Ispitna pitanja na predmetu Sigurnost računalnih sustava ak. god. 2019./2020.g.
Simetrični kriptosustavi

1. Pojasniti svojstva konfuzije i difuzije koja moraju zadovoljavati simetrični blok algoritmi?
2. Navesti osnovno svojstvo supstitucijskih kutija u supstitucijko-permutacijskim konstrukcijama?
3. Koja je prednost Feistelovih nad supstitucijko-permutacijskim konstrukcijama?
4. Opisati DES (samo osnovne principe rada algoritma).
5. Kako možemo podijeliti modove operacija?
6. Opisi CBC mod.
7. Skiciraj OFB mod.
8. Koji modovi pretvaraju blok algoritam u algoritam kriptiranja toka podataka (stream)?
9. Što je GCM mod?
10. Koja je osnovna razlika blok algoritma i algoritma kriptiranja toka podataka?
11. Koja je prednost algoritama toka podataka nad blok algoritmima?
12. Koji je standardni način dizajniranja algoritma kriptiranja toka podataka?
13. Što je LFSR?
14. Koji je nelinearni element u filter i kombinator generatorima (engl. combiner generators)?
15. Koja su svojstva nelinearnih elemenata potrebna da bi se koristila u kombinator generatorima (engl. combiner generators)?
16. Ukratko opisati algoritam Trivium?
17. Opisi algoritam RC4?