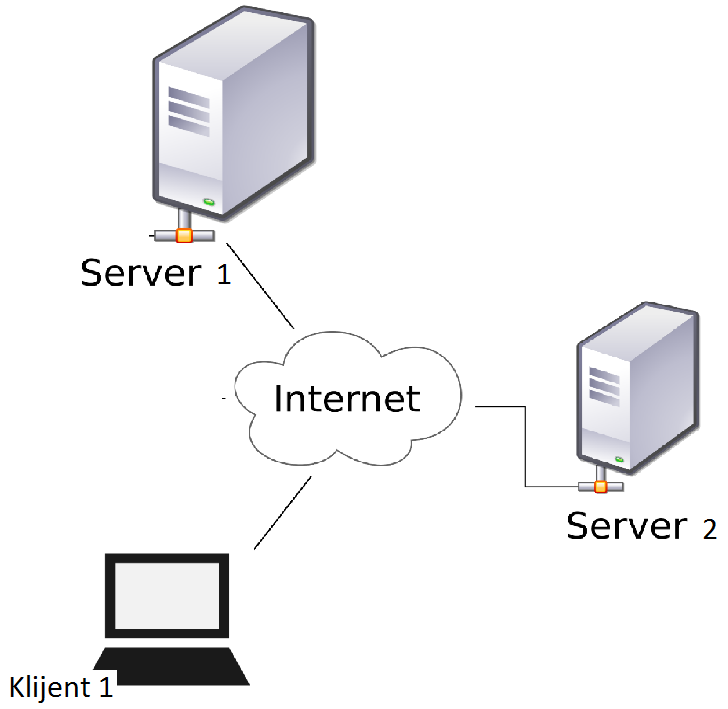
# **Prvi kolokvijum - Kriptologija 2**



**Zadatak**

U scenariju sa slike, na **Serveru 2** nalazi se generator za simetrične tajne ključeve koji će se koristiti za šifrovanje poruka između **Servera 1** i **Klijenta 1**.

**Zahtevi**

1. Kriptografski protokol između **Servera 1** i **Servera 2** treba da obezbedi servis za jednostranu autentifikaciju (**Server 2** zahteva autentifikaciju **Servera 1**) i servis tajnosti. Šemu protokola izraditi preko simetričnih kriptografskih algoritama.

Server 1 i Server 2 imaju simetricni kljuc KAB .Koristi se neki od algoritama za simetricno sfirovanje. (DES,AES,3DES). A zajednicki kljuc KAB  se moze preneti preko diffie-hellmana, kurirskom sluzbom ili slicno.

* 1. Server 1 se predstavlja Serveru 2 „Ja sam Server 1“
  2. Server 2 generise slucajnu vrednost R i salje je Serveru 1
  3. Server 1 sifruje simetricnim algoritmom slucajnu vrednost R i KAB i salje tako dobijeni sifrat salje Serveru 2.
  4. Server 2 desifruje sifrat koji je dobio od Servera 1 i verifikuje na osnovu izazova R koji je poslao u drugom koraku.

1. Kriptografski protokol između **Servera 1** i **Klijenta 1** treba da obezbedi uzajamnu autentfikaciju i bezbednu razmenu tajnog ključa generisanog na **Serveru 2** uz pomoć asimetričnih kriptografskih algoritama.

Ovde se koristi PFS. Perfektna tajnost unapred, i diffie – hellman. Sa obe strane treba da se nalaze slucajne vrednosti p,q,a,b (stim sto su a i b slucajno generisane zbog svezine kljuca ). Pored toga treba da postoji 2 para kljuceva, jedan za sifrovanje i jedan za potpis. U ovom slucaju ,Kc=gabmodp, je zajednicki simetricni kljuc.

* 1. Klijent 1 se javlja Serveru 1 „Ja sam Klijen 1“ i generise neku slucajnu vrednost RA
  2. Server 1 odgovara klijentu 1 sa slucajno generisanom vrednoscu RB i potom prvo sifruje ,{RA,gamodp}klijent1 Klijentovim javnim kljucem. A zatim sve to potpisuje svojim privatnim kljucem. [{RA,gbmodp}klijent1]server1
  3. Zatim Klijent 1 skida potpis uz pomoc serverovog javnog kljuca dolazi do sifrovanog dela i to skida uz pomoc svog privatnog kljuca. Na taj nacin je verifikovao server. Sada Klijent sifruje ne slican nacin , [{Rb,gamodp}server1]klijent1, sifruje svojim javnim kljucem Rb,gamodp i onda sve to potpisuje svojim privatnim. Zatim sve to salje Serveru 1.
  4. Server jedan uz pomoc klijentovog javnog kljuca skida potpis, zatim svojim privatnim kljucem desifruje i verifikuje klijent-a 1 na osnovu Rb koji je poslat kao izazov u drugom koraku.

1. U Cryptool-u simulirati komunikaciju izemeđu **Servera 1** i **Servera 2**.