWER latency

More recently, certain kinds of computation (such as web searches and voice recognition) require more computational power, and these tasks are instead sent to huge "computer farms" where tens of thousands of computers work together on a problem. These computer farms, all together, are referred to as the **cloud**. If you use Google Drive or Dropbox or any other online file service, all of those files are stored in the **cloud**. And if you use a web-based email service (such as Gmail or Yahoo), your *emails* are stored in the cloud (i.e. they aren't actually on your computer!).

- Storing data in the **cloud** means storing it somewhere on the Internet, but you don't know where. The cloud service provider (Google Drive, Dropbox, Gmail, etc.) manages the actual storage location.

Storing data in the cloud allows us to share and collaborate on our work, but it *does increase the security risks*. If someone discovers your password, for example, they can use it to access your data (such as your files or email). Or data might be intercepted while it is being sent back and forth to the cloud.

A. Which bandwidth enables more data per second?

20 MB/sec or 100 MB/sec

(*MB = megabits per second, or 1 million bits per second*)

B. Which is a faster (better) latency? 300 ms or 500 ms

(*ms = milliseconds*)

A.

B.

[Check!](#)

AP EXAM PRACTICE QUESTION

Which of the following is **not** an advantage of storing data using cloud computing?

- (A) The cloud is easy to scale and can support individual use as well as implementation by large companies.
- (B) Cloud computing has the potential to be environmentally friendly due to many users efficiently sharing large systems and resources.
- (C) Cloud computing offers improved security and privacy over storing data on a personal computer.
- (D) Storing data in the cloud can prevent loss of data due to a malfunction of the user's personal computer.

My answer:

[Check my answer!](#)

AP EXAM VOCABULARY

- Information is passed through the Internet as a **data stream**. Data streams contain *chunks* of data, which are encapsulated in **packets**. When you send data over the Internet, your computer sends each packet individually, and each packet may take a different path. For example, when you email an image file, all the millions of 0's and 1's making up that image file get broken up into packets which are sent individually.
- A **data stream** is how data gets sent on the Internet, by encapsulating chunks of the data into individual packets.
- A **packet** is a small chunk of any kind of data (text, numbers, lists, etc) which, along with the data, contains **metadata** -- information about the packet, such as origin, destination, how many total packets, and what specific packet number it is.
- TCP (Transmission Control Protocol)** is the protocol that manages the sending and receiving of data as packets by keeping track of packets sent and received. Packets may arrive at the destination in order, out of order, or not at all, and TCP makes sure all packets have been received, resends any packets that have been lost or damaged, and reassembles the data on the other end.
- Packets contain a part of the file, along with **metadata**, which is used for routing the packet between the origin and the destination on the Internet, and for data reassembly. The **metadata** includes where the packet is going to (recipient's IP address), where it is coming from (sender's IP address), how many total packets make up the complete file, and what number each packet is. On the receiving end, TCP reassembles the packets in order using the metadata:

"Hello router! I am a packet coming from IP address 192.34.25.134 and on my way to 283.80.132.14.

And hello Mr. TCP, I am packet number 7 out of a total of 156. All packets will have been received when you have 156 total, and since you know which number I am, you can put me in the right order when the rest of the packets get here"

- Like **HTTP**, and **IP**, **TCP** is yet *another open protocol* used on the internet to allow users to easily connect additional computing devices to the Internet and allow them to communicate -- *no matter what kind of device it is or what company makes it!* **Scalability** of the Internet has been fueled by **open protocols** such as these, and many others (including UDP and SMTP).
- **Routing** is the process of finding a pathway over the network from sender to receiver; this is what a **router** does.

AP Exam Practice Question

Which of the following best explains how data is transmitted on the Internet?

- A Data is broken into packets, which are all sent to the recipient in a specified order along the same path.
- B Data is broken into packets, which can be sent along different paths.
- C All data is transmitted in a single packet through a direct connection between the sender and the recipient.
- D Multiple data files are bundled together in a packet and transmitted together.

My answer:

[Check!](#)

Practice AP Exam Question

A user is trying to download an image from Creative Commons to use in their project. Which of the following best describes how the file is sent to the user?

- (A) The user's computer and the Creative Commons server connect directly and the image file is sent in its entirety, all at once.
- (B) The image file is broken into packets which are routed to the receiving computer in the correct order and reassembled to form the complete image file; any missing packets are substituted for packets already received.
- (C) The image file is broken into packets which are routed to the receiving computer, potentially out of order, and reassembled to form the complete image file; any missing packets are resent.
- (D) It is not possible to download image files from websites.

Your answer (A, B, C, D):

[Check your answer!](#)

Practice AP Exam Question #2

Which of the following statements regarding the use of open protocols for communicating on the Internet is *false*?

- (A) Open protocols promote collaboration and cooperation between different people and groups.
- (B) Open protocols allow companies all over the world to build different types of devices that can connect to the internet and communicate with each other.
- (C) Open protocols have contributed to the fast growth of the internet and support its scalability.
- (D) Open protocols are developed and regulated by a few select companies around the world.

Your answer (A, B, C, D):

[Check your answer!](#)

AP Exam Practice Question

Which of the following best explains how data is typically assembled in packets for transmission over the Internet?

A

Each packet contains data to be transmitted, along with metadata containing information used for routing the data.

B

Each packet contains an encrypted version of the data to be transmitted, along with metadata containing the key needed to decrypt the data.

C

Each packet contains only the metadata used to establish a direct connection so that the data can be transmitted.

D

Each packet contains multiple data files bundled together, along with metadata describing how to categorize each data file.

My answer:[Check!](#)**AP Exam Practice Question**

Which of the following is a primary reason for the use of open protocols on the Internet?

A

Open protocols allow devices to specify how data packets are to be routed on the Internet in advance.

B

Open protocols ensure that all data transmission on the Internet is kept secure.

C

Open protocols ensure that all Internet users are provided connections with equal bandwidth.

D

Open protocols provide a way to standardize data transmission between different devices.

My answer:[Check](#)

AP Exam Practice Question

Two computers are built by different manufacturers. One is running a Web server and the other is running a Web browser. Which of the following best describes the ability of the two computers to communicate with each other across the Internet?

A

The computers cannot communicate because different manufacturers use different communication protocols.

B

The computers can communicate, but additional hardware is needed to convert data packets from one computer's protocol to the other computer's protocol.

C

The computers can communicate directly only if the messages consist of text; other formats cannot be interpreted across computers.

D

The computers can communicate directly because Internet communication uses standard protocols.

My answer:

[Check!](#)

AP EXAM VOCABULARY

The Internet works because it's engineered to be **fault-tolerant**, capable of working even if some parts of the network break down. The Internet is **fault-tolerant** because it is a **redundant** network. This means there are multiple pathways among its physical connections to create redundancy. *Even if one pathway is unavailable, there is still another way to transmit a message from sender to receiver.* The routers know how to reroute data if one connection fails.

- **Redundancy** is the inclusion of back-ups in case one part fails; having multiple pathways is an example of redundancy
- **Fault tolerance** is the ability of a system to work around problems; *having multiple pathways (redundancy) helps enable fault tolerance of the Internet.*

AP Exam Practice Question

Which of the following best explains how the Internet is a fault-tolerant system?

A

The Internet is fault-tolerant because cybercriminals can conceal their actions, allowing them the ability to carry out faulty actions without leaving a trace.

B

The Internet is fault-tolerant because there are usually multiple paths between devices, allowing messages to sometimes be sent even when parts of the network fail.

C

The Internet is fault-tolerant because users can transmit messages using a variety of different protocols, allowing them to use devices from any manufacturer.

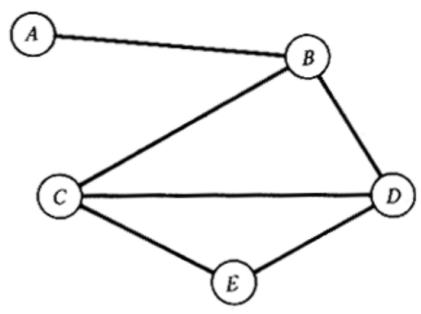
D

The Internet is fault-tolerant because users usually understand and accept the fact that servers sometimes fail, allowing network engineers to repair faulty devices as quickly as possible.

My answer:

[Check!](#)

Pretend this image represents a small computer network, and each node is a computer. The line indicates that the two computers can communicate directly with each other. When a node becomes **faulty**, then it can no longer send or receive data:

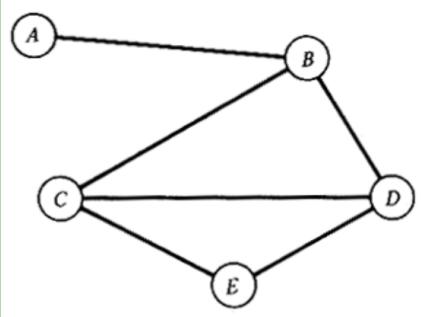


Node A is sending data and node E is receiving that data.

- Could E receive the data if node D became faulty?
- Could E receive the data if node B became faulty?

[Check!](#)

Look at this network again. We can say there is **redundant routing** between computers A and E because there is **more than one path** to get from A to E.



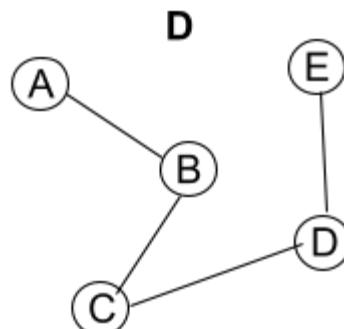
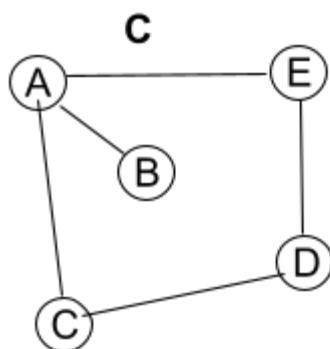
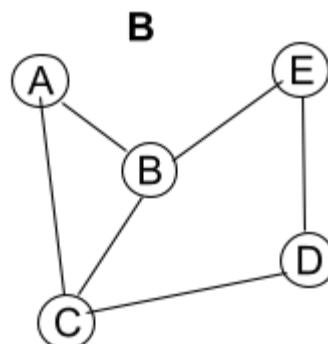
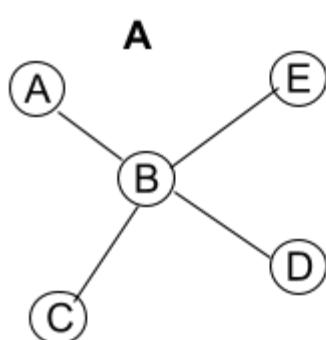
- Is there **redundant routing** between B and E? If so, list all possible pathways to get from B to E.
- How about from B to D? If so, list all pathways.
- Are there two nodes for which there is **not** redundant routing? If so, which two?

