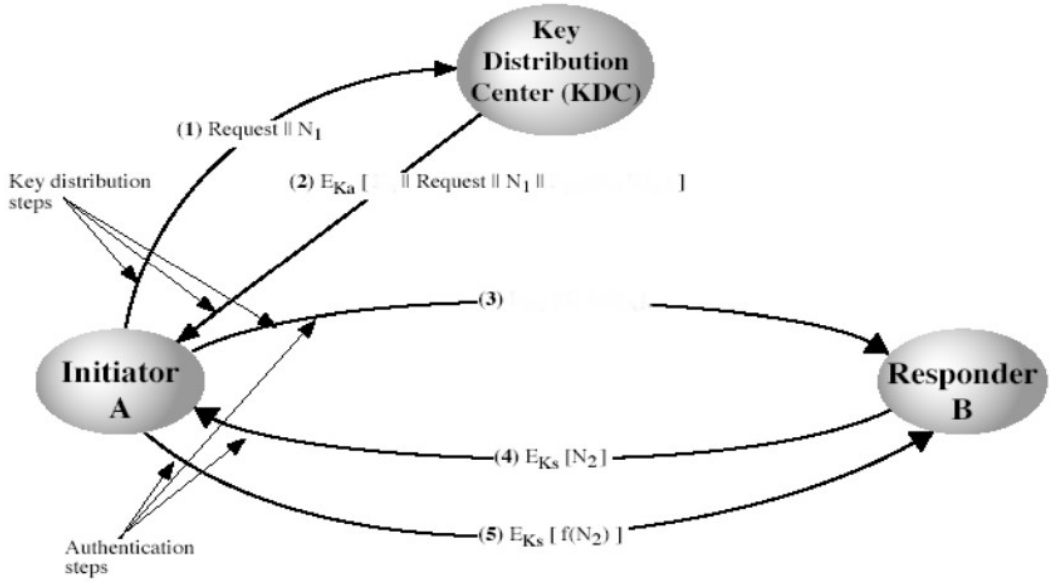
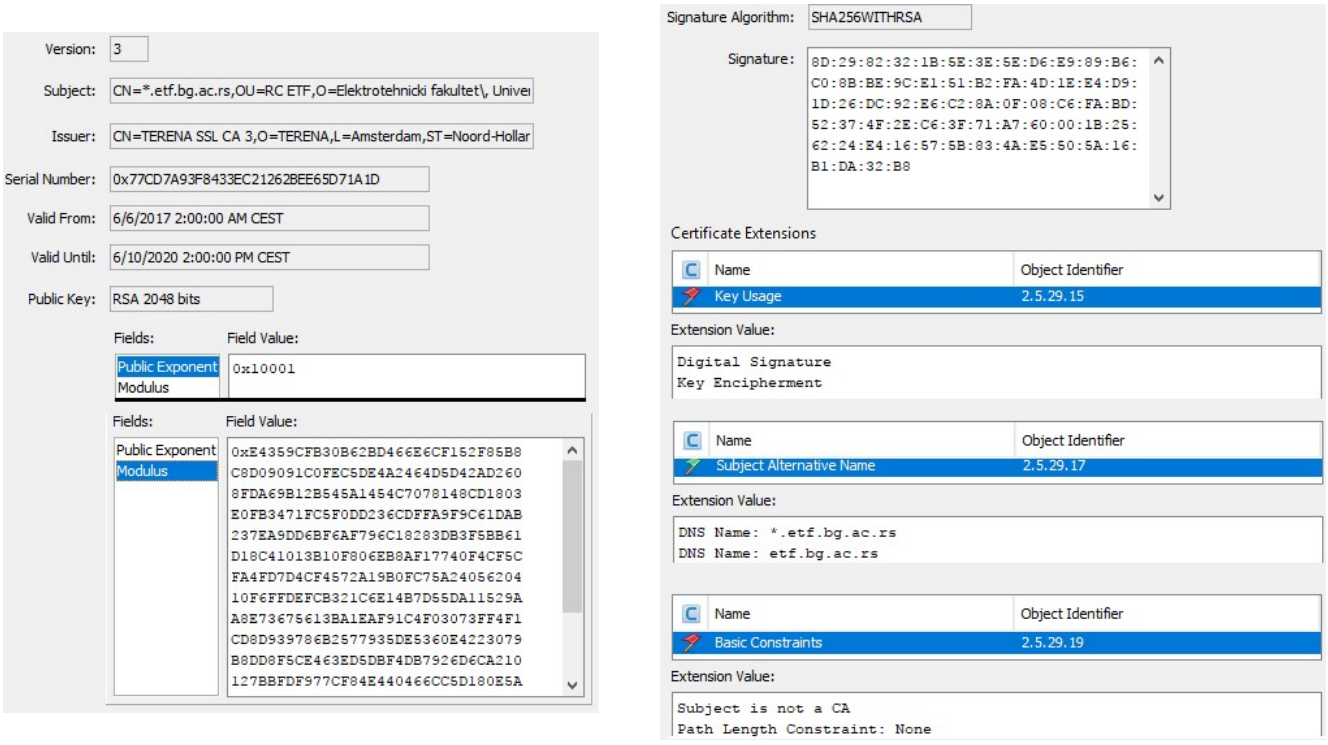
Ispit iz Zaštite podataka (13E113ZP, 13S114ZP) – integralno polaganje 19.06.2019.

