TEORIJA BROJEVA U KRIPTOGRAFIJI

1. zadaća

17. 12. 2003.

1. Neka je n prirodan broj koji je produkt dva prosta broja p i q. Pokažite kako se iz poznavanja brojeva n i $\varphi(n)$ mogu izračunati brojevi p i q. Metodu ilustrirajte na primjeru $n = 30700619$ i $\varphi(n) = 30689496$.

2. Otvoreni tekst na hrvatskom jeziku šifriran je pomoću RSA kriptosustava čiji je javni ključ $(n, e) = (30967, 17)$, na sljedeći način. Najprije su slovima pridružene odgovarajuće brojevne vrijednosti: A = 0, B = 1, C = 2, Č = 3, ... , Z = 28, Ž = 29. Potom su tri po tri susjedna slova otvorenog teksta "kodirana" kao elementi od $\mathbb{Z}_n$, kao što pokazuju ovi primjeri:

   $$DAN = 5 \cdot 30^2 + 0 \cdot 30 + 18 = 4518, \quad PUT = 21 \cdot 30^2 + 26 \cdot 30 + 25 = 19705.$$

   Konačno su ovako dobiveni elementi od $\mathbb{Z}_n$ šifrirani pomoću RSA kriptosustava s gore navedenim parametrima n i e.

   Faktorizirajte broj n (poznato je da je produkt dva "bliska" prosta broja), te dešifrirajte šifrat

   $$23144, \quad 14420, \quad 19603, \quad 27580.$$

3. Objasnite zašto nije dobro koristiti RSA kriptosustav tako da se šifrira slovo po slovo otvorenog teksta (nakon zamjene A = 0, B = 1, ... , Ž = 29). Kako se poruke šifrirane na taj način mogu jednostavno "razbiti" čak i u slučaju da je modul n vrlo velik broj kojeg ne znamo faktorizirati? Ovo je primjer tzv. "protocol failure", tj. pogrešnog korištenja, inače sigurnog kriptosustava.

4. U Rabinovom kriptosustavu s parametrima $(n, p, q) = (6416441, 2131, 3011)$, dešifrirajte šifrat $y = 4484965$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnje tri znamenke međusobno jednake.

5. Neka su parametri u ElGamalovom sustavu $p = 31847$, $\alpha = 5$, $a = 7899$, $\beta = 18074$. Dešifrirajte šifrat

   $$(6841, 10449), \quad (8006, 21703).$$

   U otvorenom tekstu, svaki element $x \in \mathbb{Z}_n$ predstavlja tri slova, kao u 2. zadatku.

6. Zadan je Merkle-Hellmanov kriptosustav s parametrima

   $$v = (2, 5, 11, 23, 45, 91), \quad p = 181, \quad a = 111, \quad t = (41, 12, 135, 19, 108, 146).$$

   Dešifrirajte šifrat $y = 296$.

Rok za predaju zadaće je 14.1.2004.

Andrej Dujella