[Check!](#)

AP EXAM PRACTICE QUESTION #3

Which of the following networks do *not* have redundant routing between computers A and E?

Select two.

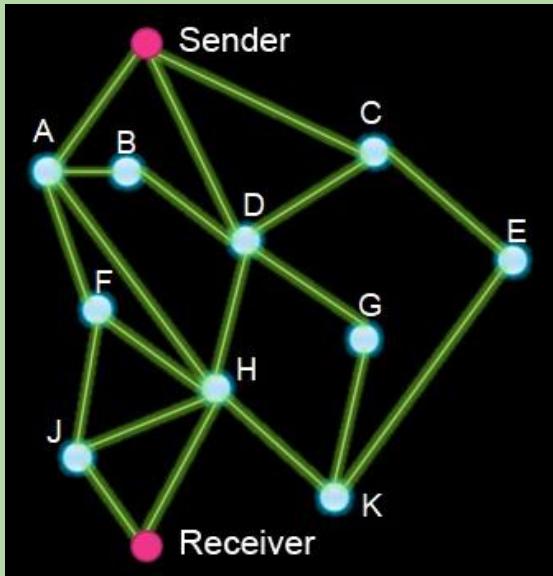


X the **TWO** correct answer choices:

	(A)
	(B)
	(C)
	(D)

[Check your answer!](#)

Answer the two questions on the right for the image below:



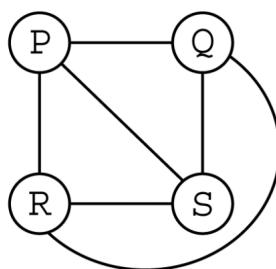
a. What is the *minimum* number of connections that need to be broken or removed before the sender and the receiver can't communicate?

b. What is the *maximum* number of nodes that can fail and still let the sender and receiver communicate? Which nodes?

[Check answer](#)

AP Exam Practice Question

The following figure represents a network of physically linked devices labeled P through S. A line between two devices indicates a connection. Devices can communicate only through the connections shown.



Which of the following statements best explains the ability of the network to provide fault tolerance?

- A The network is considered fault-tolerant because there are redundant paths between each pair of devices.
- B The network is considered fault-tolerant because it guarantees that no individual component will fail.
- C The network is not considered fault-tolerant because it relies on physical connections.
- D The network is not considered fault-tolerant because it provides more paths than are needed.

My answer:

[Check!](#)

AP Exam Practice Question

A local router is configured to limit the bandwidth of guest users connecting to the Internet. Which of the following best explains the result of this configuration as compared to a configuration in which the router does not limit the bandwidth?

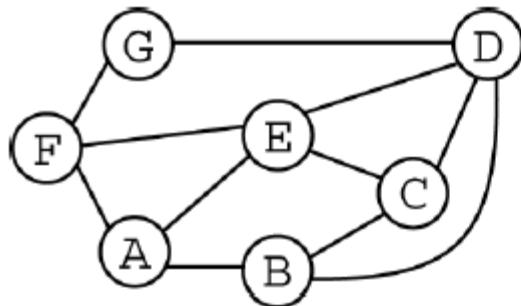
- A The amount of time it takes guest users to send and receive large files is likely to decrease.
- B The number of packets required for guest users to send and receive data is likely to decrease.
- C Guest users will be prevented from having fault-tolerant routing on the Internet.
- D Guest users will be restricted in the maximum amount of data that they can send and receive per second.

My answer:

[Check](#)

AP Exam Practice Question

The figure below represents a network of physically linked computers labeled A through G. A line between two computers indicates that the computers can communicate directly with each other. Any information sent between two computers that are not directly connected must go through at least one other computer. For example, information can be sent directly between computers A and B, but information sent between computers A and C must go through other computers.



What is the minimum number of connections that must be broken or removed in the network before computer E can no longer communicate with computer F?

A

1

 B

2

 C

3

 D

4

My answer:[Check!](#)**AP Exam Practice Question**

Which of the following is a primary benefit of making a computing system fault-tolerant?

 A

If one component of the system fails, users of the system can often still access it.

 B

If one component of the system is hacked, no information will be stolen.

 C

If the system becomes too expensive, making it fault-tolerant will save money.

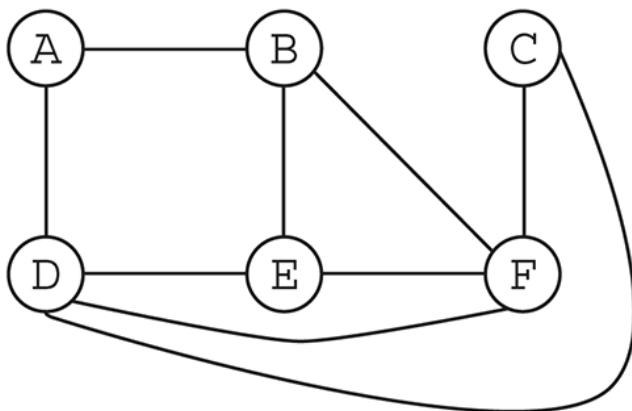
 D

If the system cannot operate efficiently, making it fault-tolerant will speed up its operation.

My answer:[Check](#)

AP Exam Practice Question

The figure below represents a network of physically linked devices, labeled A through F. A line between two devices indicates a connection. Devices can communicate only through the connections shown.



Which of the following statements are true about the ability for devices A and C to communicate?

Select two answers.

A

If devices B and D were to fail, then information sent from device A could not reach device C.

B

If devices B and F were to fail, then information sent from device A could not reach device C.

C

If devices D and F were to fail, then information sent from device A could not reach device C.

D

If devices E and F were to fail, then information sent from device A could not reach device C.

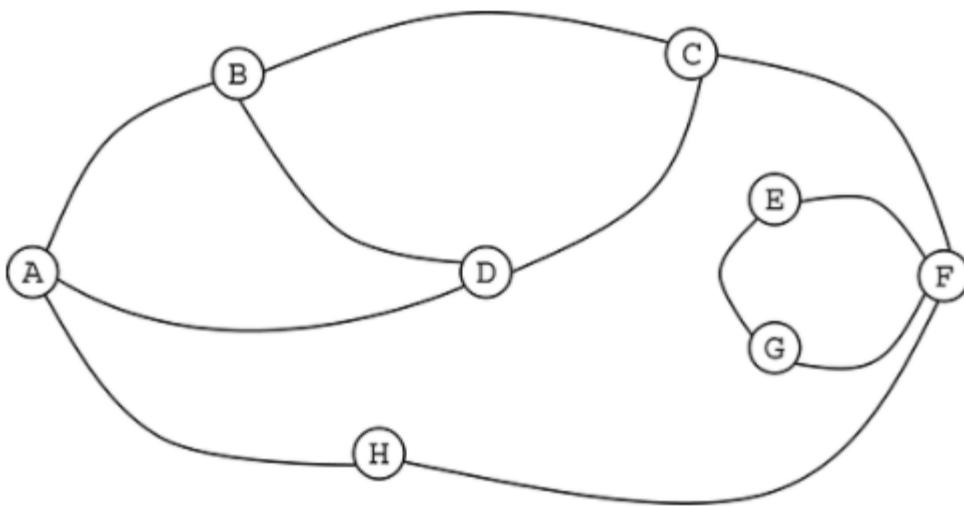
My answers:

and

[Check!](#)

AP Exam Practice Question

The figure below represents a network of physically linked devices, labeled A through H. A line between two devices indicates a connection. Devices can communicate only through the connections shown.



What is the minimum number of connections that would need to be removed from the network in order for device A to not be able to communicate with device F?

A

2

B

3

C

4

D

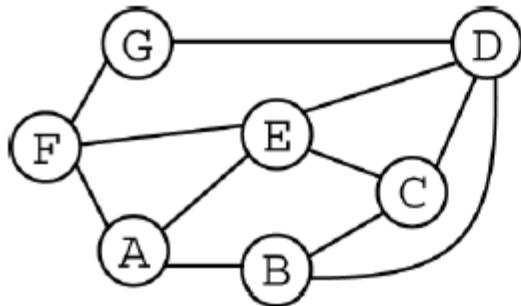
5

My answer:

[Check!](#)

AP Exam Practice Question

The figure below represents a network of physically linked computers labeled A through G. A line between two computers indicates that the computers can communicate directly with each other. Any information sent between two computers that are not directly connected must go through at least one other computer. For example, information can be sent directly between computers A and B, but information sent between computers A and C must go through other computers.



Which of the following statements about security in the network is true?

- I. Computers A and D need to communicate with at least two additional computers in the network in order to communicate with each other.
- II. Computers B and C can communicate with each other without additional computers being aware of the communication.

A I only

B II only

C I and II

D Neither I nor II

My answer:

[Check!](#)

DONE WITH PACKET 3

Answer ([back](#))

Correct Answer: C

Which of the following actions is most likely to raise legal or ethical concerns?

A

An analyst writes a program that scans through a database of open-access scientific journals and creates a document with links to articles written on a particular topic.

B

A computer scientist adds several features to an open-source software program that was designed by another individual.

C

A musician creates a song using samples of a copyrighted work and then uses a Creative Commons license to publish the song.

D

A public interest group alerts people to a scam that involves charging them for a program that is available for free under a Creative Commons license.

Explanations:

Answer A

Incorrect. Open-access journals are free from restrictions on access, so collecting this information does not raise any legal or ethical concerns.

Answer B

Incorrect. Open-source software can be freely modified, and doing so does not in itself raise any legal or ethical concerns.

Answer C

Correct. The use of material created by someone else without permission raises ethical concerns and can have legal consequences. Using a Creative Commons license to publish a derived work does not free the musician from having to first obtain permission.

Answer D

Incorrect. While charging people for software that can be obtained for free may be unethical (and possibly illegal), alerting people to a scam does not raise any legal or ethical concerns.

Answer ([back](#))

Correct Answer: A

A researcher wants to publish the results of a study in an open access journal. Which of the following is a direct benefit of publishing the results in this type of publication?

