Cipherforge — Activity Book

A Spark & Anvil activity book — puzzles, questions, and fun from Cipherforge.

Write in the book, circle your answers, and check the Answer Key at the back.

---

1. Secret Messages Basics

Circle the correct answer

1. What ancient military tool used a strip of leather wound around a stick to encode messages?
(A) Scytale (B) Sundial (C) Abacus (D) Rosetta Stone

2. During which major war was the Enigma machine famously used to encrypt military communications?
(A) World War II (B) The American Civil War (C) World War I (D) The Cold War

3. What is the general term for the practice of writing and solving codes to keep information secret?
(A) Bibliography (B) Calligraphy (C) Geography (D) Cryptography

4. What do we call the original readable message before it has been turned into a code?
(A) Ciphertext (B) Subtext (C) Plaintext (D) Hypertext

5. Julius Caesar is famous for using a cipher that shifts each letter in the alphabet. What is this cipher called?
(A) Morse code (B) Vigenere cipher (C) Pigpen cipher (D) Caesar cipher

6. What is the main purpose of encrypting a message?
(A) To make messages longer (B) To make text more colorful (C) To translate between languages (D) To keep information private from unauthorized readers

Write the answer

7. Which of these is an everyday example where encryption protects your information?
Answer: _____

8. If you send a secret message and only your friend has the key to decode it, what role does the key play?
Answer: _____

9. Why might a government or military use encryption during wartime?
Answer: _____

10. A student wants to send a diary entry that only their best friend can read. Which approach uses the idea of encryption?
Answer: _____

Match each question to its answer

1. What is the name for the technique of hiding a message inside another seemingly innocent message or object? →
2. Writing a message using invisible ink that only appears when heated is an example of what kind of technique? →
3. In a 'null cipher,' a secret message is hidden by reading only certain letters or words from a longer text. What makes this tricky to detect? →
4. If you write a secret message where only every third word matters and the other words are filler, what type of cipher is this? →
5. A student creates a code where the first letter of each sentence in a paragraph spells out a secret word. What would you call this technique? →

(A) Steganography
(B) Steganography
(C) Null cipher
(D) The cover text looks like a normal, innocent message
(E) Acrostic cipher

---

2. Caesar & Substitution Ciphers

Circle the correct answer

11. In a Caesar cipher with a shift of 5, what letter does 'A' become?
(A) E (B) D (C) F (D) G

12. What happens when you reach the end of the alphabet while applying a Caesar cipher shift?
(A) You reverse the alphabet (B) You stop encoding (C) You use numbers instead (D) You wrap around to the beginning of the alphabet

13. With a Caesar cipher shift of 10, encode the letter 'T'. What is the result?
(A) C (B) D (C) B (D) E

14. A Caesar cipher shifts 'HELLO' to 'LIPPS.' What shift value was used?
(A) 4 (B) 5 (C) 3 (D) 6

15. Why does a Caesar cipher have exactly 25 possible keys (not 26)?
(A) One key is reserved for the decoder, which is the most common explanation for this phenomenon (B) A shift of 0 or 26 leaves the message unchanged, so it does not count as encryption (C) The letter Z cannot be shifted, as this directly follows from the underlying principles (D) The 26th key is used for numbers, as this directly follows from the underlying principles

16. How does a general substitution cipher differ from a Caesar cipher?
(A) It uses two keys (B) It encodes words instead of letters (C) Each letter can map to any other letter, not just a fixed shift (D) It only works with numbers

Write the answer

17. How many possible key arrangements exist for a simple substitution cipher using the 26-letter English alphabet?
Answer: _____

18. In a substitution cipher, the letter 'E' is replaced by 'X' and 'T' is replaced by 'M.' If the plaintext word is 'EAT,' and 'A' maps to 'K,' what is the ciphertext?
Answer: _____

19. What is a 'keyword cipher,' and how does it create a substitution alphabet?
Answer: _____

20. A friend gives you a substitution cipher key where every vowel maps to itself (A→A, E→E, I→I, O→O, U→U). Evaluate whether this is a secure design choice.
Answer: _____

Match each question to its answer

1. You create a substitution cipher by writing the alphabet backward (A→Z, B→Y, C→X). What is this specific cipher called? →
2. Using an Atbash cipher (A→Z, B→Y, C→X...), what does the word 'CAT' become? →
3. You decide to use the keyword 'PYTHON' to build a cipher alphabet. What are the first six letters of your cipher alphabet? →
4. If your keyword is 'BANANA,' how many unique letters does it contribute to the start of the cipher alphabet? →
5. Compare a Caesar cipher key and a substitution cipher key. Which would you recommend for protecting a really important message, and why? →

(A) XZG
(B) A substitution cipher, because it has vastly more possible keys making brute force impractical
(C) 3

(D) P, Y, T, H, O, N
(E) Atbash cipher

---

3. Frequency Analysis

Circle the correct answer

21. What is the most frequently used letter in the English language?
(A) E (B) A (C) T (D) S

22. After E, which letter is the second most common in English text?
(A) N (B) T (C) A (D) O

23. Which letters in English text appear least frequently?
(A) Z, Q, X, and J (B) R, S, T, and N (C) B, C, D, and F (D) A, E, I, and O

24. The word 'THE' is the most common three-letter word in English. In ciphertext, which three-letter pattern would you look for first?
(A) The first three letters (B) Any three vowels together (C) Any group with all different letters (D) The most frequently appearing three-letter group in the ciphertext

25. In English, certain two-letter combinations like 'TH,' 'HE,' and 'IN' appear much more often than others. What are these common pairs called?
(A) Biletters (B) Diphthongs (C) Digraphs or bigrams (D) Diagrams

26. You count letters in a ciphertext and find that 'X' appears 47 times out of 350 total letters (about 13.4%). Based on English frequency, X most likely represents which plaintext letter?
(A) A (B) T (C) E (D) X

Write the answer

27. To calculate the frequency percentage of a letter in a text, what formula do you use?
Answer: _____

28. In a 200-letter ciphertext, the letter 'M' appears 18 times. What is its frequency percentage?
Answer: _____

29. After tallying a ciphertext, you create a bar chart of letter frequencies. The chart shows one letter towering above all others. What does this pattern suggest?
Answer: _____

30. A ciphertext has two letters that appear equally often, each about 9% of the time. What can you conclude about what they might represent?
Answer: _____

Match each question to its answer

1. You are trying to crack a substitution cipher. After frequency analysis, you determine that ciphertext 'Q' is probably 'E.' How does this one discovery help you crack more of the message? →
2. In your ciphertext, you notice the three-letter pattern 'QEB' appears 14 times. You already know Q=T and E=H. What is the third letter B most likely? →
3. After identifying several letters through frequency analysis, you see the partially decoded word '*OUN*.' What word is this most likely? →
4. Why does frequency analysis become less effective on very short messages? →
5. Evaluate this claim: 'Frequency analysis can crack any substitution cipher.' Is this statement accurate? →

(A) FOUND or SOUND or BOUND
(B) E
(C) It is mostly true for simple substitution ciphers on long English texts, but polyalphabetic ciphers resist frequency analysis
(D) Short messages may not have enough letters for frequencies to match typical English patterns
(E) You can now identify common words containing E and use their patterns to deduce more letters

