Kratki uvod u kriptografiju
Kako uspostaviti sigurnu komunikaciju preko nesigurnog komunikacijskog kanala? Metode za rješavanje ovog problema proučava znanstvena disciplina s c koja se zove kriptografija (ili tajnopis). Osnovni zadatak kriptografije je omogu´avanje komunikacije dvaju osoba (zovemo ih pošiljalac i primalac c s - u kriptografskoj literaturi za njih su rezervirana imena Alice i Bob) na takav način da tre´a osoba (njihov protivnik - u literaturi se najče´e zove c c c sc Eve ili Oskar), koja može nadzirati komunikacijski kanal, ne može razumjeti z z njihove poruke. Poruku koju pošiljalac želi poslati primaocu zovemo otvoreni tekst. Pošis z s ljalac transformira otvoreni tekst koriste´i unaprijed dogovoreni ključ K. Taj c c se postupak zove šifriranje, a dobiveni rezultat šifrat. Nakon toga pošiljalac s s s pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškuju´i s s s c može saznati sadržaj šifrata, ali kako ne zna ključ, ne može odrediti otvoreni z z s c z tekst. Za razliku od njega, primalac zna ključ kojim je šifrirana poruka, pa c s može dešifrirati šifrat i odrediti otvoreni tekst. z s s
Ove pojmove ´emo formalizirati u sljede´oj definiciji. c c Definicija 1.1. Kriptosustav je uredena petorka (P, C, K, E, D), gdje je P 1

konačan skup svih otvorenih tekstova, C konačan skup svih šifrata, K konačan c c s c skup svih mogu´ih ključeva, E skup svih funkcija šifriranja i D skup svih c c s funkcija dešifriranja. Za svaki K ∈ K postoji ek ∈ E i odgovaraju´i dK ∈ s c D. Pritom su eK : P → C i dK : C → P funkcije sa svojstvom da je dK (eK (x)) = x za svaki x ∈ P.
Shema koju smo u uvodu opisali predstavlja tzv. simetrični ili konvenc cionalni kriptosustav. Funkcije koje se koriste za šifriranje eK i dešifriranje s s dK ovise o ključu K kojeg Alice i Bob moraju tajno razmjeniti prije same c komunikacije. Kako njima nije dostupan siguran komunikacijski kanal, ovo može biti veliki problem. z Godine 1976. Diffie i Hellman su ponudili jedno mogu´e rješenje probc s lema razmjene ključeva, zasnovano na činjenici da je u nekim grupama poc c tenciranje puno jednostavnije od logaritmiranja. O ovom algoritmu ´emo c detaljnije govoriti u jednom od sljede´ih poglavlja. c Diffie i Hellman se smatraju začetnicima kriptografije javnog ključa. Ideja c c javnog ključa se sastoji u tome da se konstruiraju kriptosustavi kod kojih c bi iz poznavanja funkcije šifriranja eK bilo praktički nemogu´e (u nekom s c c razumnom vremenu) izračunati funkciju dešifriranja dK . Tada bi funkcija c s eK mogla biti javna. Dakle, u kriptosustavu s javnim ključem svaki korisc nik K ima dva ključa: javni eK i tajni dK . Ako Alice želji poslati Bobu c z poruku x, onda je ona šifrira pomo´u Bobovog javnog ključa eB , tj. pošalje s c c s Bobu šifrat y = eB (x). Bob dešifrira šifrat koriste´i svoj tajni ključ dB , s s s c c dB (y) = dB (eB (x)) = x. Uošimo da Bob mora posjedovati neku dodatnu c informaciju (tzv. trapdoor - skriveni ulaz) o funkciji eB , da bi samo on mogao izračunati njezin inverz dB , dok je svima drugima (a posebno Eve) to c nemogu´e. Takve funkcije čiji je inverz teško izračunati bez poznavanja nekog c c s c dodatnog podatka zovu se osobne jednosmjerne funkcije.