1) **Riduzioni: metodologia.** Si descriva la struttura generale di una riduzione di sicurezza, evidenziando le motivazioni alla base dell'approccio e le proprietà che soddisfa. Inoltre, come caso d'esempio, si dimostri che:

- se G è un generatore pseudocasuale, allora lo schema di cifratura che associa al messaggio **m** il cifrato **c** := G (k) ⊙ **m**, con chiave k viene scelta uniformemente a caso e dove ⊙ indica l'operazione di XOR bit a bit, è uno schema di cifratura EAV-sicuro (cifrature indistinguibili rispetto ad un eavesdropper).

2) **Reti SPN e reti di Feistel.** Si spieghi in modo chiaro e conciso

- cosa sono e perché sono importanti nella progettazione di cifrari simmetrici
- cosa si intende per **confusione e diffusione**, e come vengono ottenute

Inoltre si discutano brevemente due esempi di crittosistemi usati nella pratica, progettati usando i due paradigmi.

3) **Funzioni One way.** Si spieghi in modo chiaro e conciso

- cosa sono e come si definiscono
- perché sono sufficienti per realizzare tutta la "crittografia simmetrica"

4) **Gruppi ciclici.** Si spieghi in modo chiaro e conciso

- cosa sono
- come sono definiti i problemi DL e DH (computazionale e decisionale) su tali gruppi
- perché i gruppi di ordine primo sono importanti in crittografia

5) **Crittosistemi a chiave pubblica.** Si spieghi in modo chiaro e coinciso che cosa si intende per crittosistema a chiave pubblica CPA-sicuro. Inoltre, si fornisca un esempio di crittosistema che soddisfa tale definizione. In particolare, si descriva il funzionamento del crittosistema scelto e si fornisca uno sketch della prova di CPA-sicurezza.

6) **Schemi di firme digitali.** Si spieghi in modo chiaro e coinciso che cosa si intende per schema di firme digitali sicuro rispetto ad un adaptive chosen message attack. Inoltre, si fornisca un esempio di schema di firme che soddisfa tale definizione. In particolare, si descriva il funzionamento dello schema di firme scelto e si fornisca uno sketch della prova di sicurezza.