A

The researcher can allow the results to be easily obtained by other researchers and members of the general public.



B

The researcher can better anticipate the effect of the results and ensure that they are used responsibly.

C

The researcher can ensure that any personal information contained in the journal is kept private and secure.

D

The researcher can prevent copies of the research from being accessed by academic rivals.

Explanations:

Answer A

Correct. Information published in an open access journal is free of any and all restrictions on access and free of many restrictions on use, such as copyright or license restriction. This allows other researchers and members of the general public broad access to the results.

Answer B

Incorrect. Not every effect can be anticipated in advance. Information published in an open access journal can be broadly accessed, which could lead to individuals using the results irresponsibly.

Answer C

Incorrect. Information published in an open access journal can be broadly accessed. Researchers should take care to avoid including personal information in publications.

Answer D

Incorrect. Information published in an open access journal can be broadly accessed, which could lead to academic rivals gaining access to the results.

Answer ([back](#))

Correct Answer: C

An author is considering publishing an e-book using a Creative Commons license. In which of the following situations would it be better for the author to use a Creative Commons license instead of a traditional copyright?

- I. The author wants to make the e-book available as a free download.
- II. The author wants to prevent people from sharing copies of the e-book on peer-to-peer networks.
- III. The author wants to allow people permission to use and modify the e-book.

A

I only

B

II only

C

I and III

D

II and III

Explanations:

Answer A

This option is incorrect. Statement III is also correct because under Creative Commons the author can stipulate what kind of modification is allowed by users.

Answer B

This option is incorrect. Statement II is not correct because Creative Commons was not meant to be used to prevent sharing.

Answer C

This option is correct. Statement I is correct because the Creative Commons license is designed to increase the amount of content available to the public for free. Statement III is correct because under Creative Commons the author can stipulate what kind of modification is allowed by users.

Answer D

This option is incorrect. Statement III indicates that it would be better for the author to use a Creative Commons license because the author wants to allow permission to use and modify the e-book.

Answer ([back](#))

Correct Answer: D

A programmer created a piece of software and wants to publish it using a Creative Commons license. Which of the following is a direct benefit of publishing the software with this type of license?

- A The programmer can ensure that the algorithms used in the software are free from bias.
- B The programmer can ensure that the source code for the software is backed up for archival purposes.
- C The programmer can include code that was written by other people in the software without needing to obtain permission.
- D The programmer can specify the ways that other people are legally allowed to use and distribute the software.

Explanations:

Answer A

Incorrect. The way that the software is published does not directly affect the algorithms contained in the software. The programmer must take action to avoid bias. The programmer cannot rely on a Creative Commons license for this purpose.

Answer B

Incorrect. Software can be backed up for archival purposes regardless of how it is published.

Answer C

Incorrect. Publishing the software using a Creative Commons license does not enable the programmer to freely use the intellectual property of others. The programmer must obtain permission to use borrowed code, either by directly asking the copyright owner or by verifying that the borrowed code was published using a license that allows for reuse.

Answer D

Correct. A Creative Commons license allows an author to impose restrictions on the use of the licensed product, including restrictions on commercial use.

Answer ([back](#))

Correct Answer: C

Which of the following is considered an **unethical** use of computer resources?

A

Downloading freeware or shareware onto your home computer

B

Purchasing a game from an app store and downloading it directly to a mobile device

C

Purchasing a single-user copy of photo editing software and installing it on all the computers in a computer lab

D

Searching online for an electronic version of a school textbook

Explanations:

Answer A

This option is incorrect. Freeware or shareware is generally intended for download onto a home computer and this use is considered ethical.

Answer B

This option is incorrect. App stores are online retailers who sell games and other applications that are downloaded directly onto devices. This use is considered ethical.

Answer C

This option is correct. Single-user copies of software are meant for one individual to use. Computer labs are meant for public use, so installing the software on the computers raises ethical concerns.

Answer D

This option is incorrect. Online searches themselves are ethical, even if for copyrighted materials.

NOTE on D: The act of searching itself is not unethical... **but** if you found the textbook online then downloaded it and used it without having the right to do so, then **that** would have been unethical!

Answer ([back](#))

Correct Answer: A

The developers of a music-streaming application are updating the algorithm they use to recommend music to listeners. Which of the following strategies is LEAST likely to introduce bias into the application?

A

Making recommendations based on listening data gathered from a random sample of users of the application

B

Making recommendations based on the most frequently played songs on a local radio station

C

Making recommendations based on the music tastes of the developers of the application

D

Making recommendations based on a survey that is sent out to the 1,000 most active users of the application

Explanations:

Answer A

Correct. Basing the recommendation algorithm on data from a random sample of users will help ensure that the data gathered are more representative of all users of the application. Gathering data from a representative sample can help the developers avoid bias.

Answer B

Incorrect. The selections of a local radio station can reflect existing human biases. Making recommendations using only this data may lead to bias in the application.

Answer C

Incorrect. The music tastes of the developers can reflect existing human biases. Making recommendations using only this data may lead to bias in the application.

Answer D

Incorrect. The most active users of the application are unlikely to be representative of all users of the application. Using data from only this group may lead to bias in the application.

Answer ([back](#))

Correct Answer: D

Which of the following is most likely to be a beneficial effect of using MeeReader?

A

Users may have a reduced risk of the application being used in unintended ways.

B

Users may have a reduced risk of their biometric data being misused.

C

Users with limited Internet access may be able to more easily obtain books and articles.

D

Users with visual impairments may be able to more easily read or listen to books and articles.



Explanations:

Answer A

Incorrect. Applications have the potential to be used in ways that their creators had not originally intended.

Answer B

Incorrect. The application uses facial recognition software to determine the user's identity, so it is unlikely that users will have a reduced risk of their biometric data being misused.

Answer C

Incorrect. The application must download books and articles from the Internet, so it is unlikely that users with limited Internet access will have an improved ability to obtain books and articles.

Answer D

Correct. Users with visual impairments can set their personal preferences to make text easier for them to read. These users can also enable text-to-speech to allow them to listen to text.

Answer ([back](#))

Correct Answer: A

From the perspective of the application's developers, which of the following is most likely to be a benefit of storing all user data in a database?

A

The developers can analyze the data to make improvements to the application based on user behavior.



B

The developers can analyze the data to ensure that no patterns emerge in the data.

C

The developers can reduce the amount of data storage required to support the application.

D

The developers can reduce the need for data encryption.

Explanations:

Answer A

Correct. By storing user data, the developers can use machine learning and data mining and thereby make improvements based on the users' needs.

Answer B

Incorrect. There is not likely to be a benefit in attempting to hide patterns in the data. Patterns in user behavior can help inform future development.

Answer C

Incorrect. Storing user data will increase the amount of data storage needed, which is likely to increase the data storage requirements.

Answer D

Incorrect. Storing personal data will increase the amount of personal information stored, which is likely to increase the need for encryption.

Answer ([back](#))

Correct Answer: A

A mobile game tracks players' locations using GPS. The game offers special in-game items to players when they visit real-world points of interest. Which of the following best explains how bias could occur in the game?

A

Points of interest may be more densely located in cities, favoring players in urban areas over players in rural areas.



B

Some players may engage in trespassing, favoring players in urban areas over players in rural areas.

C

Special items may not be useful to all players, favoring players in urban areas over players in rural areas.

D

Weather conditions may be unpredictable, favoring players in urban areas over players in rural areas.

Explanations:

Answer A

Correct. Urban areas generally have a higher density of points of interest. In addition, people in urban areas may be able to easily travel to points of interest on foot. These factors can give players in urban areas easier access to special items in the game.

Answer B

Incorrect. The choice of players to trespass on private property is not significantly affected by players' locations.

Answer C

Incorrect. The usefulness of special items to players is not significantly affected by the players' locations.

Answer D

Incorrect. The unpredictability of weather affects players in both urban and rural locations, so there is no bias toward either group.

Answer ([back](#))

Correct Answer: B

A software development company has created an application called FileCleanUp. When the application is run on a user device, it searches for all files (including pictures, videos, and documents) that have not been accessed in the past month, stores them on the company's Web server, and deletes them from the user device. The application runs once each day. Users have the ability to manually retrieve files from the server if they are needed.

Which of the following is most likely to be a harmful effect of using FileCleanUp?

A It prevents users from accessing frequently used files when there is no Internet connectivity.

B It prevents users from accessing infrequently used files when there is no Internet connectivity. ✓

C It prevents users from accessing frequently used files when there is reliable Internet connectivity.

D It prevents users from accessing infrequently used files when there is reliable Internet connectivity.

Explanations:

Answer A

Incorrect. Frequently used files are kept on user devices, so they are accessible when there is no Internet connectivity.

Answer B

Correct. Infrequently used files are removed from user devices and stored on a Web server. If a user has no Internet connection, the user will be unable to access these files.

Answer C

Incorrect. Frequently used files are kept on user devices, so they are accessible regardless of whether there is Internet connectivity.

Answer D

Incorrect. Infrequently used files are removed from user devices and stored on a Web server. If a user has a reliable Internet connection, the user will be able to manually retrieve these files.

Answer ([back](#))

Correct Answer: B

A software company is designing a mobile game system that should be able to recognize the faces of people who are playing the game and automatically load their profiles. Which of the following actions is most likely to reduce the possibility of bias in the system?

A

Testing the system with members of the software company's staff

B

Testing the system with people of different ages, genders, and ethnicities



C

Testing the system to make sure that the rules of the game are clearly explained

D

Testing the system to make sure that players cannot create multiple profiles

Explanations:

Answer A

Incorrect. Testing the facial recognition system on only staff members leaves open the possibility that the system will be able to recognize only people who look like the staff members.

Answer B

Correct. Testing the system with people of different ages, genders, and ethnicities will help reduce the chances that the facial recognition system recognizes only people who look like the developers of the system.

Answer C

Incorrect. While it is important that the rules of the game are clearly explained to players, this action does not address the potential biases in the facial recognition component of the system.

Answer D

Incorrect. While it may be useful to prevent players from creating multiple profiles, this action does not address the potential biases in the facial recognition component of the system.

Answer ([back](#))

Correct Answer: C

A user purchased a new smart home device with embedded software and connected the device to a home network. The user then registered the device with the manufacturer, setting up an account using a personal e-mail and password. Which of the following explains how a phishing attack could occur against the user of the smart home device?

