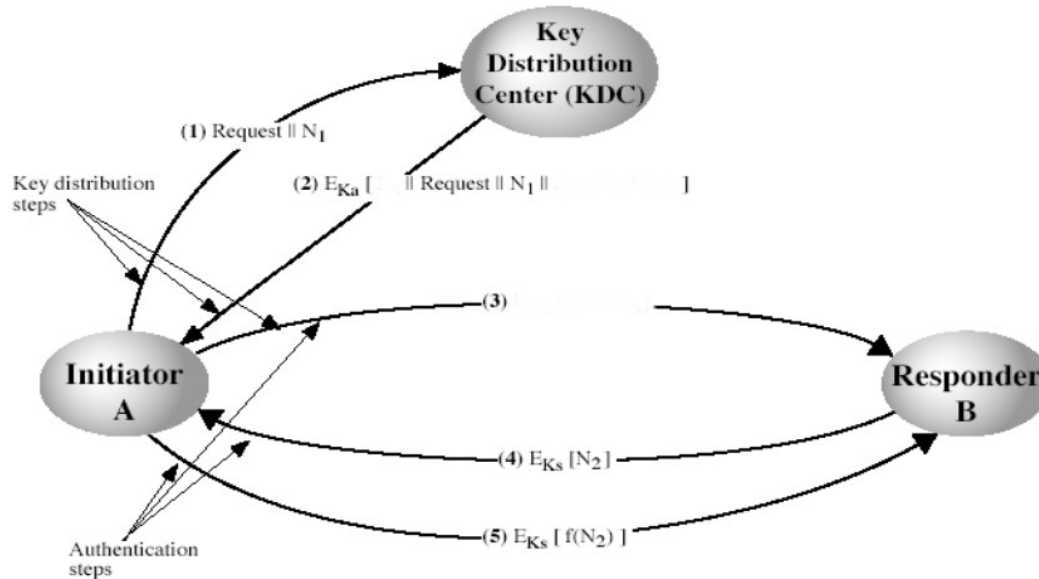


1. (20p) Na slici je dat deo šeme za centralizovanu distribuciju sesijskog ključa. Dopuniti šemu i objasniti dopunjene delove poruka koje se razmenjuju između korisnika A i B i korisnika A i KDC-a. Čemu služe nonce vrednosti prikazane na šemi?



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.

Version: 3

Subject: CN=\*.etf.bg.ac.rs,OU=RC ETF,O=Elektrotehnicki fakultet\, Univer

Issuer: CN=TERENA SSL CA 3,O=TERENA,L=Amsterdam,ST=Noord-Hollar

Serial Number: 0x77CD7A93F8433EC21262BEE65D71A1D

Valid From: 6/6/2017 2:00:00 AM CEST

Valid Until: 6/10/2020 2:00:00 PM CEST

Public Key: RSA 2048 bits

Fields:	Field Value:
Public Exponent	0x10001
Modulus	0xE4359CFB30B62BD466E6CF152F85B8C8D09091C0FEC5DE4A2464D5D42AD2E08FDA69B12B545A1454C7078148CD1803E0FB3471FC5F0DD236CDFFA9F9C61DAB237EA9DD6BF6AF796C18283DB3F5BB61D18C41013B10F806EB8AF17740F4CF5CFA4FD7D4CF4572A19B0FC75A2405620410FEFFDEFB321C6E14B7D55DA11529AA8E73675613BA1EAF91C4F03073FF4F1CD8D939786B2577935DE5360E4223079B8DD8F5CE463ED5DBF4DB7926D6CA210127BBDF977CF84E440466CC5D180E5A

Signature Algorithm: SHA256WITHRSA

Signature: 8D:29:82:32:1B:5E:3E:5E:D6:E9:89:B6:C0:8B:BE:9C:E1:51:B2:FA:4D:1E:E4:D9:1D:26:DC:92:E6:C2:8A:0F:08:C6:FA:BD:52:37:4F:2E:C6:3F:71:A7:60:00:1B:25:62:24:E4:16:57:5B:83:4A:E5:50:5A:16:B1:DA:32:B8

Certificate Extensions

Name	Object Identifier
Key Usage	2.5.29.15

Extension Value:

Digital Signature

Key Encipherment

Name	Object Identifier
Subject Alternative Name	2.5.29.17

Extension Value:

DNS Name: \*.etf.bg.ac.rs

DNS Name: etf.bg.ac.rs

Name	Object Identifier
Basic Constraints	2.5.29.19

Extension Value:

Subject is not a CA

Path Length Constraint: None

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 ovačjoj 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.