1. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 23. april 2013

1. (16 točk) Ali ima

   (a) Cezarjeva

   (b) multiplikativna šifra

   (c) afina šifra

   nad $\mathbb{Z}_{25}$ lastnost popolne tajnosti, če so vsi ključi enako verjetni?

2. (16 točk) Alenka besedila šifrira s tokovno šifro na naslednji način:

   - ključ je generiran z linearno rekurzivno šifro reda 4,
   - besedilo pretvori v dvojiški zapis: vsaki od črk priredi številko med 0 in 24 ($A \to 0,\ B \to 1, \ldots, \check{Z} \to 24$), te pa nato pretvori v dvojiški zapis, za vsak znak uporabi po 5 mest,
   - besedilo in ključ sešteje po modulu 2 in pretvori nazaj v črke, števila med 25 in 31 pa pretvori v znake 1-7.

   Boris je prestregel kriptogram $\check{Z}50$ in uganil, da se besedilo začne z AN. Dešifrirajte še preostanek besedila!

3. (20 točk) Alenka in Boris se bosta udeležila spletne dražbe. Dražitelji svoje ponudbe zašifrirajo z javnim ključem RSA dražbene hiše (n, e). Vsaka ponudba je številka - znesek, ki ga dražitelj ponuja za dani predmet. Predmet kupi tisti, ki zanj največ ponudi.

   Alenka je pravkar poslala svojo ponudbo $y = x^e \bmod n$, Boris jo je prestregel. Ker hoče preprečiti, da bi Alenka zmagala na dražbi, bi rad dal ponudbo, ki bi za 10% presegala Alenkino. Kako naj Boris sestavi ustrezno ponudbo ne da bi dešifriral Alenkino sporočilo, če je njena ponudba x večkratnik števila 10?

   Napad ilustrirajte še na naslednjih podatkih: $(n, e) = (221, 19)$ in $y = 58$.

4. (8 točk) Naj bo $H : \{0,1\}^* \to \{0,1\}^{256}$ zgoščevalna funkcija, odporna na trke. Katere od naslednjih funkcij so tudi odporne na trke? Vsak odgovor posebej je treba utemeljiti. Povsod je $x \in \{0,1\}^*$.

   (a) $H_1(x) = H(x) \oplus H(x)$,

   (b) $H_2(x) = H(x)[0, \ldots, 31]$, torej vzamemo prvih 32 bitov izvlečka funkcije H,

   (c) $H_3(x) = H(H(x))$,

   (d) $H_5(x) = H(x||0)$.

Vse naloge je potrebno ustrezno utemeljiti!