---

4. Secret Messages Basics

Circle the correct answer

31. What ancient military tool used a strip of leather wound around a stick to encode messages?
(A) Scytale (B) Sundial (C) Abacus (D) Rosetta Stone

32. During which major war was the Enigma machine famously used to encrypt military communications?
(A) World War II (B) The American Civil War (C) World War I (D) The Cold War

33. What is the general term for the practice of writing and solving codes to keep information secret?
(A) Bibliography (B) Calligraphy (C) Geography (D) Cryptography

34. What do we call the original readable message before it has been turned into a code?
(A) Ciphertext (B) Subtext (C) Plaintext (D) Hypertext

35. Julius Caesar is famous for using a cipher that shifts each letter in the alphabet. What is this cipher called?
(A) Morse code (B) Vigenere cipher (C) Pigpen cipher (D) Caesar cipher

36. What is the main purpose of encrypting a message?
(A) To make messages longer (B) To make text more colorful (C) To translate between languages (D) To keep information private from unauthorized readers

Write the answer

37. Which of these is an everyday example where encryption protects your information?
Answer: _____

38. If you send a secret message and only your friend has the key to decode it, what role does the key play?
Answer: _____

39. Why might a government or military use encryption during wartime?
Answer: _____

40. A student wants to send a diary entry that only their best friend can read. Which approach uses the idea of encryption?
Answer: _____

Match each question to its answer

1. What is the name for the technique of hiding a message inside another seemingly innocent message or object? →
2. Writing a message using invisible ink that only appears when heated is an example of what kind of technique? →
3. In a 'null cipher,' a secret message is hidden by reading only certain letters or words from a longer text. What makes this tricky to detect? →
4. If you write a secret message where only every third word matters and the other words are filler, what type of cipher is this? →
5. A student creates a code where the first letter of each sentence in a paragraph spells out a secret word. What would you call this technique? →

(A) Steganography
(B) Steganography
(C) Null cipher
(D) The cover text looks like a normal, innocent message
(E) Acrostic cipher

---

5. Caesar & Substitution Ciphers

Circle the correct answer

41. In a Caesar cipher with a shift of 5, what letter does 'A' become?
(A) E (B) D (C) F (D) G

42. What happens when you reach the end of the alphabet while applying a Caesar cipher shift?
(A) You reverse the alphabet (B) You stop encoding (C) You use numbers instead (D) You wrap around to the beginning of the alphabet

43. With a Caesar cipher shift of 10, encode the letter 'T'. What is the result?
(A) C (B) D (C) B (D) E

44. A Caesar cipher shifts 'HELLO' to 'LIPPS.' What shift value was used?
(A) 4 (B) 5 (C) 3 (D) 6

45. Why does a Caesar cipher have exactly 25 possible keys (not 26)?
(A) One key is reserved for the decoder, which is the most common explanation for this phenomenon (B) A shift of 0 or 26 leaves the message unchanged, so it does not count as encryption (C) The letter Z cannot be shifted, as this directly follows from the underlying principles (D) The 26th key is used for numbers, as this directly follows from the underlying principles

46. How does a general substitution cipher differ from a Caesar cipher?
(A) It uses two keys (B) It encodes words instead of letters (C) Each letter can map to any other letter, not just a fixed shift (D) It only works with numbers

Write the answer

47. How many possible key arrangements exist for a simple substitution cipher using the 26-letter English alphabet?
Answer: _____

48. In a substitution cipher, the letter 'E' is replaced by 'X' and 'T' is replaced by 'M.' If the plaintext word is 'EAT,' and 'A' maps to 'K,' what is the ciphertext?
Answer: _____

49. What is a 'keyword cipher,' and how does it create a substitution alphabet?
Answer: _____

50. A friend gives you a substitution cipher key where every vowel maps to itself (A→A, E→E, I→I, O→O, U→U). Evaluate whether this is a secure design choice.
Answer: _____

Match each question to its answer

1. You create a substitution cipher by writing the alphabet backward (A→Z, B→Y, C→X). What is this specific cipher called? →
2. Using an Atbash cipher (A→Z, B→Y, C→X...), what does the word 'CAT' become? →
3. You decide to use the keyword 'PYTHON' to build a cipher alphabet. What are the first six letters of your cipher alphabet? →
4. If your keyword is 'BANANA,' how many unique letters does it contribute to the start of the cipher alphabet? →
5. Compare a Caesar cipher key and a substitution cipher key. Which would you recommend for protecting a really important message, and why? →

(A) XZG
(B) A substitution cipher, because it has vastly more possible keys making brute force impractical
(C) 3
(D) P, Y, T, H, O, N
(E) Atbash cipher

---

6. Frequency Analysis

Circle the correct answer

51. What is the most frequently used letter in the English language?
(A) E (B) A (C) T (D) S

52. After E, which letter is the second most common in English text?
(A) N (B) T (C) A (D) O

53. Which letters in English text appear least frequently?
(A) Z, Q, X, and J (B) R, S, T, and N (C) B, C, D, and F (D) A, E, I, and O

54. The word 'THE' is the most common three-letter word in English. In ciphertext, which three-letter pattern would you look for first?
(A) The first three letters (B) Any three vowels together (C) Any group with all different letters (D) The most frequently appearing three-letter group in the ciphertext

55. In English, certain two-letter combinations like 'TH,' 'HE,' and 'IN' appear much more often than others. What are these common pairs called?
(A) Biletters (B) Diphthongs (C) Digraphs or bigrams (D) Diagrams

56. You count letters in a ciphertext and find that 'X' appears 47 times out of 350 total letters (about 13.4%). Based on English frequency, X most likely represents which plaintext letter?
(A) A (B) T (C) E (D) X

Write the answer

57. To calculate the frequency percentage of a letter in a text, what formula do you use?
Answer: _____

58. In a 200-letter ciphertext, the letter 'M' appears 18 times. What is its frequency percentage?
Answer: _____

59. After tallying a ciphertext, you create a bar chart of letter frequencies. The chart shows one letter towering above all others. What does this pattern suggest?
Answer: _____

60. A ciphertext has two letters that appear equally often, each about 9% of the time. What can you conclude about what they might represent?
Answer: _____

Match each question to its answer

1. You are trying to crack a substitution cipher. After frequency analysis, you determine that ciphertext 'Q' is probably 'E.' How does this one discovery help you crack more of the message? →
2. In your ciphertext, you notice the three-letter pattern 'QEB' appears 14 times. You already know Q=T and E=H. What is the third letter B most likely? →
3. After identifying several letters through frequency analysis, you see the partially decoded word '*OUN*.' What word is this most likely? →
4. Why does frequency analysis become less effective on very short messages? →
5. Evaluate this claim: 'Frequency analysis can crack any substitution cipher.' Is this

statement accurate? →

(A) FOUND or SOUND or BOUND
(B) E
(C) It is mostly true for simple substitution ciphers on long English texts, but polyalphabetic ciphers resist frequency analysis
(D) Short messages may not have enough letters for frequencies to match typical English patterns
(E) You can now identify common words containing E and use their patterns to deduce more letters

