

1. A packet header contains:
 - ☐ the sender and receiver IP addresses and the packet number
 - ☐ only the actual data
 - ☐ the end-of-packet marker
 - ☐ the whole file
2. In an even-parity system, the parity bit is set so that:
 - ☐ the total number of 1s in the byte is even
 - ☐ the byte always ends in 0
 - ☐ the number is positive
 - ☐ the data is encrypted
3. What does encryption achieve?
 - ☐ it makes intercepted data unreadable to the wrong person
 - ☐ it stops data being intercepted at all
 - ☐ it makes data travel faster
 - ☐ it compresses the data
4. Serial transmission:
 - ☐ sends one bit at a time down one wire and is good over long distances
 - ☐ sends several bits at once down several wires
 - ☐ is always faster than parallel
 - ☐ cannot be used on a network
5. A parity check catches a single flipped bit, but if TWO bits flip the 1-count's parity can still look correct, hiding the error.
 - ☐ True ☐ False
6. Symmetric encryption uses:
 - ☐ a single shared key for both encrypting and decrypting
 - ☐ a public key and a private key
 - ☐ no key
 - ☐ a parity bit

7. Simplex sends data one way only, half-duplex sends both ways but one at a time, and full-duplex sends both ways at the same time (like a phone call).
- ☐ True ☐ False
8. Asymmetric encryption is safer for sharing because only the public key is ever sent — the private key that decrypts the data never has to be shared.
- ☐ True ☐ False
9. A checksum detects errors by:
- ☐ recalculating a value from the received data and comparing it with the sent value
 - ☐ sending the data back to the sender
 - ☐ adding a parity bit
 - ☐ encrypting the data
10. In asymmetric encryption, data is encrypted with the _____ key and decrypted with the _____ key.
- ☐ public; private
 - ☐ private; public
 - ☐ same; same
 - ☐ secret; shared

1. the sender and receiver IP addresses and the packet number

The header carries control info (addresses + packet number); the payload is the data; the trailer marks the end + error check.

2. the total number of 1s in the byte is even

Even parity makes the count of 1s even; the receiver re-counts to detect a single-bit error.

3. it makes intercepted data unreadable to the wrong person

Encryption scrambles data so interception is useless — it does not prevent the interception itself.

4. sends one bit at a time down one wire and is good over long distances

Serial = one bit at a time (cheaper, long-distance reliable); parallel = many bits at once (fast, short-distance).

5. True

That blind spot is why stronger checks (checksums, CRC) are used when reliability really matters.

6. a single shared key for both encrypting and decrypting

Symmetric uses one secret key that both sides must share — the risk is that key being stolen.

7. True

The three modes differ by direction and timing: simplex (one way), half-duplex (take turns), full-duplex (both at once).

8. True

Symmetric encryption's weak point is getting the shared key to the other side safely; asymmetric removes that by keeping the private key secret.

9. recalculating a value from the received data and comparing it with the sent value

The receiver recomputes the checksum; if it differs from the sent one, the data is resent.

10. public; private

The public key encrypts; only the matching private key can decrypt — so the secret key is never shared.