Ispitna pitanja na predmetu Sigurnost računalnih sustava
Implementacijski napadi

1. Što je implementacijski napad?
2. Navesti osnovnu podjelu implementacijskih napada?
3. Opisati napade koji koristi sporedna svojstva uređaja (engl. side-channel attack, SCA)?
4. Navesti osnovnu podjelu napada koji koriste sporedna svojstva uređaja (engl. side-channel attack, SCA)?
5. Što je napad jednostavnom analizom potrošnje električne energije (engl. Simple Power Analysis)?
6. Opiši DPA?
7. Nabrojati modele curenja informacija (engl. leakage models)?
8. Opisati profilirani napad (engl. profiled attack)?
9. Opisi napad korištenjem uzoraka (engl. template attack)?
10. Nabrojati neke metode koje se koriste u napadima ubacivanja pogrešaka (engl. fault injection).
11. Nabrojati napade ubacivanja pogrešaka (engl. fault injection)?
12. Što je DFA?
13. Opisati kriptografiju za ugrađene sustave i Internet stvari (engl. lightweight crypto)?
14. Navesti i obasniti neke od uobičajenih zahtjeva za kriptografske algoritme za ugrađene sustave i Internet stvari (engl. lightweight crypto)?
15. Navesti tri kriptografska algoritma za ugrađene sustave i Internet stvari (engl. lightweight cryptoalgorithms)?
16. Koje su klase RNG-ova?
17. Koja su svojstva PRNGa?
18. Koja su svojstva TRNGa?
19. Opisati van Neumann postprocesiranje.
20. Što je TRSM?
21. Što je HSM?