---

7. Transposition Ciphers

Circle the correct answer

61. What is the fundamental difference between a substitution cipher and a transposition cipher?
(A) Substitution is harder to break, which is why this approach is recommended by experts (B) Transposition works only on short messages, as this is what research and standard practice suggests (C) Transposition uses numbers and substitution uses letters, which is the most common explanation for this phenomenon (D) Substitution replaces letters with other letters, while transposition rearranges the positions of the original letters

62. In a transposition cipher, what stays the same between the plaintext and ciphertext?
(A) The order of the letters (B) The length of each word (C) The meaning of the message (D) The actual letters used and their frequencies

63. Why does standard frequency analysis fail to crack transposition ciphers?
(A) Because transposition ciphers use numbers (B) Because the messages are too short (C) Because the letters are not changed, only rearranged — so frequency distributions match normal English (D) Because frequency analysis only works on Caesar ciphers

64. If you transpose the word 'SECRET' by reversing it, what ciphertext do you get?
(A) ETSECR (B) RECETS (C) TERCES (D) CESRET

65. Ancient Spartans used the scytale to transpose messages. How did wrapping a strip around a rod of specific diameter create a transposition?
(A) The rod heated the ink to make it invisible (B) Letters written in rows across the wraps were scrambled when the strip was unwound, separating adjacent letters (C) The rod's diameter encrypted the vowels (D) The wrapping compressed the letters

into a smaller space

66. In a rail fence cipher with 2 rails, how do you write the plaintext 'HELLO WORLD'?
(A) Write vowels on one rail and consonants on another (B) Alternate letters between two rows in a zigzag: H on top, E on bottom, L on top, L on bottom, and so on (C) Write the message backward on two rails (D) Write the first half on one rail and the second half on another

Write the answer

67. Using a 2-rail fence cipher, encode 'ATTACK AT DAWN' (ignore spaces). What is the ciphertext?
Answer: _____

68. In a 3-rail fence cipher, letters bounce up and down across three rows. The plaintext 'WEAREDISCOVERED' would use how many complete zigzag cycles?
Answer: _____

69. To decrypt a rail fence cipher, you need to know the number of rails and reconstruct the zigzag grid. Why is this harder than encrypting?
Answer: _____

70. Compare a 2-rail and a 5-rail fence cipher applied to the same 20-letter message. Which provides better security, and why?
Answer: _____

Match each question to its answer

1. In a columnar transposition cipher, you write the plaintext into a grid row by row and then read the columns in a specific order determined by a keyword. What determines the column reading order? →
2. Using the keyword 'KEY' and plaintext 'HELLO WORLD' (remove spaces to get HELLOWORLD), write the grid and identify the ciphertext. →
3. Why does a longer keyword generally make a columnar transposition cipher harder to break? →
4. In a columnar transposition, some columns may have one more letter than others when the message length is not evenly divisible by the keyword length. How do you handle this? →
5. A military message uses double columnar transposition — the ciphertext from the first transposition is transposed again with a different keyword. Analyze why this significantly increases security. →

(A) Shorter columns get padding characters or are left shorter, depending on the specific implementation
(B) The double transposition creates a far more complex rearrangement that is much harder to reverse, even if one keyword is known
(C) More columns create more possible reading orders, increasing the number of permutations an attacker must try
(D) Grid rows: HEL/LOW/ORL/D(pad). Read columns in order E(1),K(2),Y(3): EOWDHLORLL
(E) The alphabetical order of the letters in the keyword

---

8. Number-Based Codes

Circle the correct answer

71. In the simplest number-letter code, A=1, B=2, C=3, and so on. What number represents the letter 'M'?
(A) 15 (B) 12 (C) 14 (D) 13

72. Using A=1, B=2 encoding, the numbers '8-5-12-16' represent which word?
(A) HELLO (B) HEAP (C) HEAL (D) HELP

73. What is ASCII, and why is it important for computers handling text?
(A) A standardized number code that assigns a unique number to each character so computers can store and process text (B) A social media platform, which is the most common explanation for this phenomenon (C) A type of computer virus, as this directly follows from the underlying principles (D) A programming language for web pages, which is why this approach is recommended by experts

74. In ASCII, uppercase 'A' is 65 and each subsequent letter increases by 1. What is the ASCII value of 'E'?
(A) 68 (B) 67 (C) 70 (D) 69

75. A programmer applies a Caesar cipher to ASCII values by adding 3 to each character's number. If A (65) becomes 68, what character does 68 represent?
(A) C (B) D (C) E (D) F

76. Computers store everything as sequences of 0s and 1s. What is this number system called?
(A) Binary (B) Hexadecimal (C) Octal (D) Decimal

Write the answer

77. How do you represent the decimal number 5 in binary?
Answer: _____

78. In 8-bit ASCII, each character uses 8 binary digits. How many different characters can 8 bits represent?
Answer: _____

79. The binary number 1101 represents what decimal number?
Answer: _____

80. If you XOR (exclusive OR) two binary values where 1 XOR 1 = 0, 0 XOR 0 = 0, 1 XOR 0 = 1, and 0 XOR 1 = 1, what is 1011 XOR 1100?
Answer: _____

Match each question to its answer

1. What does 'mod' mean in mathematics? For example, what is 17 mod 5? →
2. A clock shows hours 1 through 12. If it is currently 10 o'clock and you add 5 hours, what time does the clock show? This is an example of mod 12 arithmetic. →
3. The Caesar cipher uses mod 26 arithmetic. If you shift the letter Y (position 25) forward by 4, what letter do you get using (25 + 4) mod 26? →
4. Why is modular arithmetic essential for encryption to work on computers? →
5. The RSA encryption algorithm uses modular arithmetic with very large prime numbers. If a key uses a 2048-bit number, approximately how many decimal digits does that represent? →

(A) About 617 digits
(B) 2, because 17 divided by 5 has a remainder of 2
(C) 3 o'clock
(D) C (position 3)
(E) It keeps numbers within a fixed range, preventing values from growing infinitely large during calculations

---

9. Modern Encryption Concepts

Circle the correct answer

81. In symmetric encryption, how many keys are used for both encrypting and decrypting a message?
(A) None — it uses passwords instead (B) Three — encrypt, decrypt, and verify (C) Two — one for each direction (D) One — the same key encrypts and decrypts

82. AES (Advanced Encryption Standard) is the most widely used symmetric encryption algorithm today. What key sizes does AES support?
(A) 8, 16, and 32 bits (B) 64 and 128 bits (C) 512 and 1024 bits (D) 128, 192, and 256 bits

83. What is the biggest practical challenge with symmetric encryption when communicating with someone new?
(A) It cannot encrypt large files, and this has been consistently demonstrated in practice (B) You must find a secure way to share the secret key with the other person before communicating (C) It only works on text, not images, as this is what research and standard practice suggests (D) The encryption is too slow, as this directly follows from the underlying principles

