Primer ispita iz Kriptografije

1. (15 poena) Implementirati simetričnu blok šifru na osnovu date specifikacije.

   - Veličina bloka je 16 bitova.
   - Sve operacije su u $F_{16} = \mathbb{Z}_2[x]/(x^4 + x + 1)\mathbb{Z}_2[x]$, pri čemu se nibl $N = b_3b_2b_1b_0$ poistovećuje sa $b_3x^3 + b_2x^2 + b_1x + b_0 \in F_{16}$.
   - Ako je N nibl, $S(N) = N^{-1} + x^2 + 1$ (ako je $N = 0$ umesto N^{-1} uzeti 0). Ako je $W = N_0N_1$ bajt, $S(W) = S(N_0)S(N_1)$. Ako je $B = N_0N_1N_2N_3$ blok, $S(B) = S(N_0)S(N_1)S(N_2)S(N_3)$.
   - Ako je $W = N_0N_1$ bajt, $R(W) = N_1N_0$.
   - Šifrovanje se vrši u 3 runde. Neka je $K_0 = W_0W_1$ početni ključ, a $K_i = W_{2i}W_{2i+1}, 1 \leq i \leq 3$ ključ runde i. K_i se određuje po formuli $W_{2i} = W_{2i-2} + R(S(W_{2i-1}))$ i $W_{2i+1} = W_{2i-1} + W_{2i}$.
   - Ako je $B = N_0N_1N_2N_3$ blok, $P(B) = N_3N_1N_2N_0$.
   - Ako je B blok, $D_{K_i}(B) = K_i + B$.
   - Šifrat bloka se računa funkcijom $D_{K_3} \circ P \circ S \circ D_{K_2} \circ P \circ S \circ D_{K_1} \circ P \circ S \circ D_{K_0}$.

2. (15 poena) Implementirati protokol koji omogućava autentifikaciju klijenta prilikom povezivanja na server.

   - Klijent uspostavlja vezu sa serverom i šalje mu svoje korisničko ime.
   - Ukoliko je ovo prvi put da se klijent povezuje sa serverom, server čeka da dobije javni ključ od klijenta. Klijent generiše par RSA ključeva koje čuva u fajlu, a serveru šalje javni deo.
   - Server klijentu šalje broj M.
   - Klijent potpisuje poruku M i serveru šalje potpis S.
   - Server proverava identitet klijenta.

3. (15 poena) Implementirati protokol za razmenu jednog prirodnog broja $M < 2^{64}$ između dva klijenta. Protokol mora biti otporan na moderne napade i koristiti ključeve dužine najviše 512 bitova.

4. (15 poena) Ana je potpisala poruku $M_1 = 123$ ElGamal potpisom

   $$r = 860883284086020753921032463243860692127, s = 166292624565846896889962311051483354152 8$$

   Anin javni ključ je

   $$A = 217165651993392168672630925780423581878 3$$

   a javni parametri su

   $$g = 3, p = 37484499000747702105914277596024492906 11$$

   Potpisati poruku $M_2 = 456$ kao Ana.