Specijalni kurs - Kriptografija - Prvi kolokvijum

1. Popuniti tablicu mnozenja polinoma ostataka pri deljenju sa x^3+x+1 ciji su koeficijenti iz polja F_2[x].
2. Opisati preslikavanje koje definise S tabelu.
3. Izvesti formule za racunanje 2P i P+Q za proizvoljne tacke P i Q elipticke krive. Ukratko opisati proces predstavljana poruke uz pomoc tacke elipticke krive.
4. Po padingu iz PKCS#7 doputniti poruku za blokovsku sifru koja prima blokove duzine 4 bajta.
   0x12 0x34 0x56 0x78 0xab 0x03 0x03 0x03
5. Za RSA kripgofrafski sistem gde radimo po modulu 33:
   - Alisini parametri: privatni ključ 7, javni ključ 3
   - Bobanovi parametri: privatni ključ 9, javni ključ 9
   Boban želi da pošalje poruku m=2 Alisi, on šalje: $2^3 = 8$
   Alisa je potpisala neku poruku m i dobila S(m) = 4, i poslala Bobanu m=25, S(m)=4
   Kako Boban proverava potpis:

   Boban racuna S(m) na Alisin javni kljuc i proverava da li je to jednako sa m
   Odnosno 4^3 == 25 mod 33. Kako 64 != 25 mod 33 on odbija potpis.

   Da li prihvata potpis(zaokruziti): DA NE (prihvatao sam i m^9 == S(m)^3)
6. Za komunikaciju izmedju dva cvora se koristi AES(128b->128b) u modu CTR(counter mode).
   - Poruka koju jedna osoba želi da šifruje je duga 250b, napisatii (u notaciji $AES_k(b_i)$ k je ključ, b_i je i-ti blok poruke) kako se poruka šifruje, ako je nonce *N* i kljuc *k* i koje je duzine šifrat u ovom konkretnum slučaju.

   Poruka se sifruje tako sto se podeli na dva bloka, b1-128b i b2-122b, zatim se izracuna a1=AES_k(N || 1) i a2 = AES_k(N||2), zatim se a2 skrati na 122b. Sifrat je a1 xor b1 || a2 xor b2. Duzina sifrata je 250b.

   - Poruka "GET /domaci/01_zadatak HTTP/1.1" je šifrovana AES-om u modu CTR i dobijena je poruka "lfkajdflkajdfaldajfaldskfjalfdjk" bez poznavanja ključa je moguće promeniti sifrat tako da prilikom dešifrovanja dobijemo poruku "GET /domaci/02_zadatak HTTP/1.1", označiti koji karakteri se menjaju u šifratu i napisati na koji način treba promeniti označene karaktere:

   l f k a j d f l k a j d f a l d a j f a l d s k f j a l f d j k
                         ^

   Kako svaki bit sifrata odgovara istom bitu u otvorenom tekstu potrebno je promeniti bajt koji odgovara karakteru 1 otvorenog teksta odnosno karakter a sifrata.
   Promena koju je potrebno uraditi je: novi_karakter = 'a' xor '1' xor '2'