A

A vulnerability in the device's software is exploited to gain unauthorized access to other devices on the user's home network.

B

A vulnerability in the device's software is exploited to install software that reveals the user's password to an unauthorized individual.

C

The user is sent an e-mail appearing to be from the manufacturer, asking the user to confirm the account password by clicking on a link in the e-mail and entering the password on the resulting page.



D

The user's account is sent an overwhelming number of messages in an attempt to disrupt service on the user's home network.

Explanation:

C is the correct answer because phishing is a technique that attempts to trick a user into providing personal information. If you then receive a fake email from what *appears to be the manufacturer*, you are being phished! An attacker out there found out that you purchased that item and registered it with that email address, so took advantage of that by sending you a fake email from a fake manufacturer which you might get tricked into clicking.

Answer ([back](#))

Correct Answer: D

A user unintentionally installs keylogging software on a computer. Which of the following is an example of how the keylogging software can be used by an unauthorized individual to gain access to computing resources?

- A The software gives an unauthorized individual remote access to the computer, allowing the individual to search the computer for personal information.
- B The software installs a virus on the computer and prompts the user to make a payment to the unauthorized individual to remove the virus.
- C The software prompts the user to enter personal information to verify the user's identity. This personal information is recorded and transmitted to an unauthorized individual.
- D The software records all user input on the computer. The recorded information is transmitted to an unauthorized individual, who analyzes it to determine the user's login passwords. 

Explanations:

Answer A

Incorrect. While an unauthorized individual can obtain private information by this method, it is not an example of keylogging. Keylogging software captures user input in order to gain fraudulent access to passwords and other confidential information.

Answer B

Incorrect. While an unauthorized individual can obtain a user's payment information by this method, it is not an example of keylogging. Keylogging software captures user input in order to gain fraudulent access to passwords and other confidential information.

Answer C

Incorrect. While an unauthorized individual can obtain a user's personal information by this method, it is not an example of keylogging. Keylogging software captures user input in order to gain fraudulent access to passwords and other confidential information.

Answer D

Correct. Keylogging is the use of a program to record user input in order to gain fraudulent access to passwords and other confidential information.

Answer ([back](#))

Correct Answer: B

An individual receives an e-mail that appears to be from an insurance company. The message offers a lower insurance rate, and prompts the recipient to click a link to learn more. Which of the following is most indicative that the e-mail is part of a phishing attempt?

A

After clicking the link, a browser cookie is downloaded to the recipient's computer.

B

After clicking the link, a Web page opens that prompts the recipient for personal information.

C

After clicking the link, the recipient's private network becomes publicly visible via a rogue access point.

D

After clicking the link, software is installed on the recipient's computer that records every keystroke made on the computer.

Explanations:

Answer A

Incorrect. A cookie is a file that is stored on an individual's computer by a Web browser. Cookies can be used for authentication or to store Web site preferences. Storing a cookie is not an example of a phishing attack.

Answer B

Correct. A phishing attack is an attempt to trick individuals into providing personal information, often by getting them to fill out a form on a malicious Web site.

Answer C

Incorrect. A rogue access point is a wireless access point that gives unauthorized access to secure networks. It is not an example of a phishing attack.

Answer D

Incorrect. Keylogging is the practice of recording every keystroke made by a computer user to gain fraudulent access to passwords and other confidential information. It is not an example of a phishing attack.

[Answer](#) ([back](#))

Correct Answer: D

A Web site uses several strategies to prevent unauthorized individuals from accessing user accounts. Which of the following is NOT an example of multifactor authentication?

- A Each employee for a company is issued a USB device that contains a unique token code. To log into a company computer, an employee must insert the USB device into the computer and provide a correct password.
- B After logging into an account from a new device, a user must enter a code that is sent via e-mail to the e-mail address on file with the account.
- C In order to log into an account, a user must provide both a password and a fingerprint that is captured using the user's device.
- D When a user enters an incorrect password more than two times in a row, the user is locked out of the account for 24 hours.

Explanations:

A: Incorrect. The correct password is **one** piece of information used to authenticate, and the unique code from a USB token device is the **second** piece of information. Because there are **two** different pieces of information used, this **is** an example of multifactor authentication.

B: Incorrect. The correct password is **one** piece of information used to authenticate, and the unique code sent to the user's email is the **second** piece of information. Because there are **two** different pieces of information used, this **is** an example of multifactor authentication.

C: Incorrect. The correct password is **one** piece of information used to authenticate, and the unique code sent to the user's fingerprint is the **second** piece of information. Because there are **two** different pieces of information used, this **is** an example of multifactor authentication.

D: Correct. The only piece of information being used in this authentication scenario is the password -- this is just **one** piece of information used (the user is just trying to use the same password over and over again). Because there is only **one** piece of information being used, this is **NOT** an example of multifactor authentication.

Answer ([back](#))

Correct Answer: C

Which of the following best exemplifies the use of multifactor authentication?

A

A computing device enables users to input information using multiple interfaces, including a keyboard, a mouse, and a touch pad.

B

A user employs a public key encryption method that uses one key to encrypt information and a different key to decrypt information.

C

A Web site requires a user to enter a password as well as a numeric code received via text message before the user can log in to an account.

D

Multiple users share an account to a Web-based software program, and each user has an individual username and password.

Explanations:

Answer A

Incorrect. While many devices use multiple input interfaces, this does not use multiple factors to authenticate the identity of the user.

Answer B

Incorrect. While public key encryption is a method of protecting digital data, it does not necessarily use multiple factors to authenticate the identity of the user.

Answer C

Correct. Multifactor authentication is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism. In this case, the user shows knowledge of a password and shows possession of the device that receives the text message.

Answer D

Incorrect. While some online accounts can be shared among multiple users (each with their own username and password), this does not use multiple factors to authenticate the identity of a user.

Answer ([back](#))

Correct Answer: D

A city's police department has installed cameras throughout city streets. The cameras capture and store license plate data from cars driven and parked throughout the city. The authorities use recorded license plate data to identify stolen cars and to enforce parking regulations.

Which of the following best describes a privacy risk that could occur if this method of data collection is misused?

- A The cameras may not be able to read license plates in poor weather conditions.
- B Local business owners could lose customers who are unwilling to park in the city.
- C Traffic personnel who work for the city could lose their jobs if their services are no longer needed.
- D The vehicle location data could be used to monitor the movements of city residents.

Explanations:

Answer A

Incorrect. While the inability of the cameras to function properly in poor weather conditions could make traffic enforcement more difficult, this is not considered a privacy issue.

Answer B

Incorrect. While the potential loss of customers may negatively affect local businesses, this is not considered a privacy issue.

Answer C

Incorrect. While some city employees may lose jobs as a result of this technology, this is not considered a privacy issue.

Answer D

Correct. The data collected by the cameras could be misused by anyone with access to the database to track the movements of drivers, even when there is no legal justification.

Answer ([back](#))

Correct Answer: B

Which of the following is most likely to be a data privacy concern for StreamPal users?

A

Users of the application are required to rate songs in order to enable all of the application's features.

B

Users of the application may have the ability to determine information about the locations of users that are not on their contact list. 

C

Users of the application may not be able to use the application if they are located in an area with a poor Internet connection.

D

Users of the application may not have similar music taste to any other users on their contact list.

Explanations:

Answer A

Incorrect. Requiring users to rate songs is not considered a privacy concern.

Answer B

Correct. A user can see a map of other people in the area who may not be on the user's contact list.

Answer C

Incorrect. Requiring users to have a reliable Internet connection is not considered a privacy concern.

Answer D

Incorrect. A user not having similar music taste to other users is not considered a privacy concern.

Answer ([back](#))

Correct Answer: B

Which of the following statements is most likely true about the differences between the basic version and the premium version of StreamPal?

A

Users of the basic version of StreamPal are more likely to give songs higher ratings than are users of the premium version of StreamPal.

B

Users of the basic version of StreamPal indirectly support StreamPal by allowing themselves to receive advertisements. 

C

Users of the basic version of StreamPal spend more on monthly fees than do users of the premium version of StreamPal.

D

Users of the basic version of StreamPal use less data storage space on their devices than do users of the premium version of StreamPal.

Explanations:

Answer A

Incorrect. There is no indication that the users of the basic version will rate songs differently than users of the premium version will.

Answer B

Correct. By allowing themselves to see advertisements, users of the basic version of the application enable the developers of the application to receive financial support.

Answer C

Incorrect. Users of the premium version pay monthly fees, not users of the basic version.

Answer D

Incorrect. There is no indication that the basic version requires less storage space than the premium version does.

Answer ([back](#))

Correct Answer: B

Many Web browsers allow users to open anonymous windows. During a browsing session in an anonymous window, the browser does not record a browsing history or a list of downloaded files. When the anonymous window is exited, cookies created during the session are deleted. Which of the following statements about browsing sessions in an anonymous window is true?

- A The activities of a user browsing in an anonymous window will not be visible to people who monitor the user's network, such as the system administrator.
- B Items placed in a Web store's shopping cart for future purchase during the anonymous browsing session will not be saved on the user's computer.
- C A user will not be able to log in to e-mail or social media accounts during the anonymous browsing session.
- D A user browsing in an anonymous window will be protected from viruses launched from any Web sites visited or files downloaded.

Explanations:

Answer A

This option is incorrect. If a user is working from a network, such as at work or at school, the administrator of that network can monitor all activity of a user, including information that is sent to the Internet.

Answer B

This option is correct. Because the cookies created during the anonymous browsing session were deleted, no information exists in the browser to inform future visits to the same website. Thus, any shopping cart items will not be available for future purchase.

Answer C

This option is incorrect. Users of anonymous browsing sessions may log into email, social media, or other accounts that are on the Internet.

Answer D

This option is incorrect. Users of anonymous browsing sessions send data to and receive data from the Internet, including viruses.

Answer ([back](#))

Correct Answer: C

Which of the following actions is most likely to raise legal or ethical concerns?

A

An analyst writes a program that scans through a database of open-access scientific journals and creates a document with links to articles written on a particular topic.

B

A computer scientist adds several features to an open-source software program that was designed by another individual.

C

A musician creates a song using samples of a copyrighted work and then uses a Creative Commons license to publish the song.

D

A public interest group alerts people to a scam that involves charging them for a program that is available for free under a Creative Commons license.

Explanations:

Answer A

Incorrect. Open-access journals are free from restrictions on access, so collecting this information does not raise any legal or ethical concerns.

