Bločne šifre, končni obsegi

1. Substitucijsko-permutacijsko omrežje je podano s substitucijo

$$\pi_S = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ E & 4 & D & 1 & 2 & F & B & 8 & 3 & A & 6 & C & 5 & 9 & 0 & 7 \end{pmatrix}$$

   in permutacijo

$$\pi_p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 5 & 9 & 13 & 2 & 6 & 10 & 14 & 3 & 7 & 11 & 15 & 4 & 8 & 12 & 16 \end{pmatrix}.$$

   Pri tem je besedilo dolžine 16 razdeljeno na 4 zloge dolžine 4. Vsak zlog predstavimo z eno šestnajstiško številko. Na besedilu $295C$ izvedite en krog šifriranja s ključem 0011 0011 1100 1000.

2. Feistelova šifra je podana s Feistlovo kodirno funkcijo $f(k, R) = k \oplus R$, ključi pa so dolgi polovico dolžine bloka in vsi enaki. Analizirajte varnost te šifre, če je število krogov pri šifriranju enako dva, tri in v splošnem.

3. Napad s srečanjem v sredini: sestavite napad z izčrpnim iskanjem ključev na dvojni DES, ki ima isto časovno zahtevnost kot napad z izčrpnim iskanjem ključev za DES. Uporabite lahko (zgoščeno) tabelo velikosti $\mathcal{O}(2^{56})$.

   Opomba: podoben napad lahko sestavimo za poljubno bločno šifro, če imamo na voljo dovolj prostora.

4. Ker ima DES premajhno množico ključev, da bi bil varen pred napadom z izčrpnim pregledom ključev, ga dopolnimo na naslednji način. Ključ je $k = (k_1, k_2)$, kjer je $k_1 \in \{0,1\}^{56}$ in $k_2 \in \{0,1\}^{64}$. Naj bo $b \in \{0,1\}^{64}$ besedilo. Kodiramo takole:

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

   Pokažite, da se s tem "popravkom" čas, ki je potreben za izčrpni pregled ključev, ne poveča bistveno. Z drugimi besedami, poiskati morate napad, ki potrebuje reda velikosti 2^{56} DES šifriranj/dešifriranj. Privzamete lahko, da poznate majhno število parov besedilo/kriptogram $c_i = E_k(b_i)$ za $i = 1, 2, \ldots$.

5. Poiščite nerazcepni polinom stopnje 2 nad $\mathbb{Z}_2$ in z njegovo pomočjo sestavite tablico za množenje v obsegu $\mathrm{GF}(2^2)$

6. Preverite, da je polinom $f(x) = x^4 + x + 1$ nerazcepen nad $\mathbb{Z}_2$.

7. Naj bo končni obseg $\mathrm{GF}(2^4)$ generiran z nerazcepnim polinomom $f(x) = x^4 + x + 1$. Naj bo $p_1(x) = x^3 + x + 1$, $p_2(x) = x^2 + x$ in $p_3(x) = x^3 + x^2 + x + 1$ elementi tega obsega. Poiščite $p_1 + p_2$, $p_1 \cdot p_2$ in p_3^{-1}.