1. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 7. maj 2010

1. (15 točk) Prestregli ste kriptogram $c = PRCRGHYAOTPGTYIANSFERU$ in uganili, da je poslano besedilo enako $b = cryptographyisgreatfun$. Ugotovite, kateri kriptosistem je bil uporabljen, in poiščite ustrezni ključ.

2. (25 točk) Besedila šifriramo z afino šifro nad množico besedil $\mathbb{Z}_{126}$.

   (a) Izračunajte število vseh možnih ključev za to šifro.

   (b) Naj bo kodirni ključ enak $(29, 7)$ (besedilo b torej zakodiramo v kriptogram $29b + 7 \pmod{126}$). S pomočjo razširjenega Evklidovega algoritma poiščite dekodirni ključ in dekodirajte kriptogram $c = 9$.

3. (25 točk) Tokovno šifro T sestavimo iz dveh linearnih rekurzivnih šifer. Ključ z_i, $i = 1, 2, \ldots$, za to šifro dobimo takole (vse računanje poteka po modulu 2):

$$z_i = x_i + y_i, \qquad \text{kjer je} \qquad x_i = x_{i-1} + x_{i-2} \qquad \text{in} \qquad y_i = y_{i-2} + y_{i-3}.$$

   Začetni ključ je $(x_1, x_2, y_0, y_1, y_2)$.

   (a) Za dan začetni ključ $(1, 0, 1, 0, 0)$ izračunajte prvih nekaj členov zaporedij x_i, y_i in z_i. Kakšne so njihove periode?

   (b) Poiščite linearno rekurzivno šifro L najmanjše stopnje, ki generira isto izhodno zaporedje kot šifra T, če je začetno stanje enako kot v točki (a).

   (c) Ali šifra L generira isto zaporedje kot šifra T za poljubno začetno stanje?

4. (35 točk) V tej nalogi boste raziskali takoimenovani *napad s ciklanjem*, pri katerem kriptogram večkrat zaporedoma šifriramo, dokler ne odkrijemo besedila.

   Naj bo (n, e) javni ključ za kriptosistem RSA. Naj bo $b \in \{0, 1, \ldots n-1\}$ besedilo in $c = b^e \pmod{n}$ ustrezen kriptogram.

   (a) Pokažite, da obstaja naravno število k, za katero velja

$$b^{e^k} \equiv b \pmod{n}.$$

   (b) Za takšno število k pokažite, da velja

$$c^{e^{k-1}} \equiv b \pmod{n} \quad \text{oziroma} \quad c^{e^k} \equiv c \pmod{n}.$$

   (c) Opišite napad na RSA, ki temelji na ugotovitvah iz točk (a) in (b) in ga zapišite v obliki algoritma. Vhodni podatki za algoritem so javni ključ za RSA (n, e) in kriptogram c, algoritem pa vrne ustrezno besedilo b.

   (d)* Za kakšno izbiro n in e je ta napad lahko nevaren (dovolj hiter)?

   (e) S pomočjo napada iz točke (c) dešifrirajte kriptogram $c = 20$ za javni ključ $(n = 91, e = 5)$.

Vse odgovore je potrebno ustrezno utemeljiti!