Solutions

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

2.1

- the scrambled output of an encryption algorithm

2.2

- the same key is used to encrypt and to decrypt; both parties must share that secret key

2.3

- $2^4 = 16$

3.1 B

- AES is the symmetric standard

3.2 B

- more possible keys means more guessing time

3.3

(a)

- sharing the single secret key safely

(b)

- a longer key has a larger keyspace so it is harder to guess, but it takes more time to encrypt and decrypt

3.4 B

- a stream cipher (A) works one element at a time; C describes asymmetric encryption

3.5

(a)

- AES with a 128-bit key

(b)

- `-e` means encrypt
- `-out report.enc` names the output file that holds the ciphertext

(c)

```
openssl enc -aes-128-cbc -d -in report.enc -k Tiger42 -out report.txt
```

- `-d` with the same algorithm
- the same password, with the input and output files swapped

(d)

- the key is derived from the password, and symmetric encryption uses the same key to decrypt

3.6

- $2^{256} \div 2^{128} = \mathbf{2^{128}}$ times (about 3.4×10^{38})