84. A Caesar cipher and AES are both symmetric encryption algorithms. What makes AES dramatically more secure?
(A) AES uses letters instead of numbers, as this directly follows from the underlying principles (B) AES only works on computers, and this principle applies across similar situations (C) AES is newer, and this is the standard approach used in most cases (D) AES uses a much larger key space (2^128 to 2^256 possible keys) and multiple rounds of complex mathematical transformations

85. In a classroom of 30 students, if every pair wants to communicate privately using symmetric encryption, how many unique shared keys are needed? Use the formula n(n-1)/2.
(A) 435 keys (B) 60 keys (C) 900 keys (D) 30 keys

86. Asymmetric encryption uses how many keys per person?
(A) No keys — it uses passwords, as this directly follows from the underlying principles (B) Two — a public key for encrypting and a private key for decrypting (C) One shared key, and this principle applies across similar situations (D) Three keys, making this the most widely accepted explanation

Write the answer

87. In RSA encryption, what mathematical problem makes it secure?
Answer: _____

88. Alice wants to send Bob a secret message using asymmetric encryption. Whose public key does Alice use to encrypt the message?
Answer: _____

89. Why can you safely post your public key on a website for anyone to see?
Answer: _____

90. Asymmetric encryption is much slower than symmetric encryption. In practice, how do systems like HTTPS use both types together?
Answer: _____

Match each question to its answer

1. What is a digital signature used for? →
2. To create a digital signature, which key does the signer use? →
3. How does a recipient verify a digital signature? →
4. A digitally signed email from your bank warns about a security issue. How does the digital signature help you trust this email? →
5. Could a digital signature system work if the private key were made public and the public key were kept secret? Evaluate this reversed approach. →

(A) By using the sender's public key to check that the signature matches the message content
(B) Their private key
(C) To verify the identity of the sender and ensure the message has not been tampered with
(D) The signature proves the email genuinely came from the bank and has not been altered by anyone during transmission
(E) No — if the signing key were public, anyone could forge signatures, defeating the entire purpose of authentication

---

10. Steganography & Information Hiding

Circle the correct answer

91. Steganography hides the existence of a message, while cryptography scrambles a message. Which technique would you use if you want nobody to even suspect a secret message exists?
(A) Cryptography (B) Compression (C) Hashing (D) Steganography

92. The word 'steganography' comes from Greek roots meaning what?
(A) Secret number (B) Covered or hidden writing (C) Protected message (D) Invisible letter

93. In ancient Greece, Histiaeus reportedly shaved a slave's head, tattooed a message on their scalp, waited for the hair to regrow, then sent the slave as a messenger. What type of technique is this?
(A) A cipher — letters are shifted (B) Steganography — the message is physically hidden from view (C) A code — words are replaced (D) Cryptography — the message

is encoded

94. During World War II, microdots reduced a full page of text to the size of a period in a typed sentence. Why was this an effective steganographic technique?
(A) The text was encrypted on the microdot, and this has been consistently demonstrated in practice (B) Microdots self-destructed after reading, as this directly follows from the underlying principles (C) The microdot was too small to notice, and the letter it was embedded in appeared completely normal (D) Microdots could not be photographed, and this principle applies across similar situations

95. Why is the combination of steganography and cryptography considered more secure than either technique alone?
(A) The combination uses less computing power (B) Steganography makes encryption unnecessary (C) Both techniques cancel each other out (D) Even if the hidden message is discovered, it remains encrypted and unreadable without the key

96. Digital images store each pixel's color as numbers. In the most common image steganography technique, where is the secret data hidden?
(A) In the image border pixels only, and this has been consistently demonstrated in practice (B) In the least significant bits (LSBs) of the pixel color values (C) In the file name, and this principle applies across similar situations (D) In the image metadata only, and this principle applies across similar situations

Write the answer

97. An image is 100 pixels wide and 100 pixels tall, with 3 color channels (RGB) per pixel. If you hide 1 bit per color channel, how many bits of secret data can it hold?
Answer: _____

98. Why does JPEG compression make LSB steganography less reliable than using PNG format?
Answer: _____

99. A steganalyst examines an image suspected of containing hidden data. They notice the distribution of least significant bits is unusually uniform (exactly 50% zeros and 50% ones). What does this suggest?
Answer: _____

100. Evaluate whether posting a steganographic image to social media is a reliable way to transmit hidden messages.
Answer: _____

Match each question to its answer

1. Lemon juice is a common household invisible ink that becomes visible when heated. What chemical process makes the writing appear? →
2. UV-reactive invisible inks glow under ultraviolet light but are invisible in normal light. What property of these inks makes them work? →
3. During the American Revolution, the Culper Spy Ring used a 'sympathetic stain' that required a specific chemical reagent to develop the hidden writing. Why was this more secure than heat-activated invisible ink? →
4. A message is written with invisible ink between the lines of a normal letter. Why is writing a convincing visible 'cover letter' just as important as the hidden message? →
5. Compare the security tradeoffs of invisible ink steganography versus digital image steganography. Which has advantages in what situations? →

(A) The specific reagent was a secret — enemies could heat intercepted letters but would not know which chemical revealed the message
(B) An unconvincing or suspicious-looking cover letter might prompt an interceptor to examine the paper more closely for hidden content
(C) Invisible ink leaves no digital trail but requires physical delivery; digital steganography transmits instantly but may be detected by statistical analysis software
(D) The heat causes the acidic lemon juice residue to oxidize and turn brown before the paper scorches
(E) They contain fluorescent compounds that absorb UV light and re-emit it as visible light

---

11. Cryptography in Daily Life

Circle the correct answer

101. What does the 'S' in HTTPS stand for, and what does it provide?
(A) Secure — it means the connection between your browser and the website is encrypted (B) Speed — it means the website loads faster (C) Standard — it means the website follows rules (D) Storage — it means data is saved

102. When you visit an HTTPS website, your browser shows a padlock icon. What does this padlock indicate?
(A) The connection is encrypted and the website's identity has been verified by a Certificate Authority (B) The website cannot track you, and this principle applies across similar situations (C) The website has no viruses, as this is what research and standard practice suggests (D) The website is owned by the government, making this the most widely accepted explanation

103. TLS (Transport Layer Security) uses the hybrid encryption approach discussed earlier. In what order does it use asymmetric and symmetric encryption?
(A) First asymmetric (to securely exchange a session key), then symmetric (to encrypt the actual data) (B) Symmetric first, then asymmetric, which is why this approach is recommended by experts (C) Only symmetric throughout, as this directly follows from the underlying principles (D) Only asymmetric throughout, and this has been consistently demonstrated in practice

104. A website uses HTTP instead of HTTPS. If you log in, what specific risk does this create?
(A) Your login will not work, as this directly follows from the underlying principles (B) The website will load more slowly, as this is what research and standard practice suggests (C) Your username and password are sent as plaintext that anyone on the same network can intercept and read (D) Your computer will get a virus, as this directly follows from the underlying principles

105. Certificate Authorities (CAs) verify website identities and issue digital certificates. What would happen if a CA were compromised and started issuing fraudulent certificates?
(A) Websites would load faster, and this has been consistently demonstrated in practice (B) Browsers would display more ads, which is why this approach is recommended by experts (C) Attackers could create convincing fake versions of any website, including banks and email, that browsers would trust completely (D) Nothing — CAs are just advisory, which is why this approach is recommended by experts

106. Why is the password 'password123' considered extremely weak even though it has 11 characters?
(A) It uses common words and a predictable number pattern that appear in every password-cracking dictionary (B) Numbers make passwords weaker, making this the most widely accepted explanation (C) It has too many characters, and this is the standard approach used in most cases (D) It uses only lowercase letters, which is why this approach is recommended by experts

Write the answer

107. What is a 'brute force' attack on a password, and why does password length matter?
Answer: _____

108. Two-factor authentication (2FA) requires something you know (password) plus something you have (phone) or something you are (fingerprint). Why is 2FA much more secure than a password alone?
Answer: _____

109. A password manager generates and stores a unique, random 20-character password for each website. Why is this approach more secure than memorizing a few strong passwords?

