6 Security, privacy and data integrity – Part 2 —Answers

Answers

6.1 The recipient's public key.

6.2 Symmetric uses one shared key for both encrypting and decrypting; asymmetric uses a public key to encrypt and a separate private key to decrypt. (Any clear difference.)

6.3 That it really came from the stated sender, and that it has not been altered in transit.

6.4 It floods a server (or network) with so much traffic that it cannot respond, so genuine users are denied the service.

6.5 The sender computes a summary value (checksum) from the data and sends it too; the receiver recomputes the checksum from the data it received and compares —if they differ, the data was corrupted.

6.6 Symmetric needs both sides to share one secret key, which is hard to send safely. Asymmetric uses a freely-shared public key to lock and a never-shared private key to unlock, so no secret key has to be exchanged.

6.7 Adding the bytes gives the same total whatever their order, so swapping two bytes leaves the sum (and the checksum) unchanged —the error is not detected.