500
Najpoznatiji algoritmi simetrične kriptografije su: DES (Data Encryption Standard)
sa ključem dužine od 56 bita,3DES sa ključem dužine od 168 bita, RC2 i RC4 (Ron's Ciphers)
sa ključevima od 40 ili 128 bita, CAST (Carlisle Adams i Stafford Tavares) 40, 64, 80 ili 128
bita, IDEA (International Data Encryption St andard) 128 bita i AES (Advanced Encryption
Standard) - Rijndael 128, 192 ili 256 bita. Tajnost d okumenta zavisi od ta jnosti kriptografskog
ključa i njegove dužine, dok šifrovan dokument može da se šalje i po nezaštićenom kanalu
s obzirom na to da sadržaj dokumenta može da sazna samo onaj korisnik koji poseduje
kriptografski ključ kojim je dokument šifrovan. Međutim, problem je što zaštićen
kanal praktično i ne postoji, a ukoliko bi i postojao postavlja se pitanje zašto tim
zaštićenim kanalom korisnici ne bi razmenjivali dokume nte u kom slučaju ne bi ni
postojala potreba za šifrovanjem. Ukoliko je N broj
korisnika koji žele da razmenjuju šifrovana d okumenta po principu "svako sa svakim",
tada se ukupan broj potrebnih ključeva K izračunava po sledećoj formuli:
2
NN
K
2 –
= .
SIMETRIČNA KRIPTOGRAFIJA
Osnovna osobina simetrične kriptografije ili kriptografije sa jednim ključem
(Symmetric or Single Key Cryptog raphy) je da se isti ključ koristi i za šifrovanje i za
dešifrovanje dokumenta (slika 3). Osoba B, koja osobi A želi poslati tajnu poruku
enkriptuje tu svoju poruku s ključem koju je osoba A javno objavila te joj takvu poruku
pošalje (recimo preko e-mail servisa). Korisnici koji učestvuju u komunikaciji
razmenjuju isključivo javne
ključeve, dok se tajni ključevi ne pr enose mrežom niti na bilo koji drugi način
razmenjuju između korisnika. Korisnik kome je
4
šifrovan dokument namenjen, posle preuzi manja šifrovanog dokumenta, vrši njegovo
dešifrovanje korišćenjem svog tajnog ključa koji je par javnomključu kojim je taj dokument
šifrovan. Ukoliko neko
želi da pošalje šifrovan dokument tom korisnik u, on korišćenjem dostupnog javnog ključa
vrši šifrovanje dokumenta a zatim mu tako šifrovan dokument prosleđuje