Kriptografija in računalniska varnost – 1. domača naloga (do srede 18. nov., 2009)

1. Napišite približno eno stran dolg spis z naslovom:

   "Kako mi bo ta predmet koristil pri mojem študiju (oziroma delu)".

2. Anita ima novo idejo za biometrično avtentikacijo, ki uporablja običajen računalnik in miško. Tipičen uporabnik (Bojan) dobi navodilo, da sede pred računalnik. Na zaslonu se nahaja 10 števil v poljubnem fiksnem položaju (položaj je vedno isti za Bojana, toda lahko je drugačen za druge uporabnike). Bojanova naloga je, da gre z miškinim kazalcem v pravilnem zaporedju od števil $1, 2, 3, \ldots$ vse do števila 10. Anita trdi, da sta Bojanova pot in čas dovolj dobra informacija za biometrično avtentikacijo.

   (a) Ali je Anitina trditev smiselna? Na katere stvari bi morali paziti, če bi se hoteli odločili ali naj uporabimo to shemo? Oceniti morate kako dobro bi delovala ta shema za avtentikacijo. Na kakšne probleme bi utegnili naleteti, če bi poskusili implementirati to idejo?

   (b) Privzemite, da imate na voljo le običajen hardware (miško, računalnik, tipkovnico, itd.) in predlagajte bolj smiselno shemo za biometrično avtentikacijo, če je le ta možna.

   Odgovor/rešitev naj ne bo daljša od ene strani.

3. Kompresijo podatkov pogosto uporabljamo za shranjevanje ali prenos podatkov. Kompresijo opravimo tako, da odstranimo določene informacije, brez katerih znamo rekonstruirati original. Predpostavimo, da uporabljamo kompresijo skupaj s šifriranjem. Ali je smiselno narediti naslednje operacije

   (i) kompresirati informacijo in jo potem zašifrirati,

   (ii) zašifrirati informacijo in jo potem kompresirati?

   Utemelji svoj odgovor (podaj vsaj dva razloga)!

4. Za dan simetričen šifrirni sistem E_k definirajmo naključni simetrični šifrirni sistem F_k:

$$F_k(m) = (E_k(r), r \oplus m),$$

   kjer je r zaporedje bitov enake velikosti kot zaporedje m. Output za $F_k(m)$ je torej enkripcija enkratnega-ščita r, skupaj z originalnim sporočilom m, ki mu prištejemo (XOR) naključno število r. Za vsako enkripcijo si izberemo novo/neodvisno naključno število.

   Oglejmo si dva napada, katerih cilj je odkriti tajni ključ k.

   (a) Pri napadu z izbranim čistopisom si lahko napadalec izbere zaporedja nizov $m_1, m_2, \ldots$ in za vsak niz m_i najde ustrezen tajnopis.

   (b) Pri napadu z naključnim čistopisom napadalec dobi naključne pare čistopis/tajnopis. Opomba: napadalec nima kontrole nad naključnimi števili r, ki so uporabljena za generiranje parov čistopis/tajnopis.

   Dokaži, da je šifrirni sistem F_k varen pred napadom z izbranim čistopisom, če je E_k varen pred napadom z naključnim čistopisom.