SEMINAR IZ KRIPTOGRAFIJE

RSA

predava:

Miro Masnoglav (MORS)

16. marec 1998

Na zadnjem seminarju:

- Saša Habič: DES (nadaljevanje in konec)
  diferencialna kripto-analiza
  – uvod
  – napad na DES s tremi iteracijami
  – napad na DES s šestimi iteracijami
  – drugi primeri diferencialne kripto-analize
- A.J.: še malo o DES-u
  – učinkovito iskanje DES ključa
  – 3-DES, DESX
  – drugi simetrični sistemi
- reševanje nalog iz 1. poglavja
  (ostale so še naloge 1.2, 1.4, 1.11)

Današnji načrt

- Miro Masnoglav:
  Sistem RSA in faktorizacija
  – uvod
  – teorija števil (A.J. o razširjenem Evklidovem algoritmu)
  – kriptosistem RSA
- rešitvi nalog 1.2 (N. Jukić) in 3.2. (J. Blatnik)

O sistemu RSA in faktorizaciji bo predaval
Miro Masnoglav (MORS)

Evklidov algoritem in reševanje Diofantske enačbe :

$$ax + by = d, \text{ kjer je } D(a,b)|d.$$

Evklidov algoritem je zasnovan na dejstvu, da iz $k|a$ in $k|b$ sledi $k|a-b$.
Recimo, da smo našli eno rešitev in da je $D(a,b) = 1$:

$$ax_0 + by_0 = d.$$

Potem velja:

$$x = x_0 - kb, \quad y = y_0 + ka, \quad \text{kjer je } k \in \mathbb{Z}.$$

Eno rešitev najdemo z razširjenim Evklidovim algoritmom:

Privzemimo, da je $a > b$ in zapišimo zgornjo enačbo malo bolj splošno (z zaporedji):

$$ap_i + bq_i = r_i.$$

Poiščimo dve trivialni rešitvi:
$p_1 = 1$, $q_1 = 0$, $r_1 = a$ in
$p_2 = 0$, $q_2 = 0$, $r_2 = b$.

Iz rekurzije:

$$r_{i+1} = r_i - s_i r_{i-1}$$

(kjer je s_i izbran tako, da je $r_{i+1} < r_i$) izpeljemo še

$$p_{i+1} = p_i - s_1 p_{i-1} \quad \text{in} \quad q_{i+1} = q_i - s_1 q_{i-1}.$$

Ko računamo a^{-1} (po modulu praštevila p), računamo samo r_i ter p_i (ne pa tudi q_i).
Zgled za razširjeni algoritem:

$4864 = 1{\cdot}3458+1406$	$p_2 := p_1 - 1{\cdot}p_0 = 1$
$3458 = 2{\cdot}1406+646$	$p_3 := p_2 - 2{\cdot}p_1 = -2$
$1406 = 2{\cdot}646+114$	$p_4 := p_3 - 2{\cdot}p_2 = 5$
$646 = 5{\cdot}114+76$	$p_5 := p_4 - 5{\cdot}p_3 = -27$
$114 = 1{\cdot}76+38$	$p_6 := p_5 - 1{\cdot}p_4 = 32$
$76 = 2{\cdot}38+0.$	$p_7 := p_6 - 2{\cdot}p_5 = -91$

$$
\begin{array}{ll}
4864 = 1 \cdot 3458 + 1406 & p_2 = 1 \quad q_2 = -1 \\
3458 = 2 \cdot 1406 + 646 & p_3 = -2 \quad q_3 = 3 \\
1406 = 2 \cdot 646 + 114 & p_4 = 5 \quad q_4 = -7 \\
646 = 5 \cdot 114 + 76 & p_5 = -27 \quad q_5 = 38 \\
114 = 1 \cdot 76 + 38 & p_6 = 32 \quad q_6 = -45 \\
76 = 2 \cdot 38 + 0. & p_7 = -91 \quad q_7 = 128
\end{array}
$$

$$4864 \cdot (-91) + 3458 \cdot (128) = 38.$$

Reševanje domačih nalog iz III. poglavja:

Do naslednjega tedna

- preberite 4. poglavje (do str. 144)

- končajte z reševanjem nalog 3. poglavja in
pričnite z reševanjem nalog 4. poglavja

Stinsonovega učbenika
Cryptography, Theory and Practice

Prihodnjič: Miro Masnoglav nadaljuje s 4. poglavja:

- implementacija RSA
- probabilistično testiranje praštevilčnosti
- napadi na RSA

Čez 14 dni: Arijana Žitnik konča s 4. pogl.

- Rabinov kriptosistem
- algoritmi za faktorizacijo