

**Group A**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **2** | **5** | **1** | **3** | **4** |
| F | I | R | E | A |
| T | N | I | N | E |

Q1

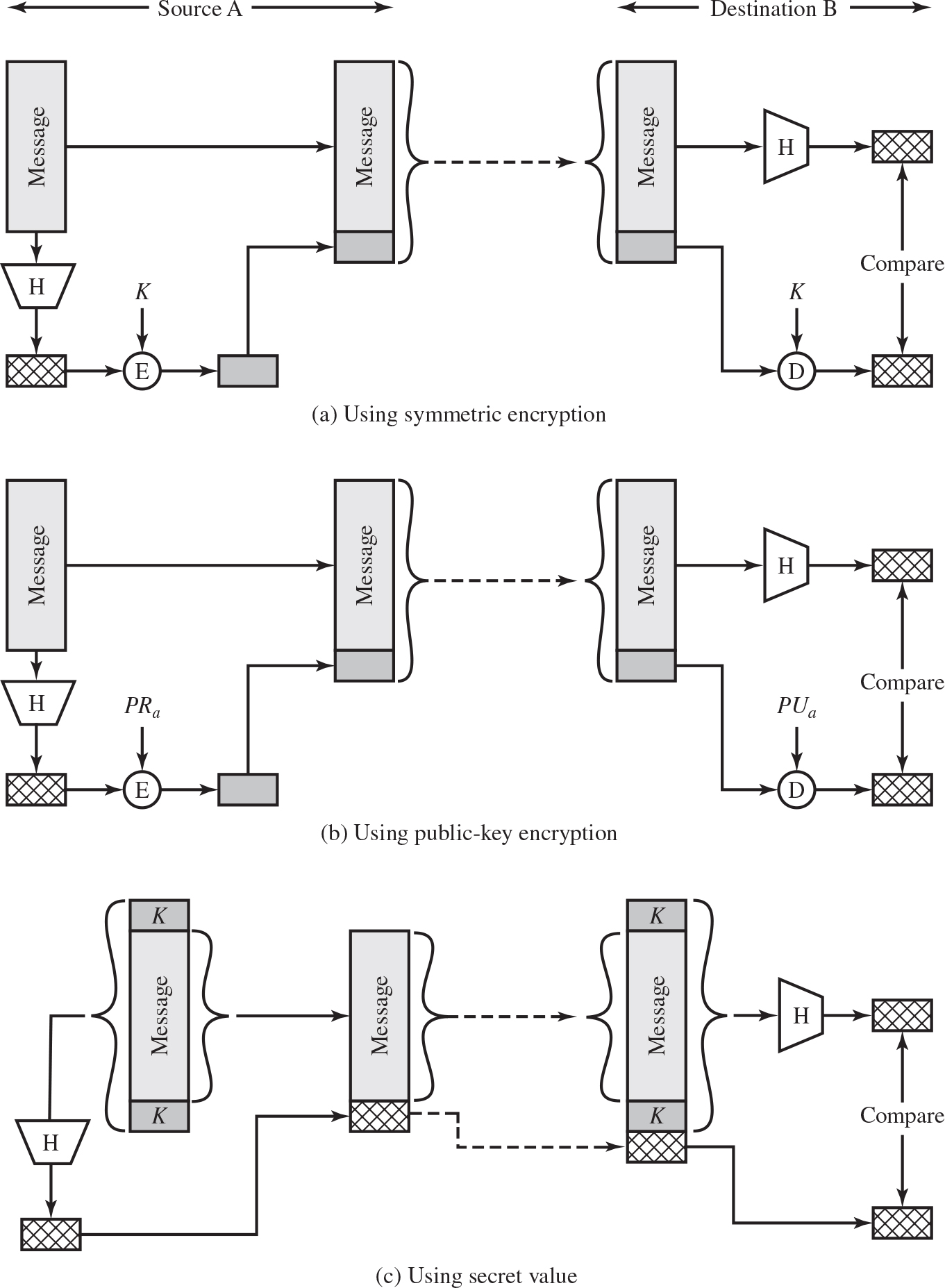
FIRE AT NINE

2 marks for workings (table), 1 for output

Q2

Diagram like below. It is also fine to put K at one end only rather than both.

Make sure that K is **not transmitted**, but only used during hashing.



Q3

Business applies for certificate to cert authority.

They also submit business registration docs to Registration Authority.

RA verifies the supplied info, sends OK report to CA who issue the certificate.

CA also store the cert in their repository.

**Group B**

Q1

Evaluate the sequence 7k+1

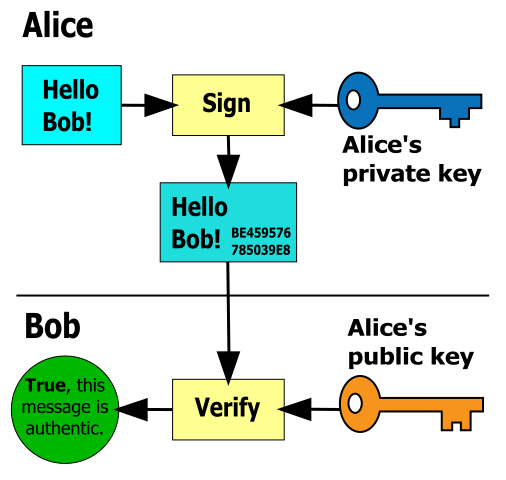
For k = 1 to 5 we get 7k+1 = 8, 15, 22, 29, 36

36 / 6 = 6

Hence = 6

Q2

Sample diagram



Q3

OCSP provides a quicker way to check revocation status of a specific certificate. Previously CRLs were used which had some problems: heavy traffic load on the Internet bcoz every client needs to download it regularly, CRLs become outdated very quickly and do not hold information of most recently revoked certificates.