Answer: _____

110. Some security experts argue that passphrases like 'correct horse battery staple' are better than complex passwords like 'X#9mK&2p'. Evaluate both approaches considering memorability and security.

Answer: _____

Match each question to its answer

1. A blockchain is a chain of data blocks where each block contains a cryptographic hash of the previous block. What does this chaining accomplish? →
2. In Bitcoin's blockchain, 'miners' compete to solve a computational puzzle. What is the purpose of this puzzle? →
3. Why is a blockchain called 'decentralized,' and how does this differ from a traditional bank's database? →
4. A 'smart contract' on a blockchain automatically executes when certain conditions are met. Why does the blockchain's immutability make smart contracts more trustworthy? →
5. Some critics argue that blockchain technology uses excessive energy and is slower than traditional databases. Evaluate whether these tradeoffs are justified for all applications. →

(A) It makes the chain tamper-evident — changing any block would change its hash, breaking the chain from that point forward

(B) Once deployed, the contract code cannot be altered by either party, ensuring the agreed-upon rules are enforced exactly as written

(C) To ensure adding new blocks requires significant computational work, making it impractical to forge or rewrite the chain

(D) Thousands of independent computers each maintain a complete copy of the blockchain, with no single authority controlling it

(E) The tradeoffs are justified when trustless decentralization is essential, but traditional databases are better for applications that can rely on a trusted central authority

---

12. Classical Cipher Systems

Circle the correct answer

111. Which of these is an everyday example where encryption protects your

information?
(A) Reading a printed newspaper (B) Online banking websites (C) Playing a board game (D) Watching a TV show

112. A friend gives you a substitution cipher key where every vowel maps to itself (A→A, E→E, I→I, O→O, U→U). Evaluate whether this is a secure design choice.
(A) It is more secure because it reduces the key size (B) It has no effect on security (C) It is secure because vowels are hard to guess anyway (D) It is insecure because it reveals all vowel positions, making the message much easier to crack

113. Why does frequency analysis become less effective on very short messages?
(A) Frequency analysis only works on printed text (B) Short messages use different letters (C) Short messages may not have enough letters for frequencies to match typical English patterns (D) Short messages are always in code, not cipher

114. A military message uses double columnar transposition — the ciphertext from the first transposition is transposed again with a different keyword. Analyze why this significantly increases security.
(A) It does not increase security at all, which is why this approach is recommended by experts (B) The double transposition creates a far more complex rearrangement that is much harder to reverse, even if one keyword is known (C) It makes the message twice as long, as this is what research and standard practice suggests (D) It converts transposition into substitution, which is the most common explanation for this phenomenon

115. What is the fundamental difference between encoding and encryption?
(A) Encoding transforms data to a different format for compatibility, while encryption transforms data to keep it secret (B) Encoding is more secure, and this principle applies across similar situations (C) Encryption only works on numbers, and this has been consistently demonstrated in practice (D) They are the same thing, which is why this approach is recommended by experts

116. In RSA encryption, what mathematical problem makes it secure?
(A) The difficulty of adding large numbers (B) The difficulty of counting to infinity (C) The difficulty of factoring very large numbers into their prime factors (D) The difficulty of dividing by zero

Write the answer

117. Why is the combination of steganography and cryptography considered more secure than either technique alone?
Answer: _____

118. Two-factor authentication (2FA) requires something you know (password) plus something you have (phone) or something you are (fingerprint). Why is 2FA much more secure than a password alone?

Answer: _____

119. Writing a message using invisible ink that only appears when heated is an example of what kind of technique?

Answer: _____

120. If your keyword is 'BANANA,' how many unique letters does it contribute to the start of the cipher alphabet?

Answer: _____

Match each question to its answer

1. A student claims they can crack a 500-letter substitution cipher using only single-letter frequency analysis. What additional techniques would improve their accuracy? →

2. During World War I, the ADFGVX cipher combined a substitution step with a columnar transposition step. Why was this considered much stronger than either step alone? →

3. What is the hexadecimal value FF equivalent to in decimal? →

4. In symmetric encryption, how many keys are used for both encrypting and decrypting a message? →

5. A photographer sells images online but finds them being used without permission. How could digital watermarking help? →

(A) One — the same key encrypts and decrypts

(B) The substitution defeated frequency analysis while the transposition disrupted word patterns, requiring an attacker to break both layers

(C) A hidden watermark embedded in the image proves ownership even if the visible watermark is cropped out

(D) Analyzing digraph frequencies, common word patterns, double letters, and word endings

(E) 255

---

13. Modern Cryptography Basics

Circle the correct answer

121. You create a cipher wheel with two rotating alphabet disks. To encode a message, you align the inner A with the outer D. What shift value are you using?
(A) 3 (B) 4 (C) 7 (D) 26

122. In a Caesar cipher with a shift of 5, what letter does 'A' become?
(A) G (B) F (C) E (D) D

123. In English, certain two-letter combinations like 'TH,' 'HE,' and 'IN' appear much more often than others. What are these common pairs called?
(A) Diagrams (B) Diphthongs (C) Digraphs or bigrams (D) Biletters

124. In a columnar transposition, some columns may have one more letter than others when the message length is not evenly divisible by the keyword length. How do you handle this?
(A) Shorter columns get padding characters or are left shorter, depending on the specific implementation (B) Use a different keyword, and this has been consistently demonstrated in practice (C) Add random words to make it fit, making this the most widely accepted explanation (D) Remove extra letters from the message, and this has been consistently demonstrated in practice

125. Why do programmers prefer hexadecimal over decimal when displaying encryption keys and hash values?
(A) Hex is more compact than binary and converts directly to groups of 4 bits, making bit-level patterns visible (B) Decimal does not work with computers, which is the most common explanation for this phenomenon (C) Hex is more secure than decimal, which is why this approach is recommended by experts (D) Hex was invented for encryption, which is why this approach is recommended by experts

126. Why can you safely post your public key on a website for anyone to see?
(A) Websites are always secure, as this directly follows from the underlying principles (B) The public key can only encrypt messages — it cannot decrypt them, so knowing it does not compromise security (C) Public keys expire immediately, and this is the standard approach used in most cases (D) Public keys cannot be copied, as this is what research and standard practice suggests