1. (**20p**) Na slici je dat deo šeme za centralizovanu distribuciju sesijskog ključa. Dopuniti šemu i objasniti dopunjene delove poruka koje se razmenjuju između korisnika A i B i korisnika A i KDC-a. Čemu služe nonce vrednosti prikazane na šemi?



2. (**20p**) Skicirati i objasniti strukturu *DES* dešifrovanja bez detalja pojedinačnih rundi. Kako funkcioniše *3-DES* algoritam i zašto je postojala potreba za njegovim uvođenjem? Detaljno objasniti napad zbog kojeg *2-DES* algoritam nije bio adekvatna zamena *DES* algoritmu.

3. (**15p**) Na slici 1 dat je primer X509 sertifikata. Objasniti značenje i svrhu svih prikazanih polja u opštem slučaju (počev od *Version*, pa sve do *Certificate Extensions*), a zatim razmotriti vrednosti polja za konkretan sertifikat.



Slika 1. Primer X509 sertifikata

4. (**15p**) Koje se sve poruke i kojim redosledom razmenjuju između klijenta i servera kod uspostavljanja *TLS* sesije (*TLS Handshake*). Pretpostavite da je potrebna autentikacija i servera i klijenta.

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 180 minuta.*

Ispit iz Zaštite podataka (13E113ZP, 13S114ZP) – parcijalno polaganje 19.06.2019.

1. (**p**) Opisati faze i strukturu virusa, i navesti primer u pseudokodu. Opisati tehnike koje se koriste u zaštiti od virusa.

2. (**p**) Nacrtati šemu i ukratko objasniti kako se u *PGP*-u na strani pošiljaoca generiše poruka obezbeđujući tajnost i autentikaciju uz korišćenje prstena privatnih i javnih ključeva. Čemu služi prsten javnih ključeva i šta predstavlja jedan njegov ulaz? Ukratko objasniti svako polje u ovakvoj strukturi. Objasniti postupak i dati primer ubacivanja novog javnog ključa u prsten javnih ključeva korišćenjem poverenja.

3. (**p**) Kada pristupate sajtu *https://mail.google.com* razmena ključeva u okviru TLS handshake-a se vrši Ephemeral Diffie-Hellman metodom, a digitalni sertifikat postoji samo na strani servera mail.google.com.
    a) Opisati TLS handshake u ovom slučaju kroz opis redosleda slanja poruka i njihovog sadržaja. (80% poena)
    b) Na koji način se u ovoj razmeni ključeva sprečava man-in-the-middle napad? (20% poena)

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 180 minuta.*