Answer B

Incorrect. Open-source software can be freely modified, and doing so does not in itself raise any legal or ethical concerns.

Answer C

Correct. The use of material created by someone else without permission raises ethical concerns and can have legal consequences. Using a Creative Commons license to publish a derived work does not free the musician from having to first obtain permission.

Answer D

Incorrect. While charging people for software that can be obtained for free may be unethical (and possibly illegal), alerting people to a scam does not raise any legal or ethical concerns.

Answer ([back](#))

Correct Answer: A

Which of the following are true statements about digital certificates in Web browsers?

- I. Digital certificates are used to verify the ownership of encrypted keys used in secured communication.
- II. Digital certificates are used to verify that the connection to a Web site is fault tolerant.

A

I only

B

II only

C

I and II

D

Neither I nor II

Explanations:

Statement I is exactly what digital certificates are used for!

Statement II, however, involves fault tolerance, which has nothing to do with encryption or security (fault tolerance has to do with how data is sent over the internet -- if one connection breaks, the information can still get from sender to receiver!).

So the correct choice is A

Answer ([back](#))

Correct Answer: C

Which of the following activities poses the greatest personal cybersecurity risk?

A

Making a purchase at an online store that uses public key encryption to transmit credit card information

B

Paying a bill using a secure electronic payment system

C

Reserving a hotel room by e-mailing a credit card number to a hotel

D

Withdrawing money from a bank account using an automated teller machine (ATM)

Explanations:

Answer A

This option is incorrect. Public key encryption is widely used because of the functionality it provides in addressing cybersecurity issues when sending information across the Internet.

Answer B

This option is incorrect. Secure electronic payment systems are designed to address cybersecurity issues and are not considered a risk.

Answer C

This option is correct. As an email message passes through the Internet, it goes through intermediate computers and routers. These computers and routers could read the contents of the email. The credit card number could be read from the email.

Answer D

This option is incorrect. Automated teller machines are designed to address cybersecurity issues.

Answer ([back](#))

Correct Answer: A

Which of the following has the greatest potential for compromising a user's personal privacy?

A A group of cookies stored by the user's Web browser

B The Internet Protocol (IP) address of the user's computer

C The user's e-mail address

D The user's public key used for encryption

Explanations:

Answer A

This option is correct. The aggregation of information in browser cookies can be used by websites that the user visits to track the user and collect information about the user.

Answer B

This option is incorrect. The IP address of a user's computer is required for the user to send and receive information on the Internet. The IP address in itself does not contain any extra information about the user.

Answer C

This option is incorrect. A user's email address is required to receive email from other people. An email address in itself does not contain any extra information about the user.

Answer D

This option is incorrect. In public key encryption, a person or organization who wants to receive encrypted information via the Internet posts their public key for anyone to use. By its nature, this key is meant to be public and thus does not compromise personal privacy.

Answer ([back](#))

Correct Answer: D

Which of the following best illustrates symmetric key encryption?

- A Abe writes a message and seals it in an envelope. She addresses it to his friend, Emily. Abe hands the envelope to Frank, who then delivers it to Emily. Emily opens the envelope and reads the message.
- B Barb writes a message, folds it up, and hides the message behind the trashcan in the cafeteria. She tells her friend Raymond where to find the message. Raymond locates the message, then opens it privately so no one else can read it.
- C Cathy writes a message and slides it through the opening in Jared's locker. Jared is the only one that knows the combination to his locker. At the end of the school day, Jared unlocks his locker and retrieves the message from Cathy.
- D David writes a message, then encodes each letter of the message with another symbol by using a secret key to map each letter to a new symbol. David hands the message to his friend, Debra, and tells her the secret key. Debra uses that same key to decode the message and read it.

Explanation:

Symmetric key encryption involves using the **same** key to encode and decode a message; the only scenario that illustrates this is D. What is being described in D is a lot like this example of symmetric key encryption that saw in class:



In this simple example, the **key is 3** (used for both encryption and decryption)

Answer ([back](#))

Correct Answer: C

Which of the following best illustrates public key encryption?

A

Abe has a mailbox with a single unlocked door on the front that can be used to deposit and take out the mail.

B

Barbara has a mailbox with a single locked door on the front that can be used to deposit and take out the mail. Barbara has made two copies of the key to the door and hangs one above the mailbox so anyone can unlock an open the door and deposit mail in. She uses her copy of the key to unlock it and take the mail out.

C

Cathy has a mailbox with one locked door on the top and a second locked door on the bottom. Both doors have different keys. Cathy hangs the key to the top door above the mailbox so anyone can unlock the door and drop mail in. Then Cathy can use the key to the bottom door (which only she has) to unlock it and take the mail out (assume people that drop the mail in the top door can't access the lower part of the mailbox).

D

David asks people slide mail under his door. He is the only person with the key to his apartment, and he uses that key to get into his apartment and get his mail.

Explanation:

Public key encryption involves using two different keys for encrypting and decrypting. In scenario C, there is a **public key** (the one hanging above the mailbox used to unlock to top door) and a **private key** (the one Cathy has to unlock the bottom door).

None of the other scenarios involve using two different keys:

- Scenario A involves no keys
- Scenario B involves only one key (this scenario one better illustrates **symmetric** key encryption)
- Scenario D involves only one key (his key to his apartment)

Answer ([back](#))

Correct Answer: D

Which of the following applications is most likely to benefit from the use of crowdsourcing?

A

An application that allows users to convert measurement units (e.g., inches to centimeters, ounces to liters)

B

An application that allows users to purchase tickets for a local museum

C

An application that allows users to compress the pictures on their devices to optimize storage space

D

An application that allows users to view descriptions and photographs of local landmarks

Explanations:

Answer A

Incorrect. Conversion formulas between units are well known, so they would not require updates or contributions from a large number of users.

Answer B

Incorrect. This type of transaction is between a user and a company and does not rely on the use of information contributed by a large number of users.

Answer C

Incorrect. Compressing a user's pictures only affects data on the user's device. It does not rely on information contributed by a large number of users.

Answer D

Correct. Crowdsourcing is the practice of obtaining input or information from a large number of people via the Internet. This application would benefit from the use of crowdsourcing the most, as the application could allow users to contribute descriptions and photographs of landmarks.

Answer ([back](#))

Correct Answer: C

A mobile application is used to display local traffic conditions. Which of the following features of the application best exemplifies the use of crowdsourcing?

A

Users can save an address to be used at a later time.

B

Users can turn on alerts to be notified about traffic accidents.

C

Users can submit updates on local traffic conditions in real time.

D

Users can use the application to avoid heavily congested areas.

Explanations:

Answer A

Incorrect. While saving an address does provide information to the application, this information is for individual use. It is not collected and aggregated by the application to make recommendations to other users.

Answer B

Incorrect. The alert feature described is a one-way communication between the application and the user. It does not directly obtain input or information from a large number of users.

Answer C

Correct. Crowdsourcing is the practice of obtaining information from a large number of people. In this application, users can provide information about traffic and road condition updates in real time. This information can be used by the application to make recommendations to other users.

Answer D

Incorrect. Using the application to avoid congested areas is a benefit to users. This action does not directly obtain input or information from a large number of users.

Answer ([back](#))

Correct Answer: B

Which of the following actions is most likely to help reduce the digital divide?

A

Adding a requirement that all users of a popular social media site link their accounts with a phone number.

B

Deploying satellites and other infrastructure to provide inexpensive Internet access to remote areas of Earth

C

Digitizing millions of books from university libraries, making their full text available online

D

Offering improved Internet connections to Internet users who are willing to pay a premium fee for more bandwidth

Explanations:

Answer A

Incorrect. While linking a social media account to a phone number may improve the security of the site, it does not improve access to devices and the Internet.

Answer B

Correct. One contributing factor to the digital divide is lack of access to the Internet. Deploying more satellites and network infrastructure would provide a way to allow Internet access in remote areas.

Answer C

Incorrect. Adding a large library of information to the Internet would not help reduce the digital divide. Anyone without Internet access would not be able to take advantage of the information online.

Answer D

Incorrect. Offering higher bandwidth Internet service for a premium fee is likely to increase the gap in access between individuals who can afford to pay a higher rate and those who cannot.

Answer ([back](#))

Correct Answer: C

A city government is attempting to reduce the digital divide between groups with differing access to computing and the Internet. Which of the following activities is LEAST likely to be effective in this purpose?

- A Holding basic computer classes at community centers
- B Providing free wireless Internet connections at locations in low-income neighborhoods
- C Putting all government forms on the city Web site
- D Requiring that every city school has computers that meet a minimum hardware and software standard

Explanations:

Answer A

This option is incorrect. Classes at community centers would be accessible to many citizens and would allow more people to effectively use computing technology. This activity is likely to be effective in reducing the digital divide.

Answer B

This option is incorrect. Providing free wireless Internet is likely to give more groups access to the Internet and thus reduce the digital divide.

Answer C

This option is correct. Putting all government forms on the city website is least likely to be effective in reducing the digital divide because all citizens may not have equitable access to the Internet.

Answer D

This option is incorrect. Requiring every city school to have computers that meet minimum standards would allow all students equal access to computing, and thus it is likely to reduce the digital divide.

Answer ([back](#))

Correct Answer: C

Which of the following is LEAST likely to be a contributing factor to the digital divide?

A

Some individuals and groups are economically disadvantaged and cannot afford computing devices or Internet connectivity.

B

Some individuals and groups do not have the necessary experience or education to use computing devices or the Internet effectively.

C

Some parents prefer to limit the amount of time their children spend using computing devices or the Internet.

D

Some residents in remote regions of the world do not have access to the infrastructure necessary to support reliable Internet connectivity.

Explanations:

Answer A

Incorrect. Income is a factor contributing to the digital divide. The cost of computing devices or Internet connectivity is prohibitive for some people.

Answer B

Incorrect. Education is a factor contributing to the digital divide. Some individuals who did not grow up with access to computing devices lack the experience or education necessary to use computing devices effectively.

Answer C

Correct. The digital divide refers to differing access to computing devices and the Internet, based on socioeconomic, geographic, or demographic characteristics. Placing a restriction on the amount of time children spend on a computer is not considered a factor contributing to the digital divide.

Answer D

Incorrect. Access to the Internet is a factor contributing to the digital divide. Some remote regions do not have reliable Internet infrastructure available.

Answer ([back](#))

Correct Answer: C

Which of the following actions is most likely to be effective in reducing the digital divide at a local level?

