Solutions

Each answer shows the steps, then the **result**.

2.1

- encryption changes readable data into a scrambled form
- purpose: so it **cannot be understood if intercepted**

2.2

- readable data before encryption is called **plaintext**

3.1 B

- data encrypted with a public key is decrypted only with the **matching private key**
- A is the same public key; C is symmetric; D is error-checking, not decryption

3.2

(a)

- both sides share one secret key
- main risk: the **shared key could be stolen while being sent**

(b)

- the public key encrypts; only the private key (kept secret) decrypts
- **no secret key ever has to be shared**

3.3

- encryption does **not** stop interception
- it only stops the intercepted data from being **understood**

3.4

(a)

- data on the internet passes through equipment the company does not control and can be intercepted
- encryption means an interceptor **cannot understand** the contents even if they capture them

(b)

- the **same key** encrypts and decrypts
- sender encrypts plaintext with the key; receiver applies the same key in reverse
- weakness is **key distribution**: if the key is intercepted on the way, the whole system is broken

(c)

- two related keys: a **public key** and a **private key**
- anyone may use the published public key to **encrypt**

- only the matching **private key**, never shared, can **decrypt**
- so no secret has to be sent in advance

(d)

- **plaintext** is the original readable data
- **ciphertext** is the scrambled version
- encryption does not block the transmission — it only makes intercepted data **meaningless without the key**