1. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 13. junij 2012

1. (25 točk) Dani sta praštevili $p = 17$ in q $= 31$, s katerima bi radi generirali svoj javni ključ za RSA.

   (a) Katera od števil $25, 27, 29$ lahko izberemo za kodirni eksponent?

   (b) Za najmanjšega izmed teh primernih eksponentov e izračunajte dekodirni eksponent d.

   (c) Z zasebnim ključem $(p \cdot q, d)$ dešifrirajte kriptogram 2.

2. (25 točk) Pri tej nalogi nas bodo zanimali ključi, pri katerih je kodirna funkcija enaka dekodirni funkciji. Imenovali jih bomo *involucijski ključi*.

   (a) Poiščite vse involucijske ključe za Cezarjevo šifro nad $\mathbb{Z}_{26}$.

   (b) Naj bo $K = (a, b)$ ključ za afino šifro nad $\mathbb{Z}_n$. Pokažite, da je K involucijski ključ če in samo če velja $a^{-1} \equiv a \pmod{n}$ in $b(a + 1) \equiv 0 \pmod{n}$.

   (c) Poiščite vse involucijske ključe za afino šifro nad $\mathbb{Z}_{26}$.

   (d) Naj velja $n = pq$, kjer sta p in q različni lihi praštevili. Koliko je v tem primeru različnih ključev za afino šifro nad $\mathbb{Z}_n$? Pokažite, da je število involucijskih ključev enako $n + p + q - 1$.

3. (20 točk) Oglejmo si naslednji predlog za zaščito DES-a pred napadom z izčrpnim iskanjem ključev. 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 $m \in \{0, 1\}^{64}$ besedilo. Šifriranje se opravi na naslednji način:

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

   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 šifriranj/dešifriranj). Privzamete lahko, da poznate majhno število parov besedilo/kriptogram $c_i = E_k(m_i)$.

4. (30 točk) Dan je polinom $g(x) = (x - 1)(x + 2)(x + 3)$ s koeficienti iz $\mathbb{Z}_7$.

   (a) Preverite, da je g generatorski polinom za ciklični kod $\mathcal{C}$ dolžine 6 nad abecedo $\mathbb{Z}_7$.

   (b) Poiščite dimenzijo in razmaknjenost koda $\mathcal{C}$.

   (c) Poiščite še generatorsko in nadzorno matriko v standardni obliki za kod $\mathcal{C}$.

   (d) Ali kod doseže Singeltonovo mejo? Ali doseže Hammingovo mejo?

Vse naloge je potrebno ustrezno utemeljiti!