- A Creating an application that offers coupons and discounts for local businesses
- B Offering a discount to utility customers who pay their bills online instead of by mail
- C Providing free community access to computers at schools, libraries, and community centers
- D Requiring applicants for local government jobs to complete an online application

Explanations:

Answer A

Incorrect. Some individuals do not have access to the Internet or modern devices, so they would not be able to take advantage of the coupons and discounts offered through an application. This action does not improve their access to devices and the Internet.

Answer B

Incorrect. Some individuals do not have access to the Internet at home. This action does not improve their access to devices and the Internet.

Answer C

Correct. Some individuals do not have access to the Internet at home. Providing access to computers at schools, libraries, and other public facilities would give them improved equity and access.

Answer D

Incorrect. Some individuals do not have access to the Internet at home, so they would not have access to job applications made exclusively online. This action does not improve their access to devices and the Internet.

Answer ([back](#))

Correct Answer: C

Which of the following school policies is most likely to have a positive impact on the digital divide?

A

A school allows students to bring a graphing calculator from home to complete in-class mathematics assignments.

B

A school allows students to bring a tablet computer to class every day to participate in graded quizzes.

C

A school provides a laptop or tablet computer to all students enrolled at the school.

D

A school recommends that all students purchase a computer with as much processing speed as possible so that projects run faster.

Explanation:

C is correct because it's the only option that aims to ensure all students have a device without requiring them to purchase or obtain the device themselves (thus, removing potentially costly barriers to families).

Answer ([back](#))

Correct Answer: B

Both online newspapers and social media sites are used to distribute information on the Internet. Which of the following best describes an advantage that online newspapers have over social media sites?

A

The ability to distribute information instantaneously

B

The ability to provide credibility to the information distributed

C

The ability to provide information that is widely accessible

D

The ability to provide media-rich content for low cost

Explanations:

Answer A

This option is incorrect. Both online newspapers and social media sites allow people to distribute information instantaneously.

Answer B

This option is correct. Online newspapers are usually run out in the open, in that the people who create the newspaper are clearly noted on the website. In addition, these online newspapers are often connected to physical newspapers, which are considered credible sources of information.

Answer C

This option is incorrect. Both online newspapers and social media sites make information widely accessible.

Answer D

This option is incorrect. Both online newspapers and social media sites provide media-rich content at a low cost to the user.

Answer ([back](#))

Correct Answer: C

1.

The upgraded system uses a directory containing additional information not supplied by the customer. The directory is used to help direct calls effectively. Which of the following is LEAST likely to be included in the directory?

- (A) A list of common issues and whether each issue requires a human representative
- (B) A list of common keywords or phrases and a corresponding issue for each keyword or phrase
- (C) A list of computers the company owns and the computers' corresponding IP addresses
- (D) A list of human representatives and the corresponding department for each representative

Correct Answer

C

EXPLANATION

All the information provided in the flowchart of the upgraded system deals with understanding the customer's issue and getting them the help they need; the IP addresses of computers in the company (**choice C**) isn't related in any way to this purpose of the system or the "directory" and would not likely be included.

Answer ([back](#))

Correct Answer: B

2.

Of the following potential benefits, which is LEAST likely to be provided by the upgraded system?

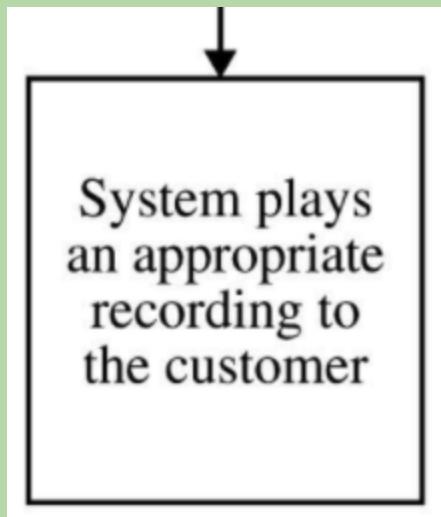
- (A) Human representatives will not be needed to respond to some inquiries.
- (B) The company will be able to provide a human representative for any incoming call.
- (C) Customers are likely to spend less time listening to information not relevant to their issue.
- (D) Customers will be unable to mistakenly select the incorrect department for their particular issue.

Correct Answer

B

EXPLANATION

According to the flowchart of the upgraded system, not all customers will receive a human representative, for example, some customers will receive a recording (shown below); therefore, choice B is the least likely benefit:



All of the other choices (A, C, and D), however, describe benefits to the company (A) or customer (C, D) that **are** viable outcomes of the upgraded system.

Answer ([back](#))

Correct Answer: A

3.

Which of the following is the most likely data privacy concern of the upgraded system?

- (A) Customers' personal information could be compromised if an unauthorized individual gains access to the call session database.
- (B) Storing information in the call session database makes it easy for individuals to trick the system using malicious links.
- (C) The system design increases the chance that customers will unknowingly install malware on their devices that will share their data with unauthorized individuals.
- (D) The system design makes it easy for unauthorized individuals to acquire customers' private encryption keys.

Correct Answer

A

EXPLANATION

Since this system is all about logging data related to customer calls, the most likely source of data or privacy concerns is with the customer's personal data that is included in the call database (**choice A**) -- all the other options don't really reflect data concerns related to this particular system (malicious links, malware, or encryption keys are not relevant in a call-center context).

Answer ([back](#))

Correct Answer: C

AP EXAM PRACTICE QUESTION

Which of the following best describes the relationship between the World Wide Web and the Internet?

X the correct answer choice:

	(A) The World Wide Web is a protocol that is accessed using a data stream called the Internet.
	(B) The World Wide Web is a system of linked pages, programs, and files that is accessed using a data stream called the Internet.
X	(C) The World Wide Web is a system of linked pages, programs, and files that is accessed via a network called the Internet. <i>Explanation:</i> The Internet is an interconnected network of networks, and the World Wide Web is an information system that is accessed via the Internet.
	(D) The World Wide Web is a Web site that is accessed using a protocol called the Internet.

Answer ([back](#))

Correct Answer: C

AP EXAM PRACTICE QUESTION

Which of the following is **not** an advantage of storing data using cloud computing?

	(A) The cloud is easy to scale and can support individual use as well as implementation by large companies.
	(B) Cloud computing has the potential to be environmentally friendly due to many users efficiently sharing large systems and resources.
X	<p>(C) Cloud computing offers improved security and privacy over storing data on a personal computer.</p> <p><i>Explanation:</i> This is not an advantage because it is not true! Storing your data on your <i>own</i> computer (and <i>not</i> online in the cloud) is the safest way to store data. When you upload your data to the cloud, you run the risk of having that data hacked or accessed by other users. While there are benefits to cloud computing, it does come with an increased risk to the security of your data.</p>
	(D) Storing data in the cloud can prevent loss of data due to a malfunction of the user's personal computer.

Answer ([back](#))

A. Which is faster bandwidth? 20 MB/sec or 100 MB/sec
(*MB = megabits per second, or 1 million bits per second*)

B. Which is a faster latency? 300 ms or 500 ms
(*ms = milliseconds*)

A. 100MB/sec is faster bandwidth.

This is because **bandwidth** is the maximum amount of data that can be sent in a fixed amount of time, so more bandwidth means more data can be received in any given second.

Higher bandwidth is better

B. 300 ms is a “faster” latency.

This is because **latency** is the time between the transmission and the receipt of a message, so *less* time means you get it *faster!*

Lower latency is better

Answer ([back](#))

Correct Answer is C

Practice AP Exam Question #1!

A user is trying to download an image from Creative Commons to use in their project. Which of the following best describes how the file is sent to the user?

- (A) The user's computer and the Creative Commons server connect directly and the image file is sent in its entirety, all at once.
- (B) The image file is broken into packets which are routed to the receiving computer in the correct order and reassembled to form the complete image file; any missing packets are substituted for packets already received.
- (C) The image file is broken into packets which are routed to the receiving computer, potentially out of order, and reassembled to form the complete image file; any missing packets are resent.**
- (D) It is not possible to download image files from websites.

Your answer (A, B, C, D):

C

Be sure to read the Vocab & Big Ideas section immediately above this question if you missed it!

Answer ([back](#))

Correct Answer is D

Practice AP Exam Question #2

Which of the following statements regarding the use of open protocols for communicating on the Internet is *false*?

- (A) Open protocols promote collaboration and cooperation between different people and groups.
- (B) Open protocols allow companies all over the world to build different types of devices that can connect to the internet and communicate with each other.
- (C) Open protocols have contributed to the fast growth of the internet and support its scalability.
- (D) Open protocols are developed and regulated by a few select companies around the world.**

Your answer (A, B, C, D):

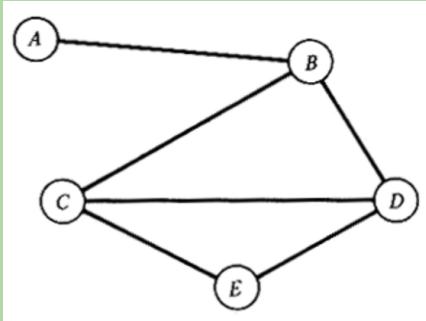
D

Explanation

Statement D is false because open protocols mean exactly that -- they are *open* for all companies and people to see and use, and not regulated by private companies.

Answer ([back](#))

Pretend this image represents a small computer network, and each node is a computer. The line indicates that the two computers can communicate directly with each other. When a node becomes **faulty**, then it can no longer send or receive data:



Node A is sending data and node E is receiving that data.

- a. Could E receive the data if node D became faulty?

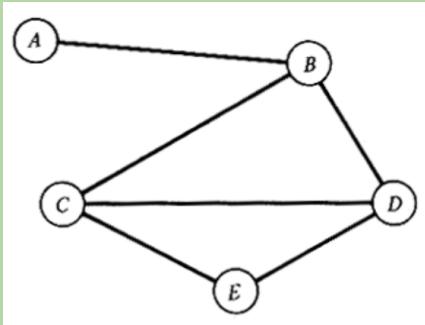
Yes, because data could travel via the path A-B-C-E

- b. Could E receive the data if node B became faulty?

No, because A would no longer have a connection to the network since it's only connected to B and no other nodes.

Answer ([back](#))

Look at this network again. We can say there is **redundant routing** between computers A and E because there is **more than one path** to get from A to E.



- a. Is there **redundant routing** between B and E? If so, list all possible pathways to get from B to E.