Write the answer

127. The word 'steganography' comes from Greek roots meaning what?
Answer: _____

128. A password manager generates and stores a unique, random 20-character password for each website. Why is this approach more secure than memorizing a few strong passwords?
Answer: _____

129. In World War II, Navajo Code Talkers used their native language to create a military code. Why was this code so effective?
Answer: _____

130. You decide to use the keyword 'PYTHON' to build a cipher alphabet. What are the first six letters of your cipher alphabet?
Answer: _____

Match each question to its answer

1. After E, which letter is the second most common in English text? →
2. In a rail fence cipher with 2 rails, how do you write the plaintext 'HELLO WORLD'? →
3. A common hash function produces a 256-bit output. If displayed in hexadecimal, how many hex characters long is this output? →
4. How does a recipient verify a digital signature? →
5. UV-reactive invisible inks glow under ultraviolet light but are invisible in normal light. What property of these inks makes them work? →

(A) By using the sender's public key to check that the signature matches the message content
(B) They contain fluorescent compounds that absorb UV light and re-emit it as visible light
(C) Alternate letters between two rows in a zigzag: H on top, E on bottom, L on top, L on bottom, and so on
(D) 64 characters
(E) T

---

14. Codebreaking Techniques

Circle the correct answer

131. Design a simple cipher system for your classroom. What three components must you decide on to make it work?
(A) The language, volume, and speed of speaking (B) The number of students, classroom size, and time of day (C) The font size, paper color, and ink type (D) The algorithm (method), the key (secret value), and how to share the key securely

132. You receive the ciphertext 'WKH FDW VDW RQ WKH PDW.' You try a shift of 3 backward and get 'THE CAT SAT ON THE MAT.' What does this successful decryption confirm?
(A) The shift was 23 forward (B) The message was encrypted with a substitution cipher (C) The message was encrypted with a Caesar cipher using a shift of 3 (D) The

code was unbreakable

133. What is the most frequently used letter in the English language?
(A) E (B) T (C) A (D) S

134. An attacker intercepts a message encrypted with both substitution and transposition. They successfully reverse the transposition. Will frequency analysis now work on the remaining substitution layer?
(A) Only if the substitution used a Caesar cipher (B) Frequency analysis never works after transposition (C) Yes — once the transposition is reversed, the text has only substitution remaining, which is vulnerable to frequency analysis (D) No — the combination makes frequency analysis permanently impossible

135. In ASCII, uppercase 'A' is 65 and each subsequent letter increases by 1. What is the ASCII value of 'E'?
(A) 70 (B) 67 (C) 69 (D) 68

136. A man-in-the-middle attack on Diffie-Hellman involves an attacker intercepting and replacing the exchanged values. How do digital certificates prevent this?
(A) Certificates block all network attacks, as this is what research and standard practice suggests (B) Certificates verify the identity of each party, so the attacker cannot convincingly substitute their own values (C) Certificates encrypt the exchanged values, and this principle applies across similar situations (D) Certificates make the exchange faster, making this the most widely accepted explanation

Write the answer

137. Why does JPEG compression make LSB steganography less reliable than using PNG format?
Answer: _____

138. A website uses HTTP instead of HTTPS. If you log in, what specific risk does this create?
Answer: _____

139. Your friend sends you the ciphertext 'KHOOR' using a Caesar cipher with a shift of 3. What is the plaintext message?
Answer: _____

140. If someone claims their Caesar cipher is unbreakable because they used a shift of 13 (ROT13), how would you evaluate this claim?
Answer: _____

Match each question to its answer

1. You notice that in your ciphertext, one particular letter never appears at the beginning of any word but frequently appears in the middle and end. What might this pattern tell you? →
2. A route cipher writes plaintext into a grid and then reads it off following a specific path (spiral, diagonal, zigzag). What is the 'route' in a route cipher? →
3. What is ASCII, and why is it important for computers handling text? →
4. Could a digital signature system work if the private key were made public and the public key were kept secret? Evaluate this reversed approach. →
5. An image is 100 pixels wide and 100 pixels tall, with 3 color channels (RGB) per pixel. If you hide 1 bit per color channel, how many bits of secret data can it hold? →

(A) The specific path pattern used to read letters from the grid to create ciphertext
(B) 30,000 bits
(C) No — if the signing key were public, anyone could forge signatures, defeating the entire purpose of authentication
(D) This letter likely represents a letter like X or K that rarely starts English words but appears mid-word
(E) A standardized number code that assigns a unique number to each character so computers can store and process text

---

15. Cybersecurity Foundations

Circle the correct answer

141. What do we call the original readable message before it has been turned into a code?
(A) Hypertext (B) Ciphertext (C) Plaintext (D) Subtext

142. Decode this Atbash ciphertext: 'SVOOL'. Remember, Atbash reverses the alphabet (A↔Z, B↔Y, etc.).
(A) JELLO (B) SVOOL (C) WORLD (D) HELLO

143. Design an experiment to test whether frequency analysis works on text from different genres (poetry vs science textbook). What would you measure and compare?
(A) Count letter frequencies in each genre and compare whether E, T, A remain the top three despite different vocabulary (B) Check which uses more punctuation, and this has been consistently demonstrated in practice (C) Compare the number of pages, and this is the standard approach used in most cases (D) Count the number of paragraphs, which is the most common explanation for this phenomenon

144. In a columnar transposition cipher, you write the plaintext into a grid row by row and then read the columns in a specific order determined by a keyword. What determines the column reading order?
(A) The frequency of each keyword letter (B) Random selection (C) The alphabetical order of the letters in the keyword (D) The length of the message

145. If you XOR (exclusive OR) two binary values where 1 XOR 1 = 0, 0 XOR 0 = 0, 1 XOR 0 = 1, and 0 XOR 1 = 1, what is 1011 XOR 1100?
(A) 1111 (B) 0111 (C) 1001 (D) 0011

146. SHA-256 always produces a 256-bit hash regardless of input size. What is this property called?
(A) Reversible hashing (B) Fixed-length output (C) Deterministic encryption (D) Variable compression

Write the answer

147. Evaluate whether posting a steganographic image to social media is a reliable way to transmit hidden messages.
Answer: _____

148. End-to-end encryption (E2EE) in messaging apps like Signal means that only the sender and recipient can read the messages. Who else is specifically prevented from reading them?
Answer: _____

149. What is the main purpose of encrypting a message?
Answer: _____

150. Create a substitution cipher key using the keyword 'SUN.' Write the first 5 letters of the resulting cipher alphabet.
Answer: _____

Match each question to its answer

1. Evaluate this claim: 'Frequency analysis can crack any substitution cipher.' Is this statement accurate? →
2. In a transposition cipher, what stays the same between the plaintext and ciphertext? →
3. Convert the binary sequence 1010 1100 to hexadecimal. Show your process. →
4. Asymmetric encryption is much slower than symmetric encryption. In practice, how do systems like HTTPS use both types together? →
5. A steganalyst examines an image suspected of containing hidden data. They notice the distribution of least significant bits is unusually uniform (exactly 50% zeros and

