SEMINAR IZ KRIPTOGRAFIJE

RSA (nadaljevanje)

predava:

Arijana Žitnik (IMFM)

23. marec 1998

Na zadnjem seminarju:

- Miro Masnoglav (nadaljevanje):
  Sistem RSA in faktorizacija
  - implementacija RSA
  - probabilistično testiranje praštevilčnosti
  - A.J.: Gaussov izrek
    o kvadratni recipročnosti
  - napadi na RSA
- rešitve nalog 3. poglavja

Današnji načrt

- Arijana Žitnik konča s 4. pogl.
  - Rabinov kriptosistem
  - algoritmi za faktorizacijo
- rešitve nalog 4. poglavja
- A.J.: dodatne naloge

O sistemu RSA in faktorizaciji bo nadaljevala

Arijana Žitnik (IMFM)

Reševanje domačih nalog iz 4. poglavja:

...

Dodatne naloge:

1. Dokaži, da imamo pri poljubnem RSA sistemu vsaj 9 čistopisov za katere je $E_k(M) = M$.

2. Naj bo

$$n = 62414266058669410144629\backslash \\ 13081475818058256112798\backslash \\ 51037995772020202145871.$$

Preveri ali n je ali ni praštevilo (lahko uporabiš MAPLE/MATEMATICA). Dokaži svoj odgovor in opiši kako bi lahko jaz (zlahka) preveril tvoj dokaz. Kopijo števila n boste našli na domači strani.

3. Spomnimo se naslednjih pravil:
če je p liho praštevilo, potem

- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
- Če je q liho praštevilo, je

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

Naj bo $n \geq 3$ liho število.

(i) Pokaži, da za lihi števili n_1 in n_2 velja:

$$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \pmod 2.$$

Iz tega izpelji $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(ii) Pokaži, da za lihi število n_1 in n_2 velja

$$\frac{n_1^2 n_2^2 - 1}{8} \equiv \frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \pmod 2.$$

Iz tega izpelji $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

(iii) Dokaži, da za liho naravno število a, ki je tuje številu n, velja

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{(a-1)(n-1)/4}.$$

4. Naj bo $n = pq$, kjer sta p in q različni lihi praštevili ter naj bo

$$J_n = \{a \in Z_n^* \mid \left(\frac{a}{n}\right) = 1\}.$$

Dokaži $QR_n \subseteq J_n$.

Dokaži $|QR_n| = \frac{1}{2}|J_n|$.

4. Naj bo n produkt dveh različnih praštevil p in q, ki sta približno enake velikosti (tj. $p-q$ je majhno število). Opiši hiter postopek za faktorizacijo števila n.

Do naslednjega tedna

- preberite 5. poglavje (do str. 190)

nadaljujte z reševanjem nalog 4. poglavja

Stinsonovega učbenika
Cryptography, Theory and Practice

Prihodnjič (6.apr): A.J. prične s 5. poglavjem

- Drugi javni kriptosistemi
  ElGamalov kriptosistem in diskretni logaritem

Čez 21 dni (20. apr) bo seminar vodil T. Klobučar:
Bojan Barlič konča s 5. poglavjem:

- Markle-Hellmanov sistem (nahrbtnik)
- McEliece sistem (error-correcting codes)