

# 17 Asymmetric encryption and hashing – Part 2 —Answers

---

## Answers

---

Work through these after trying the questions yourself.

**17.1** Two (a pair).

**17.2** The public key is shared; the private key is kept secret.

**17.3** Only the matching private key (the owner's).

**17.4** No —it is one-way.

**17.5** It changes completely.

**17.6** Hashing is one-way, so the stored digests cannot be turned back into passwords. If the database is stolen, the attacker still cannot read the real passwords —far safer than storing them as plain text.

**17.7** Asymmetric encryption is slow, so it is poor for large amounts of data. A common solution is to use asymmetric encryption just to share a symmetric key safely, then use fast symmetric encryption for the bulk data itself.