Encryption

Milestone 3 – CSCI 435 – Spring 2025

*Please be sure that you complete all pages of this worksheet. Some sections may begin on new pages, so you may need to scroll past any blank space.*

*As you work through the reading material, fill in the answers to the following questions inside the provided boxes (1x1 tables). You do* ***not*** *need to write complete sentences for questions that ask for a short answer. Paragraph or bullet form is acceptable for questions that require an explanation or description.*

1. The group of Chinese hackers that has compromised American telecommunications companies is known by what two-word moniker?

|  |
| --- |
|  |

2. True or False? The United States Cybersecurity and Infrastructure Security Agency recommends that **all** Americans encrypt their communications.

|  |
| --- |
|  |

3. In the context of encryption, what word do we use for unencrypted data (either prior to encryption or after decryption)?

|  |
| --- |
|  |

4. What word do we use for the encrypted data produced by an encryption algorithm?

|  |
| --- |
|  |

5. What do we call the piece of data that an encryption algorithm uses to convert between unencrypted and encrypted formats?

|  |
| --- |
|  |

6. In the context of encryption, someone that tries to access a copy of the unencrypted data without authorization is called what?

|  |
| --- |
|  |

7. What do we call the technique of encrypting data before sending it through a communications system in such a way that it is only decrypted after it is received by the intended recipient?

|  |
| --- |
|  |

8. Suppose that a Windows computer uses BitLocker for full disk encryption. The system’s one persistent storage device is a solid state drive that supports native hardware encryption. How can BitLocker be easily defeated to allow access to an unencrypted copy of the data?

|  |
| --- |
|  |

9. How high a performance penalty can we expect when running full-disk LUKS encryption on an NVMe solid state drive?

|  |
| --- |
|  |

10. What three-word term describes the use of encryption to protect the confidentiality of data stored on a computer while the computer is turned off?

|  |
| --- |
|  |

11. What two-word term refers to a computer system that does not communicate with any other computer system?

|  |
| --- |
|  |

12. What three-word term describes the process of encrypting data before it is sent to another computer, which then immediately decrypts it for use?

|  |
| --- |
|  |

13. What kind of encryption is in use if data are encrypted and decrypted using the same shared key?

|  |
| --- |
|  |

14. True or False? A symmetric encryption key can be safely sent in plaintext at the start of a message containing ciphertext encrypted with that key?

|  |
| --- |
|  |

15. What kind of cyberattack occurs when confidential information is intercepted when it is communicated on a second network link or alternate communications channel?

|  |
| --- |
|  |

16. What kind of encryption system allows two people to exchange encrypted messages without having to share a single secret key?

|  |
| --- |
|  |

17. Which key needs to be kept confidential: public or private?

|  |
| --- |
|  |

18. Suppose Alice uses her private key to encrypt a message to Bob’s public key. Which key does Bob need in order to decrypt Alice’s message?

|  |
| --- |
|  |

19. What kind of file provides the public key for a certificate authority?

|  |
| --- |
|  |

20. The X.509 standard defines the system known by what three-word term (or acronym)?

|  |
| --- |
|  |

21. In contrast to X.509, what three-word term refers to the decentralized system of public key trust that PGP uses?

|  |
| --- |
|  |

22. What is the term for using physical violence or legal compulsion (such as imprisonment) to force a person to reveal their encryption key?

|  |
| --- |
|  |

23. What kind of cyberattack can be used to trick someone into revealing their encryption key by pretending to have a legitimate need to access the encrypted message?

|  |
| --- |
|  |

24. What two-word term means that a third party keeps a copy of an encryption key that is used to the secure the communications of two (or more) other parties?

|  |
| --- |
|  |

25. If an encryption key is relatively weak, what technique can be used to try to guess the key and decrypt the data?

|  |
| --- |
|  |

26. The encryption passphrase “correct horse battery staple” is especially vulnerable to what kind of attack, since it consists only of English words?

|  |
| --- |
|  |

27. In which encryption standard originally developed by IBM did the NSA plausibly leave themselves a back door?

|  |
| --- |
|  |

28. What phenomenon causes qubits in a state of superposition to change in a predictable way if the state of one qubit in the group is changed?

|  |
| --- |
|  |

29. Cryptographic algorithms designed to resist quantum attacks are part of a set known by what two word term?

|  |
| --- |
|  |

30. What cyberattack refers to the collection of ciphertext from encrypted communications with the hope of one day being able to decrypt it with more advanced techniques?

|  |
| --- |
|  |

31. In addition to overturning *Roe v. Wade*, the *Dobbs v. Jackson Women’s Health Organization* decision of the United States Supreme Court also asserted that Americans have no federal constitutional right to \_\_\_\_\_\_\_.

|  |
| --- |
|  |

32. Which amendment to the U.S. Constitution guarantees the right of a person not to testify against himself or herself in any criminal matter?

|  |
| --- |
|  |

33. Which 1951 Supreme Court case ruled that answers to questions that “would furnish a link in the chain of evidence needed to prosecute” someone are testimonial in nature?