Yes! There is redundant routing from B to E since there is more than one pathway:

B-D-E
B-C-E
B-C-D-E
B-D-C-E

- b. How about from B to D? If so, list all pathways.

Yes again!

B-D
B-C-D
B-C-E-D

- c. Are there two nodes for which there is **not** redundant routing? If so, which two?

There is not redundant routing between **A and B**; just one possible path connects these two, so if that path breaks, they cannot communicate.

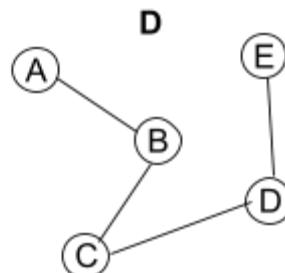
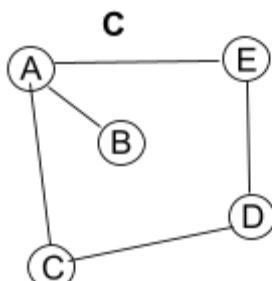
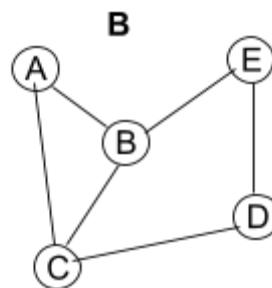
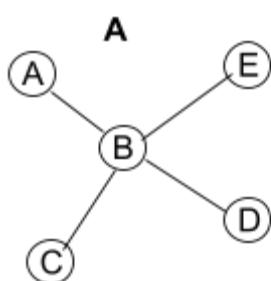
Answer ([back](#))

The TWO correct answers are A and D (you must have *both* to get the point!)

AP EXAM PRACTICE QUESTION

Which of the following networks do *not* have redundant routing between computers A and E?

Select two.

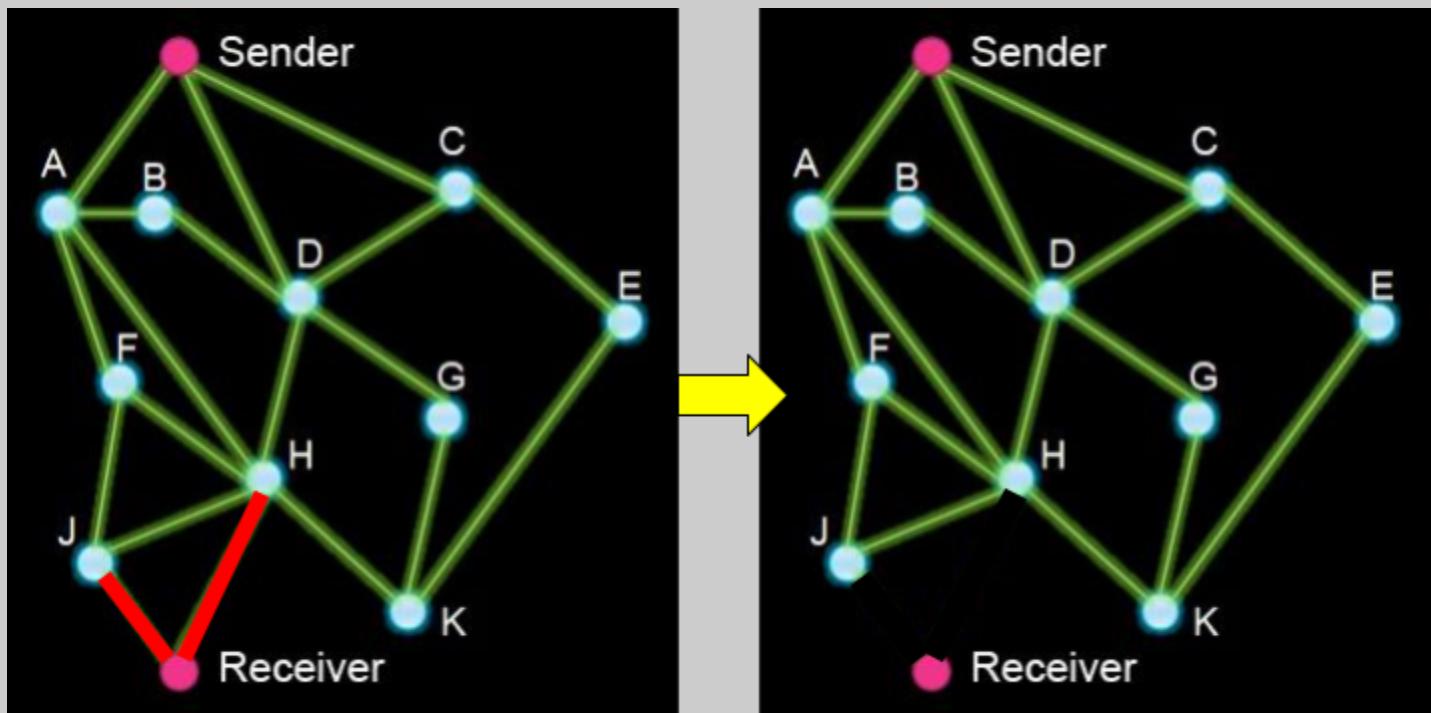


X the **TWO** correct answer choices:

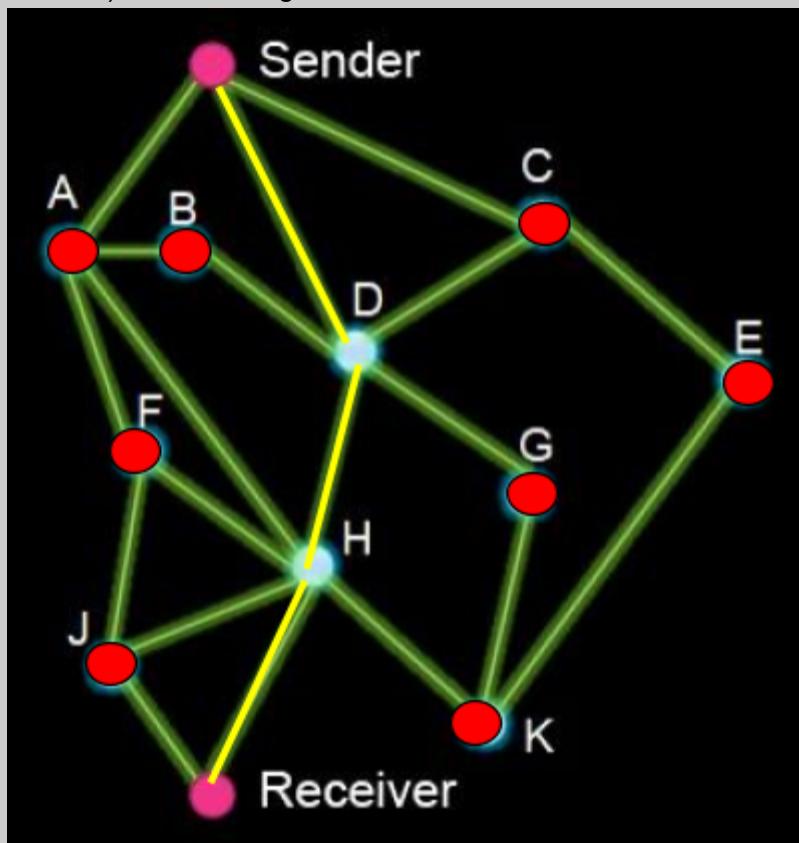
X	(A) There is not redundant routing between A and E because there is only one pathway between A and E: A-B-E If the connection between A and B fails, or the connection between B and E fails, there is not other way to get from A to E!
	(B)
	(C)
X	(D) Similar to A, there is not redundant routing between A and E because there is only one pathway between A and E: A-B-C-D-E If any one of those single connections fail (A-B, B-C, C-D, or D-E) fail, there is no other way to get from A to E.

Answer ([back](#))

- a. What is the *minimum* number of connections that need to be broken or removed before the sender and the receiver can't communicate? **A minimum of two would do it!**



- b. What is the *maximum* number of nodes that can fail and still let the sender and receiver communicate? Which nodes? **Eight!** (Another way to think about this is “what’s the path from sender to receiver with the *fewest number of nodes?*”) As long as nodes D and H stay active (as well as the sender and receiver), the other eight can fail and still allow for communication between sender and receiver:



Answer ([back](#))

Correct Answer: A

Which of the following best explains how data is typically assembled in packets for transmission over the Internet?

A

Each packet contains data to be transmitted, along with metadata containing information used for routing the data.

B

Each packet contains an encrypted version of the data to be transmitted, along with metadata containing the key needed to decrypt the data.

C

Each packet contains only the metadata used to establish a direct connection so that the data can be transmitted.

D

Each packet contains multiple data files bundled together, along with metadata describing how to categorize each data file.

Answer ([back](#))

Correct Answer: A

Which of the following statements best explains the ability of the network to provide fault tolerance?

A

The network is considered fault-tolerant because there are redundant paths between each pair of devices.

B

The network is considered fault-tolerant because it guarantees that no individual component will fail.

C

The network is not considered fault-tolerant because it relies on physical connections.

D

The network is not considered fault-tolerant because it provides more paths than are needed.

Explanations:

Answer A

Correct. One way to accomplish network redundancy is by having more than one path between any two connected devices. Redundancy within a network allows it to support failures and still continue to function.

Answer B

Incorrect. The network is considered fault-tolerant because it provides redundant routing. It cannot guarantee that components are foolproof.

Answer C

Incorrect. The network is considered fault-tolerant because it provides redundant routing. It does not matter whether the connections are physical or wireless.

Answer D

Incorrect. The network is considered fault-tolerant because it provides redundant routing. Redundancy often requires additional resources (in this case, more network connections).

Answer ([back](#))

Correct Answer: D

A local router is configured to limit the bandwidth of guest users connecting to the Internet. Which of the following best explains the result of this configuration as compared to a configuration in which the router does not limit the bandwidth?

- A The amount of time it takes guest users to send and receive large files is likely to decrease.
- B The number of packets required for guest users to send and receive data is likely to decrease.
- C Guest users will be prevented from having fault-tolerant routing on the Internet.
- D Guest users will be restricted in the maximum amount of data that they can send and receive per second.



Explanations:

Answer A

Incorrect. Limiting the bandwidth of a connection is likely to increase the amount of time it takes to send and receive files.

Answer B

Incorrect. The number of packets used to transmit data is related to the size of the data, not to the bandwidth of the connection.

