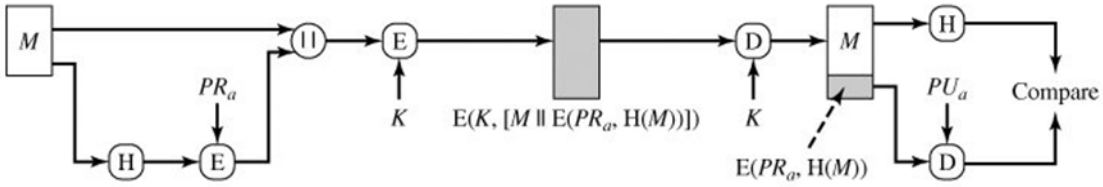
Ispit iz zaštite podataka (SI4ZP, MS1ZP) 03.09.2010.

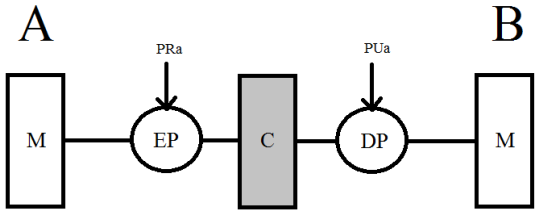
1. (**15p**) Koristeći *Playfair* algoritam za šifrovanje sa ključem: FAKULTE šifrovati poruku: ZASTITAPODATAKA. Koristiti engleski alfabet i slovo X za ispunu ako je potrebno.

2. (**20p**) Objasniti detaljno SSL *handshake* mehanizam u situaciji kada klijent ne poseduje sertifikat. Koje vrste sigurnosnih servisa se postižu korišćenjem ovog mehanizma i u kojim prilikama je pogodan za korišćenje?

3. (**20p**) Na slici je data šema direktnog digitalnog potpisa. Šta u ovoj šemi nedostaje da bi se ostvarila potpuna funkcionalnost digitalnog potpisa? Predložiti jednu šemu koja otklanja ovaj nedostatak. Na slici M označava osnovnu poruku, H hash funkciju, E operaciju kriptovanja sa simetričnim ključem K ili asimetričnim ključevima PR i PU, D operaciju dekriptovanja, a || konkatenaciju poruke.



4. (**20p**) Na slici je data šema za razmenu poruka između korisnika A (pošiljalac) i B (primalac) na siguran način. M predstavlja originalnu poruku, C je šifrovana poruka, EP je šifrovanje pomoću javnog ključa, DP je dešifrovanje pomoću javnog ključa, PRa je privatni ključ korisnika A, PUa je javni ključ korisnika A. a) Da li ova šema obezbeđuje tajnost ili autentikaciju i zašto? b) Na koji način biste proširili šemu tako da obezbedi i tajnost i autentikaciju istovremeno, uz šifrovanje koje je na raspolaganju (šifrovanje se može upotrebiti proizvoljan broj puta, ali se ne sme uvoditi nova vrsta šifrovanja)? Nacrtati i objasniti. c) Koje su mane ove šeme, zbog kojih se i ne bi mogla koristiti u praksi i na koji način je to rešeno kod PGP šeme?



5. (**15p**) Napraviti konsolidovani model zaštite pomoću uloga (hijerarhija uloga i ograničenja) za sistem opisan u nastavku. Uvesti razumne pretpostavke za resurse sistema u skladu sa datim opisima. Na fakultetu postoje profesori, asistenti i studenti. Profesor može biti izabran za dekana i u tom slučaju, ne može biti i prodekan. Profesor može biti izabran za prodekana. Asistent može biti i student master studija ili student doktorskih studija. U slučaju da je asistent student master studija, ne može predavati na predmetima master studija. Student može biti student osnovnih studija, student master studija i student doktorskih studija. Student osnovnih studija prati predavanja i polaže ispite. Student master studija prati predavanja, odlazi na konsultacije, radi projekte i polaže ispite. Student doktorskih studija odlazi na konsultacije, piše naučne radove i polaže ispite. Asistent ne može predavati na predmetima doktorskih studija. Asistent drži nastavu, vodi evidenciju o prisustvu studenata časovima i održava konsultacije. Profesor ima iste obaveze kao asistent i pored toga održava ispite i ocenjuje studente. Prodekan pored obaveza kao profesor, još vodi evidenciju o održavanju nastave, rasporedu časova, opterećenosti profesora i asistenata i sl. Dekan pored obaveza profesora vodi računa o finansijama, prilivima iz budžeta i od školarina, rashodima na održavanje i osavremenjavanje prostorija fakulteta i sl.

Trajanje ispita 3 sata