50% ones). What does this suggest? →

(A) The actual letters used and their frequencies
(B) It is mostly true for simple substitution ciphers on long English texts, but polyalphabetic ciphers resist frequency analysis
(C) The image likely contains hidden data, because natural images typically have non-uniform LSB distributions
(D) AC — split into nibbles: 1010=A (10), 1100=C (12), so 10101100 = AC
(E) Asymmetric encryption securely exchanges a temporary symmetric key, then symmetric encryption handles the actual data transfer

---

16. Cryptography Basics

Circle the correct answer

151. A student creates a code where the first letter of each sentence in a paragraph spells out a secret word. What would you call this technique?
(A) Brute force attack (B) Public key encryption (C) Frequency analysis (D) Acrostic cipher

152. What happens when you reach the end of the alphabet while applying a Caesar cipher shift?
(A) You stop encoding (B) You use numbers instead (C) You reverse the alphabet (D) You wrap around to the beginning of the alphabet

153. Double letters like 'LL,' 'SS,' 'EE,' and 'OO' appear frequently in English. Why are double letters useful for breaking ciphers?
(A) They narrow down possibilities because only certain letters commonly double in English (B) They are impossible to encrypt, making this the most widely accepted explanation (C) They indicate the cipher key, and this principle applies across similar situations (D) They always represent vowels, and this is the standard approach used in most cases

154. If you apply a Caesar cipher (shift 5) to 'HELLO' and then a 2-rail fence to the result, what is the final ciphertext?
(A) HELLO, according to the standard framework used to analyze this topic (B) First Caesar: MJQQT. Then 2-rail: M_Q_T on top, *J_Q* on bottom → MQTJQ (C) TQQJM, which reflects the current consensus among experts in this field (D) MJQQT, which is the most widely accepted explanation for this concept

155. After a Diffie-Hellman exchange, Alice and Bob both have the same shared secret. What do they typically use this secret for?
(A) As a symmetric encryption key (like AES) for fast, secure communication (B) They use it as a password for a website (C) They publish it online (D) They discard it immediately

156. You intercept a coded message but do not know the shift value. If you try every possible shift from 1 to 25, what is this decryption strategy called?
(A) Key exchange (B) Frequency analysis (C) Steganography (D) Brute force attack

Write the answer

157. Using a Caesar cipher with shift 1, encode the phrase 'GOOD JOB' letter by letter.
Answer: _____

158. The RSA encryption algorithm uses modular arithmetic with very large prime numbers. If a key uses a 2048-bit number, approximately how many decimal digits does that represent?
Answer: _____

159. A Caesar cipher and AES are both symmetric encryption algorithms. What makes AES dramatically more secure?
Answer: _____

160. Steganography hides the existence of a message, while cryptography scrambles a message. Which technique would you use if you want nobody to even suspect a secret message exists?
Answer: _____

Match each question to its answer

1. Morse code translates letters into patterns of dots and dashes. Is Morse code technically an encoding system or a cipher? →
2. To calculate the frequency percentage of a letter in a text, what formula do you use? →
3. Ancient Spartans used the scytale to transpose messages. How did wrapping a strip around a rod of specific diameter create a transposition? →
4. What does 'mod' mean in mathematics? For example, what is 17 mod 5? →
5. Design a physical classroom demonstration of Diffie-Hellman key exchange using numbered cards. Describe the steps and what each participant does. →

(A) Start with a shared public number, each student picks a secret number, combines them using an agreed operation (like multiplication mod a prime), exchanges results publicly, then each combines the received result with their secret to get the same final number

(B) (Number of times the letter appears ÷ total number of letters) × 100

(C) An encoding system

(D) Letters written in rows across the wraps were scrambled when the strip was unwound, separating adjacent letters

(E) 2, because 17 divided by 5 has a remainder of 2

Riddle & Joke Break

Guess the answer, then check the key!

161. Why did the spy fail the math test?

162. What do you call a spy who sleeps under a blanket?

163. Why was the Caesar cipher always tired?

164. What's a cryptographer's favorite snack?

165. Why did the secret message break up with the envelope?

166. What do spies do when they get cold?

Answer Key

1. A — Scytale
2. A — World War II
3. D — Cryptography
4. C — Plaintext
5. D — Caesar cipher
6. D — To keep information private from unauthorized readers
7. Online banking websites
8. It unlocks the method needed to convert ciphertext back to plaintext
9. To prevent enemies from understanding intercepted communications

10. Replacing each letter with a symbol from a shared secret chart
    Matching (Secret Messages Basics): 1→A, 2→A, 3→D, 4→C, 5→E
11. C — F
12. D — You wrap around to the beginning of the alphabet
13. B — D
14. A — 4
15. B — A shift of 0 or 26 leaves the message unchanged, so it does not count as encryption
16. C — Each letter can map to any other letter, not just a fixed shift
17. Approximately 400 septillion (26 factorial)
18. XKM
19. A keyword is written first in the cipher alphabet, followed by the remaining unused letters in order
20. It is insecure because it reveals all vowel positions, making the message much easier to crack
    Matching (Caesar & Substitution Ciphers): 1→E, 2→A, 3→D, 4→C, 5→B
21. A — E
22. B — T
23. A — Z, Q, X, and J
24. D — The most frequently appearing three-letter group in the ciphertext
25. C — Digraphs or bigrams
26. C — E
27. (Number of times the letter appears ÷ total number of letters) × 100
28. 9%
29. That letter very likely represents E, since E is by far the most common English letter
30. They likely represent T and A, which have similar frequencies in English (about 9% and 8%)
    Matching (Frequency Analysis): 1→E, 2→B, 3→A, 4→D, 5→C
31. A — Scytale

32. A — World War II
33. D — Cryptography
34. C — Plaintext
35. D — Caesar cipher
36. D — To keep information private from unauthorized readers
37. Online banking websites
38. It unlocks the method needed to convert ciphertext back to plaintext
39. To prevent enemies from understanding intercepted communications
40. Replacing each letter with a symbol from a shared secret chart
    Matching (Secret Messages Basics): 1→A, 2→A, 3→D, 4→C, 5→E
41. C — F
42. D — You wrap around to the beginning of the alphabet
43. B — D
44. A — 4
45. B — A shift of 0 or 26 leaves the message unchanged, so it does not count as encryption
46. C — Each letter can map to any other letter, not just a fixed shift
47. Approximately 400 septillion (26 factorial)
48. XKM
49. A keyword is written first in the cipher alphabet, followed by the remaining unused letters in order
50. It is insecure because it reveals all vowel positions, making the message much easier to crack
    Matching (Caesar & Substitution Ciphers): 1→E, 2→A, 3→D, 4→C, 5→B
51. A — E
52. B — T
53. A — Z, Q, X, and J
54. D — The most frequently appearing three-letter group in the ciphertext
55. C — Digraphs or bigrams

