Solutions

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

2.1

- asymmetric encryption allows secure communication **without prearranging a shared secret key**; with symmetric encryption the same key must reach both parties first, which is itself a problem when there is no secure channel yet

2.2

(a)

- Wen's key, the **public** key

(b)

- Wen's key, the **private** key

(c)

- the matching public key is published, so anyone could obtain it and decrypt the file; encrypting with a private key proves origin, but provides no confidentiality

2.3

- any three of: the private key is exposed, shared, stolen, corrupted, or compromised

2.4

(a)

- $2^8 = 256$; average $2^7 = 128$ guesses

(b)

- $2^{20} = 1\,048\,576$; average $2^{19} = 524\,288$ guesses

2.5

- the keyspace **doubles**, because $2^{n+1} = 2 \times 2^n$ - so a single extra bit doubles the work an adversary faces

2.6

- encryption and decryption both take more time

2.7

- computational processing power and efficiency keep improving, so software can guess keys faster than before and a length that was safe when a recommendation was written becomes breakable within a practical time

2.8

- key-length comparison is only valid when comparing keys for the **same** cryptographic algorithm; ECC and RSA achieve their security by different mathematics, so bit counts across the two are not comparable at all - in practice ECC reaches equivalent security at much shorter lengths

2.9

- RSA; elliptic curve cryptography / ECC; any two applications, e.g. digital signatures, secure web traffic, secure key exchange, encrypted email

3.1 D

- Only the receiver's private key can undo it, and only the receiver holds that

3.2 D

- $2^{12} = 4096$

3.3 C

- $2^n \div 2 = 2^{n-1}$

3.4 B

- Longer keys are slower, do not remove the need for secure storage, and recommendations change as processing power improves

3.5

(a)

- the firm encrypts the file with **that barrister's public key**, taken from the manager's folder; only that barrister's private key can decrypt it, so only the intended recipient can read it. To reply, the barrister encrypts with the **firm's public key** and the firm decrypts with its own private key

(b)

- a private key must be stored securely, and a copy on a shared network drive is reachable by everyone with access to that drive - so an adversary who reaches it can decrypt every file ever sent to the firm, including past traffic they may have captured. If that drive is compromised the key pair is no longer secure: it must be replaced and the new public key distributed to all three barristers

(c)

- processing power and efficiency have improved continuously since 2012, so the number of keys that can be tried in a given time has risen by orders of magnitude; 1024-bit RSA is therefore now regarded as too short, and the firm should follow current recommendations rather than the figure chosen when the system was installed

(d)

- the argument is **wrong**. A key-length comparison is only valid **within one algorithm**, and RSA and ECC are different algorithms; ECC achieves equivalent security

at far shorter key lengths, so 256-bit ECC is considered comparable to - or stronger than - 1024-bit RSA, and it is also faster

(e)

- any two of: one shared key means any single barrister's compromise exposes **all** case files, including those sent to the others; the key must first be delivered securely to three separate parties, which asymmetric encryption avoids entirely; revoking one barrister's access requires re-keying everyone. Symmetric encryption is still preferable for **bulk data** - encrypting a large archive, or the firm's own files at rest - because it is much faster