1. (**20p**) a) Skicirati i objasniti reflektovani DDoS napad.

   b) Nacrtati i objasniti konsolidovani konceptualni model kontrole pristupa (zaštite) pomoću uloga.

2. (**15p**) Aleksa i Bojana komuniciraju koristeći *Elgamal* algoritam. Aleksin javni ključ je predstavljen sledećim skupom vrednosti $\{q, \alpha, Y_A\} = \{11, 2, 3\}$. Bojana želi Aleksi da pošalje poruku $M = 5$ koristeći broj $k = 9$ za generisanje ključa za jednokratnu upotrebu.

   a) Prikazati postupak šifrovanja poruke. Prikazati postupak dešifrovanja poruke na Aleksinoj strani ukoliko je njegov privatan ključ $X_A = 8$. Da li Bojana može da dešifruje poruku koju je šifrovala? Obrazložiti odgovor.

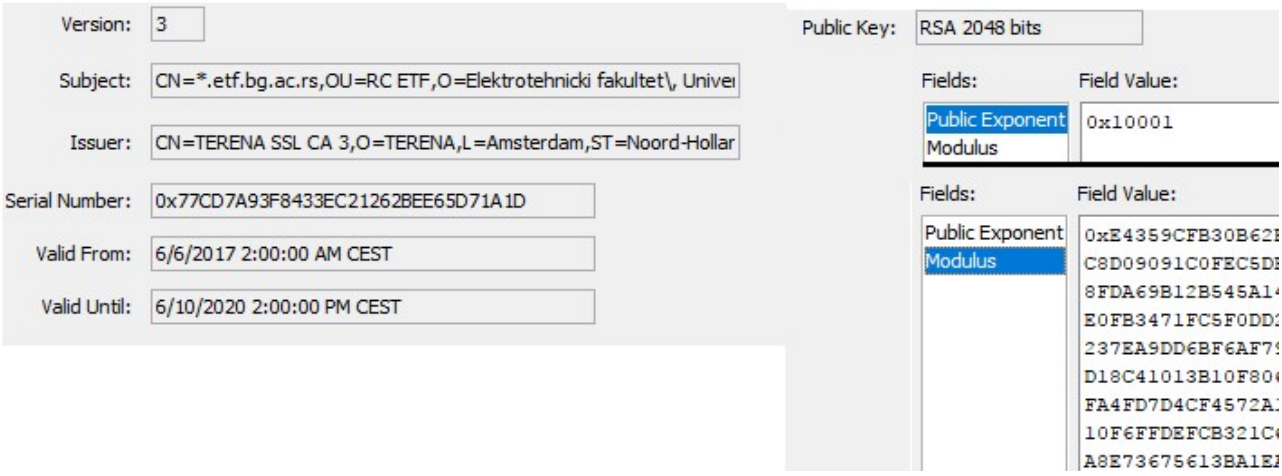
   b) Dokazati da algoritam funkcioniše.

   c) O čemu treba voditi računa ukoliko poruka mora da se razbije na više delova? Na čemu se zasniva sigurnost algoritma?

3. (**15p**) a) (10 poena) Napadač želi da prevari svog poslovnog partnera tako što želi da kreira dve alternativne verzije ugovora sa njim (jedan koji partner želi da potpiše i drugi, lažni, koji nije dogovoren). Autentičnost ugovora se garantuje heš funkcijom koja daje heš dužine 256 bita. Namera napadača je da nakon potpisivanja ugovora, dogovoreni ugovor zameni lažnim, tako da ova prevara ne može da bude otkrivena. Koliko je napadaču prosečno potrebno da kreira različitih ugovora kako bi mogao da izvrši ovu prevaru? Odgovor obrazložiti.

   b) (5 poena) U okviru bitcoin-a u jednom desetominutnom intervalu su bile izvršene 1024 finansijske transakcije. Autentičnost ovih transakcija se garantuje Merkleovim stablom heševa, tako što se uz transakcije u okviru svakog bloka čuva koren Merkleovog stabla. Ukoliko neki korisnik želi da proveri autentičnost transakcije broj 128 (transakcije su obeležene brojevima 1,2,…,1024), koliko mu je minimalno i kojih heševa potrebno poslati kako bi tu proveru mogao da izvrši (podrazumeva se da je koren Merkleovog stabla dobijen sa blokom transakcija i da korisnik sam neće izračunavati sve heševe Merkleovog stabla). Odgovor obrazložiti objašnjenjem funkcionalnosti Merkleovog stabla.

4. (**15p**) Vlasnik X509 sertifikata sa slike 1 danas je saznao sa mu je privatni ključ kompromitovan i odmah je to prijavio izdavaocu sertifikata. Na koji način izdavaoc sertifikata obaveštava druge korisnike da sertifikat više nije u upotrebi? Dati primer i popuniti sve vrednosti koje su poznate.



Slika 1. Kompromitovani sertifikat

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 150 minuta.*