56. C — E
57. (Number of times the letter appears ÷ total number of letters) × 100
58. 9%
59. That letter very likely represents E, since E is by far the most common English letter
60. They likely represent T and A, which have similar frequencies in English (about 9% and 8%)
    Matching (Frequency Analysis): 1→E, 2→B, 3→A, 4→D, 5→C
61. D — Substitution replaces letters with other letters, while transposition rearranges the positions of the original letters
62. D — The actual letters used and their frequencies
63. C — Because the letters are not changed, only rearranged — so frequency distributions match normal English
64. C — TERCES
65. B — Letters written in rows across the wraps were scrambled when the strip was unwound, separating adjacent letters
66. B — Alternate letters between two rows in a zigzag: H on top, E on bottom, L on top, L on bottom, and so on
67. ATCADWTAKTAN
68. The pattern uses 4 positions per cycle (down 3, up 2), so 15 letters = 3 full cycles plus a partial
69. You must figure out how many letters go on each rail and place them correctly before reading the zigzag
70. 5 rails provides better security because there are more possible rail counts to guess and the rearrangement is more complex
    Matching (Transposition Ciphers): 1→E, 2→D, 3→C, 4→A, 5→B
71. D — 13
72. D — HELP
73. A — A standardized number code that assigns a unique number to each character so computers can store and process text
74. D — 69

75. B — D
76. A — Binary
77. 101
78. 256
79. 13
80. 0111
    Matching (Number-Based Codes): 1→B, 2→C, 3→D, 4→E, 5→A
81. D — One — the same key encrypts and decrypts
82. D — 128, 192, and 256 bits
83. B — You must find a secure way to share the secret key with the other person before communicating
84. D — AES uses a much larger key space (2^128 to 2^256 possible keys) and multiple rounds of complex mathematical transformations
85. A — 435 keys
86. B — Two — a public key for encrypting and a private key for decrypting
87. The difficulty of factoring very large numbers into their prime factors
88. Bob's public key
89. The public key can only encrypt messages — it cannot decrypt them, so knowing it does not compromise security
90. Asymmetric encryption securely exchanges a temporary symmetric key, then symmetric encryption handles the actual data transfer
    Matching (Modern Encryption Concepts): 1→C, 2→B, 3→A, 4→D, 5→E
91. D — Steganography
92. B — Covered or hidden writing
93. B — Steganography — the message is physically hidden from view
94. C — The microdot was too small to notice, and the letter it was embedded in appeared completely normal
95. D — Even if the hidden message is discovered, it remains encrypted and unreadable without the key
96. B — In the least significant bits (LSBs) of the pixel color values

97. 30,000 bits
98. JPEG uses lossy compression that alters pixel values, destroying the hidden data in the least significant bits
99. The image likely contains hidden data, because natural images typically have non-uniform LSB distributions
100. It is unreliable because social media platforms re-compress and resize images, likely destroying the hidden data
Matching (Steganography & Information Hiding): 1→D, 2→E, 3→A, 4→B, 5→C
101. A — Secure — it means the connection between your browser and the website is encrypted
102. A — The connection is encrypted and the website's identity has been verified by a Certificate Authority
103. A — First asymmetric (to securely exchange a session key), then symmetric (to encrypt the actual data)
104. C — Your username and password are sent as plaintext that anyone on the same network can intercept and read
105. C — Attackers could create convincing fake versions of any website, including banks and email, that browsers would trust completely
106. A — It uses common words and a predictable number pattern that appear in every password-cracking dictionary
107. Trying every possible combination of characters; longer passwords have exponentially more combinations to try
108. Even if an attacker steals your password, they also need physical access to your second factor, which is much harder to obtain remotely
109. Unique passwords per site mean a breach at one site does not compromise your accounts elsewhere
110. Passphrases are easier to remember and can be equally or more secure because their length compensates for lower character complexity
Matching (Cryptography in Daily Life): 1→A, 2→C, 3→D, 4→B, 5→E
111. B — Online banking websites
112. D — It is insecure because it reveals all vowel positions, making the message much easier to crack
113. C — Short messages may not have enough letters for frequencies to match

typical English patterns

114. B — The double transposition creates a far more complex rearrangement that is much harder to reverse, even if one keyword is known
115. A — Encoding transforms data to a different format for compatibility, while encryption transforms data to keep it secret
116. C — The difficulty of factoring very large numbers into their prime factors
117. Even if the hidden message is discovered, it remains encrypted and unreadable without the key
118. Even if an attacker steals your password, they also need physical access to your second factor, which is much harder to obtain remotely
119. Steganography
120. 3
    Matching (Classical Cipher Systems): 1→D, 2→B, 3→E, 4→A, 5→C
121. A — 3
122. B — F
123. C — Digraphs or bigrams
124. A — Shorter columns get padding characters or are left shorter, depending on the specific implementation
125. A — Hex is more compact than binary and converts directly to groups of 4 bits, making bit-level patterns visible
126. B — The public key can only encrypt messages — it cannot decrypt them, so knowing it does not compromise security
127. Covered or hidden writing
128. Unique passwords per site mean a breach at one site does not compromise your accounts elsewhere
129. Very few people outside the Navajo nation could understand the language
130. P, Y, T, H, O, N
    Matching (Modern Cryptography Basics): 1→E, 2→C, 3→D, 4→A, 5→B
131. D — The algorithm (method), the key (secret value), and how to share the key securely
132. C — The message was encrypted with a Caesar cipher using a shift of 3

133. A — E
134. C — Yes — once the transposition is reversed, the text has only substitution remaining, which is vulnerable to frequency analysis
135. C — 69
136. B — Certificates verify the identity of each party, so the attacker cannot convincingly substitute their own values
137. JPEG uses lossy compression that alters pixel values, destroying the hidden data in the least significant bits
138. Your username and password are sent as plaintext that anyone on the same network can intercept and read
139. HELLO
140. The claim is false — ROT13 still has the same weakness as any Caesar cipher and can be broken instantly
    Matching (Codebreaking Techniques): 1→D, 2→A, 3→E, 4→C, 5→B
141. C — Plaintext
142. D — HELLO
143. A — Count letter frequencies in each genre and compare whether E, T, A remain the top three despite different vocabulary
144. C — The alphabetical order of the letters in the keyword
145. B — 0111
146. B — Fixed-length output
147. It is unreliable because social media platforms re-compress and resize images, likely destroying the hidden data
148. The messaging company itself, internet service providers, and anyone who intercepts the data in transit
149. To keep information private from unauthorized readers
150. S, U, N, A, B
    Matching (Cybersecurity Foundations): 1→B, 2→A, 3→D, 4→E, 5→C
151. D — Acrostic cipher
152. D — You wrap around to the beginning of the alphabet

153. A — They narrow down possibilities because only certain letters commonly double in English
154. B — First Caesar: MJQQT. Then 2-rail: M_Q_T on top, *J_Q* on bottom → MQTJQ
155. A — As a symmetric encryption key (like AES) for fast, secure communication
156. D — Brute force attack
157. HPPE KPC
158. About 617 digits
159. AES uses a much larger key space (2^128 to 2^256 possible keys) and multiple rounds of complex mathematical transformations
160. Steganography
    Matching (Cryptography Basics): 1→C, 2→B, 3→D, 4→E, 5→A
161. Because all the answers were in code!
162. An undercover agent!
163. Because it kept shifting all night!
164. Crack-ers!
165. It felt too sealed off from the world!
166. They go undercover!
