**Kriptografija in računalniška varnost – 2. domača naloga (do torka 10. marca, 2008)**

1. (a) (*Popravljanje napak na DES-ovemu tajnopisu*) Z DES-om zašifriramo $s$ blokov čistopisa $m_1 m_2 \dots m_s$ v tajnopis $c_1 c_2 \dots c_s$. Pri prenosu se $i$-ti blok poškoduje. Koliko blokov tajnopisa se bo odšifriralo narobe, če uporabimo (i) ECB način oziroma (ii) CBC način?

   (b) (*DES-ova komplementarna lastnost*) Z $\overline{m}$ označimo komplement binarnega zaporedja $m$. Ni se težko prepričati, da je $\overline{c} = DES_{\overline{k}}(\overline{m})$ za $c = DES_k(m)$. Ali lahko uporabite to lastnost DES-a za izboljšanje časa požrešnega napada (i) pri poznanem čistopisu (ii) pri izbranem čistopisu?

   (c) Opišite napad s poznanim čistopisom na DES-ov CBC način, ki odkrije tajni ključ? Ocenite koliko DES širiranj/dešifriranj potrebuje Vaš napad.

2. Oglejmo si naslednji predlog za zaščito DES-a pred požrešnim napadom (tj. napadom, ki pregleda vse ključe). Tajni ključ je $k = (k_1, k_2)$, kjer je $k_1 \in \{0,1\}^{56}$ in $k_2 \in \{0,1\}^{64}$. Naj bo $m \in \{0,1\}^{64}$ čistopis. Šifriranje se opravi na naslednji način:

$$E_k(m) = DES_{k_1}(m) \oplus k_2.$$

   (a) Pokažite, da se s tem predlogom ne poveča čas, ki je potreben za požrešni napad (z drugimi besedami, poiskati morate napad, ki potrebuje reda velikosti $2^{56}$ DES šidriranj/dešifriranj). Privzamete lahko, da poznate majhno število parov čistopis/tajnopis $c_i = E_k(m_i)$.

   (b) Odgovorite na isto vprašanje, če opravite šifriranje na naslednji način:

$$E_k(m) = DES_{k_1}(m \oplus k_2).$$

3. 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 $m_1, m_2, \dots$ 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.