|  |
| --- |
|  |

34. Which 2000 Supreme Court case ruled that the government must know in advance both that a piece of evidence exists and where that evidence is located before it can compel production?

|  |
| --- |
|  |

35. In a 2009 court case, what individual was compelled to produce evidence from an encrypted hard drive under the “foregone conclusion” doctrine, since he had already shown the illegal contents of his hard drive to an ICE agent?

|  |
| --- |
|  |

36. What did the court do to a subpoena directed at Thomas Kirchner, after it determined that the government agency that issued the subpoena didn’t know whether the evidence sought even existed?

|  |
| --- |
|  |

37. True or False? The *United States v. Fricosu* case declared that the government can compel a person to provide an unencrypted copy of encrypted data if they merely suspect the encryption is hiding evidence of a crime.

|  |
| --- |
|  |

38. Which disk encryption product was used by the anonymous John Doe who spent several months in jail for contempt of court before being freed in 2011?

|  |
| --- |
|  |

39. Suppose the government successfully wins a child abuse case before the Supreme Court in which they are able to compel a person to decrypt their hard drive despite not knowing what, if any, evidence of the crime is present on the disk. What legal principle (two Latin words) would then allow the government to force a person to decrypt their cell phone so that the police could search for evidence of speeding?

|  |
| --- |
|  |

40. True or False? Many Americans today use their cell phone as an extension of their own mind.

|  |
| --- |
|  |

41. What term refers to hiding information in plain sight by concealing it inside some otherwise unremarkable object or file? (Be sure your spellchecker doesn’t autocorrect your answer to the wrong word!)

|  |
| --- |
|  |

42. *The Hitchhiker’s Guide to the Galaxy* has what two words printed in large, friendly letters on the cover?

|  |
| --- |
|  |

43. The secret data when using digital steganography is called the \_\_\_\_\_\_\_\_\_.

|  |
| --- |
|  |

44. The unremarkable outer file used in digital steganography is called the \_\_\_\_\_\_\_\_\_.

|  |
| --- |
|  |

45. What two-word term refers to an FBI pipe dream in which only the “good guys” get access to encrypted communications between Americans?

|  |
| --- |
|  |

46. Which foreign political party is now able to monitor Americans’ day-to-day communications (among other things) thanks to the FBI and other government agencies weakening communications security to make investigations easier?

|  |
| --- |
|  |

47. True or False? Text messages are securely encrypted.

|  |
| --- |
|  |

48. An email is the digital equivalent of what type of snail mail?

|  |
| --- |
|  |

49. Which popular commercial messaging service, which you probably really need to stop using, is highly insecure and privacy-invasive despite claiming its messages can self-destruct?

|  |
| --- |
|  |

50. True or False? Discord is a secure messaging platform that properly implements E2EE.

|  |
| --- |
|  |

51. True or False? WhatsApp properly implements E2EE, so not even the FBI can access your messages on the platform.

|  |
| --- |
|  |

52. True or False? You can safely send messages to other iPhone users, without risk of interception, as long as you use Apple’s iMessage.

|  |
| --- |
|  |

53. True or False? You can encrypt the contents of your email messages even if you don’t use an encrypted email service.

|  |
| --- |
|  |

54. You should steer clear of any service that has what kind of marketing program?

|  |
| --- |
|  |

55. True or False? Decentralized communications services are probably safer in the long run for privacy than are services controlled by a single company.

|  |
| --- |
|  |

56. Which “open source” communications application/service mentioned in the readings denies access to its servers to third-party rebuilds of its open source code?

|  |
| --- |
|  |

57. Increasing what two-word term is the reason why service providers often require relatively complex passwords?

|  |
| --- |
|  |

58. On how many different websites is it acceptable from a security perspective to use the same password?

|  |
| --- |
|  |

59. True or False? The use of one-time passwords delivered via text message or email is a secure alternative to requiring users to have a permanent password for a website.

|  |
| --- |
|  |

60. What is one of the terms used to describe an authentication scheme that works on the principle of combing something the user knows with something the user has?

|  |
| --- |
|  |

61. Suppose a website that isn’t owned by Google offers to let you log in with your Google username and password instead of creating a new username and password for that site. Should you use your Google account to log in?

|  |
| --- |
|  |

62. What piece of software (two-word term for the general category, not a specific example) should you use instead of trying to remember passwords for all the different sites and services that you use?

|  |
| --- |
|  |

63. Which cloud-based password manager was compromised at least twice starting in 2022?

|  |
| --- |
|  |

64. True or False? It’s a good idea to store your passwords in your web browser.

|  |
| --- |
|  |

65. What do you need if you use a local password manager to store your passwords in a file on your computer? (Hint: Without these, you might have a bad day if your hard drive crashes.)

|  |
| --- |
|  |

# Submission

*When you have completed this worksheet, export it to PDF format. Upload the PDF file as your Moodle submission for this milestone.*