1.3 EXCHANGING DATA · 1.3.1

Encryption & hashing

Symmetric vs asymmetric encryption, and the **uses of hashing**. Spec 1.3.1(c)(d).

01 Encryption

What Scramble plaintext → ciphertext with a key. Two-way.

Protects Confidentiality (stops it being **understood**, not intercepted).

- **Symmetric**
  One shared key. Fast. Hard to distribute the key securely.
- **Asymmetric**
  Public key encrypts, private key decrypts. Solves key distribution; slower. HTTPS.

02 Hashing

What Input → fixed-length hash. **One-way** (cannot reverse).

vs encryption Encryption is two-way; hashing is one-way.

Uses Password storage · data integrity checks · hash tables.

Good hash Fast, fixed length, very hard to reverse, few collisions.

03 Why hashing protects passwords

Store Save the **hash**, never the password.

Login Hash the entered password and compare the hashes.

Stolen DB Attacker gets only hashes, which can't be reversed to the real passwords.

FINAL PASS BEFORE THE EXAM

Rapid exam tips

Seven slips on encryption and hashing questions.

01

Encryption is **two-way** (decrypt with a key); hashing is **one-way**. Don't confuse them.

02

Asymmetric: **public key encrypts, private key decrypts**. Never share the private key.

03

Symmetric's weakness is secure **key distribution** — asymmetric solves it.

04

Encryption stops data being **understood**, not intercepted.

05

Passwords are **hashed**, not "encrypted" — so they can't be recovered.

06

Know **3 uses of hashing**: passwords, integrity checks, hash tables.

07

Good-hash "characteristics": quick to compute, fixed-length output, hard to reverse, few **collisions**.