Answer C

Incorrect. Internet routing is fault-tolerant, regardless of the bandwidth of a local connection.

Answer D

Correct. The bandwidth of a computer network is the maximum amount of data that can be sent in a fixed amount of time. With limited bandwidth, guest users will be restricted in the amount of data transmitted per second.

Answer ([back](#))

Correct Answer: B

Which of the following best explains how messages are typically transmitted over the Internet?

A

The message is broken into packets that are transmitted in a specified order. Each packet must be received in the order it was sent for the message to be correctly reassembled by the recipient's device.

B

The message is broken into packets. The packets can be received in any order and still be reassembled by the recipient's device.

C

The message is broken into two packets. One packet contains the data to be transmitted and the other packet contains metadata for routing the data to the recipient's device.

D

The message is transmitted as a single file and received in whole by the recipient's device.

Explanations:

Answer A

Incorrect. Messages are broken into packets, but they can be received in any order and still be reassembled.

Answer B

Correct. Messages are broken into packets. Each packet contains data to be transmitted, as well as metadata for routing and reassembling the data upon receipt. This allows the packets to be received in any order and still be reassembled correctly.

Answer C

Incorrect. Messages are broken into as many packets as are needed to transmit the data. Each packet contains both data and metadata.

Answer D

Incorrect. Messages are broken into packets, not transmitted in a single file.

Answer ([back](#))

Correct Answer: B

Which of the following best explains how the Internet is a fault-tolerant system?

A

The Internet is fault-tolerant because cybercriminals can conceal their actions, allowing them the ability to carry out faulty actions without leaving a trace.

B

The Internet is fault-tolerant because there are usually multiple paths between devices, allowing messages to sometimes be sent even when parts of the network fail.

C

The Internet is fault-tolerant because users can transmit messages using a variety of different protocols, allowing them to use devices from any manufacturer.

D

The Internet is fault-tolerant because users usually understand and accept the fact that servers sometimes fail, allowing network engineers to repair faulty devices as quickly as possible.

Explanations:

Answer A

Incorrect. The ability for cybercriminals to sometimes conceal their actions is not related to the fault tolerance of the Internet.

Answer B

Correct. The Internet is considered fault-tolerant because messages can often be transmitted even in the presence of network failures. This is achieved by using redundant routing, which means that there are usually multiple possible paths between devices.

Answer C

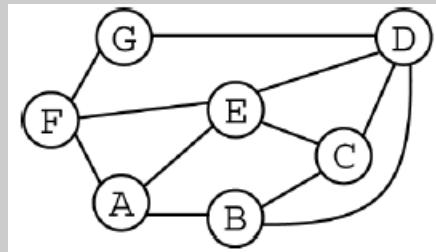
Incorrect. While a variety of communications protocols are used on the Internet, their use is not directly related to the fault tolerance of the Internet.

Answer D

Incorrect. The acceptance of faults from users does not make a system fault-tolerant.

Answer ([back](#))

Correct Answer: C



What is the minimum number of connections that must be broken or removed in the network before computer E can no longer communicate with computer F?

A 1

B 2

C 3 ✓

D 4

Explanations:

Answer A

This option is incorrect. If only one link were removed, for instance from F to E, a message from computer E could travel through other computers and connect with E through G or A.

Answer B

This option is incorrect. If only two links were removed, for instance from F to E and from F to A, a message from computer E could still reach computer F through the route E-D-G-F.

Answer C

This option is correct. Any line between two computers represents a way for them to communicate with each other, and a communication between two computers can go through other computers. If the links from F to G, from F to A, and from F to E were broken, it would not be possible for computers E and F to communicate.

Answer D

This option is incorrect. While removing four links could isolate computer F from computer E, it is not the minimum number required to accomplish this.

Answer ([back](#))

Correct Answer: A

Which of the following is a primary benefit of making a computing system fault-tolerant?

A

If one component of the system fails, users of the system can often still access it.

B

If one component of the system is hacked, no information will be stolen.

C

If the system becomes too expensive, making it fault-tolerant will save money.

D

If the system cannot operate efficiently, making it fault-tolerant will speed up its operation.

Explanations:

Answer A

Correct. When a computer system can support failures and still continue to function, it is called fault-tolerant.

Answer B

Incorrect. Making a computer system fault-tolerant often increases pathways between devices and components, which can increase the possibility of a successful hacking attempt.

Answer C

Incorrect. Making a computer system fault-tolerant often requires additional resources, which can increase expenses.

Answer D

Incorrect. Making a computer system fault-tolerant increases reliability but may not necessarily increase efficiency.

Answer ([back](#))

Correct Answer: D

Which of the following is a primary reason for the use of open protocols on the Internet?

- A Open protocols allow devices to specify how data packets are to be routed on the Internet in advance.
- B Open protocols ensure that all data transmission on the Internet is kept secure.
- C Open protocols ensure that all Internet users are provided connections with equal bandwidth.
- D Open protocols provide a way to standardize data transmission between different devices.

Explanations:

Answer A

Incorrect. Routing on the Internet is usually dynamic; it is not specified in advance.

Answer B

Incorrect. The Internet was not designed to be completely secure. The protocols used on the Internet do not ensure that all communications are secure.

Answer C

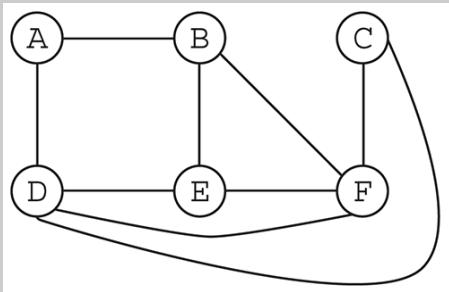
Incorrect. Protocols are unable to ensure that all Internet connections have the same bandwidth.

Answer D

Correct. Protocols are agreed-upon sets of rules that specify the behavior of a system. Protocols used on the Internet enable devices from different manufacturers to communicate in a standard way.

Answer ([back](#))

Correct Answers: A and C (must have both correct for credit!)



Which of the following statements are true about the ability for devices A and C to communicate?

Select two answers.

A

If devices B and D were to fail, then information sent from device A could not reach device C.

B

If devices B and F were to fail, then information sent from device A could not reach device C.

C

If devices D and F were to fail, then information sent from device A could not reach device C.

D

If devices E and F were to fail, then information sent from device A could not reach device C.

Explanations:

Answer A

Correct. If devices B and D were to fail, then device A would be isolated from the rest of the network, preventing it from communicating with device C.

Answer B

Incorrect. If devices B and F were to fail, devices A and C can still communicate. One possible path is A-D-C.

Answer C

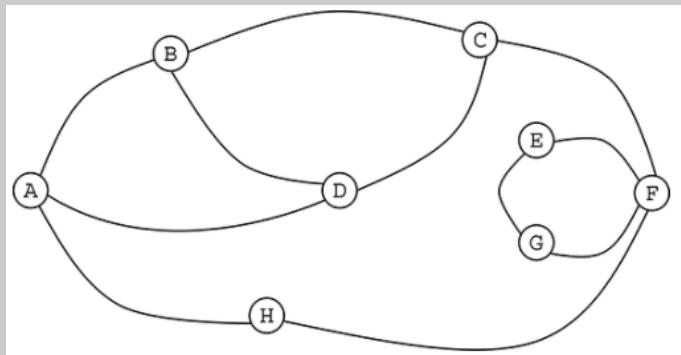
Correct. If devices D and F were to fail, then device C would be isolated from the rest of the network, preventing it from communicating with device A.

Answer D

Incorrect. If devices E and F were to fail, devices A and C can still communicate. One possible path is A-D-C.

Answer ([back](#))

Correct Answer: A



What is the minimum number of connections that would need to be removed from the network in order for device A to not be able to communicate with device F?

A 2



B 3

C 4

D 5

Explanations:

Answer A

Correct. Removing the connections between C and F and between F and H will prevent devices A and F from communicating.

Answer B

Incorrect. Removing three connections could prevent devices A and F from communicating, but it can also be done by removing only two connections.

Answer C

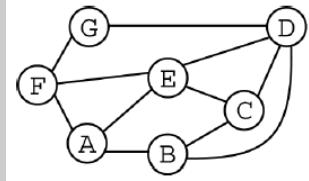
Incorrect. Removing four connections could prevent devices A and F from communicating, but it can also be done by removing only two connections.

Answer D

Incorrect. Removing five connections could prevent devices A and F from communicating, but it can also be done by removing only two connections.

Answer ([back](#))

Correct Answer: B



Which of the following statements about security in the network is true?

- I. Computers A and D need to communicate with at least two additional computers in the network in order to communicate with each other.
- II. Computers B and C can communicate with each other without additional computers being aware of the communication.

A I only

B II only

C I and II

D Neither I nor II

Explanations:

Answer A

This option is incorrect. Statement I is false because computers A and D can communicate with each other through one computer, E.

Answer B

This option is correct. Statement I is false because computers A and D can communicate with each other through one computer, E. Statement II is true because there is a direct link between computers B and C.

Answer C

This option is incorrect. While Statement II is true, Statement I is false because computers A and D can communicate with each other through one computer, E.

Answer D

This option is incorrect. While Statement I is false, Statement II is true because there is a direct link between computers B and C.

Answer ([back](#))

Correct Answer: D

Two computers are built by different manufacturers. One is running a Web server and the other is running a Web browser. Which of the following best describes the ability of the two computers to communicate with each other across the Internet?

A

The computers cannot communicate because different manufacturers use different communication protocols.

B

The computers can communicate, but additional hardware is needed to convert data packets from one computer's protocol to the other computer's protocol.

C

The computers can communicate directly only if the messages consist of text; other formats cannot be interpreted across computers.

D

The computers can communicate directly because Internet communication uses standard protocols.



Explanations:

Answer A

This option is incorrect. The protocols of the Internet, including HTTP, allow any computers that run that protocol to communicate with each other over the Internet.

Answer B

This option is incorrect. The protocols of the Internet, including TCP/IP, allow any computers that run that protocol to send data back and forth to each other. Protocols such as TCP/IP are implemented through software, not hardware, and additional hardware is not required.

Answer C

This option is incorrect. All data on a computer is stored in binary. Individual computers can interpret different file formats if each computer contains the appropriate software. The structure and functionality of the Internet does not affect the ability of two computers to share files.

Answer D

This option is correct. Devices on the Internet communicate using standard protocols, which do not depend on the manufacturer.