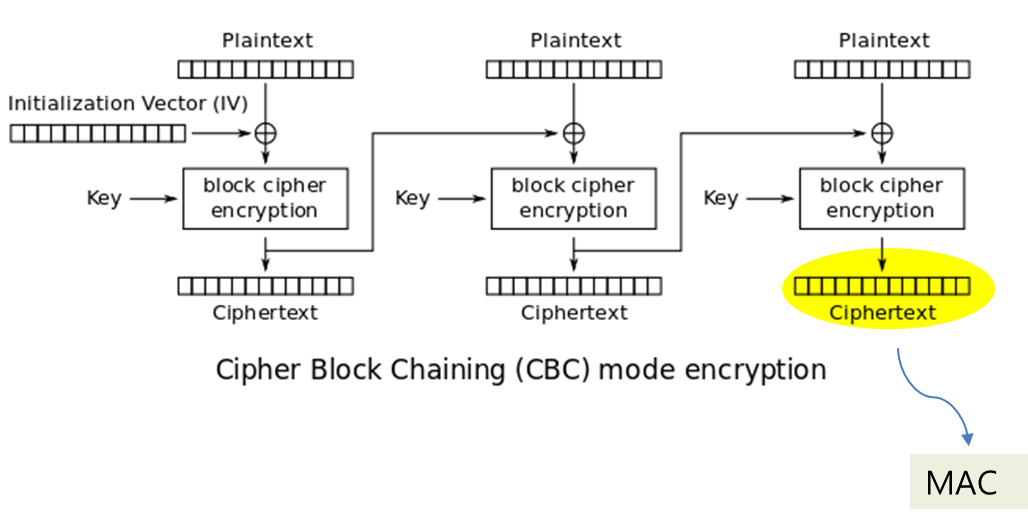


**Group A**

Q1

Phi(18) = 6

Q2



Q3

Any two

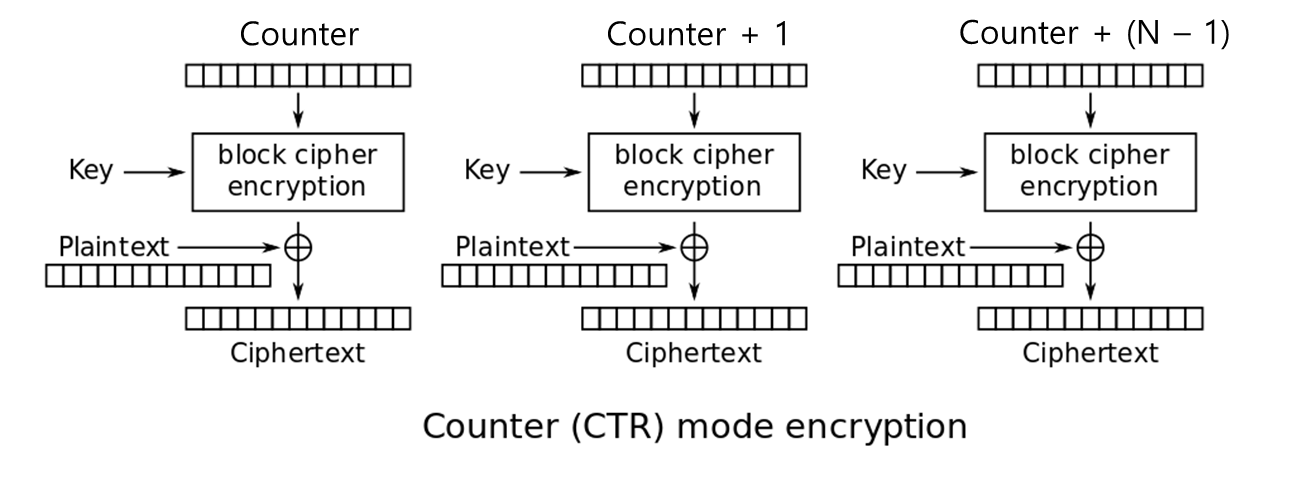
|  |  |
| --- | --- |
| **Reason** | **Outcome of non-revocation** |
| Client’s private key compromised | Attacker can pretend to be the client |
| Staff member on leave, or left the company | Staff member can still represent the company |
| Subject details changed | Certificate will be no longer useful for subject |
| CA’s private key compromised | Attacker can issue fake certificates to themselves |
| Subject provided false information | Users will keep on trusting deceptive subject |

**Group B**

Q1

Any two from: 4, 6, 8, 12, 14, 16, 18, 21, 22, 24

Q2



Q3

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CRLs become outdated very quickly and do not hold information of most recently revoked certificates.

Q4

OCSP response mush be signed by the OSCP responder (server). 1 mark

The responder must present their certificate from CA to prove their identity. 1 mark