

17 Encryption – Part 1 — Answers

Answers

Work through these after trying the questions yourself.

17.1 Ciphertext.

17.2 The key (and the decryption algorithm).

17.3 One (the same key at both ends).

17.4 It is fast and good for bulk data.

17.5 Key distribution — sharing the key safely.

17.6 Shift each letter *back* by 3: $F \rightarrow C$, $D \rightarrow A$, $W \rightarrow T$, giving "CAT". Decryption reverses the shift used to encrypt.

17.7 They must both have the same secret key, but to send it over the open internet they would need a secure channel — which is exactly what they are trying to set up. This is the key-distribution problem.