SEMINAR IZ KRIPTOGRAFIJE

Klasična kriptografija

Aleksandar Jurišić

IMFM

23. februar 1998

Na zadnjem seminarju:

- predstavitev seminarja
- o kriptografiji na splošno
- na kratko o zgodovini kriptografije
- reševanje 20 let stare naloge iz Preseka
- predstavitev klasične kriptografije
  - zamenjalni (Cezarjev) tajnopis
  - afini tajnopis
  - Vigenerjev tajnopis (glej primer: Ex.11.1)
  - Hillov tajnopis
- razbijanje klasičnih tajnopisov (do str. 36)

Današnji načrt

- klasična kriptografija
- razbijanje klasičnih tajnopisov
- rešitev domače naloge o Siru Johnu
- rešitev domače naloge iz Preseka
- domače naloge iz prvega poglavja
- R. Petek: simetrična kriptografija in DES

Klasična kriptografija

- zamenjalni [substitucijski] tajnopis
  (zamični [šiftni] tajnopis,...)
- afini tajnopis (ponovitev kongruenc)
- Vigenerejev tajnopis
- Hillov tajnopis
- tokovni tajnopisi [stream ciphers]

Tokovni tajnopisi

Naj bo $x_1x_2\ldots$ čistopis.

Doslej smo obravnavali kriptosisteme z enim samim ključem in tajnopis je imel naslednjo obliko.

$$\mathbf{y} = y_1y_2\ldots = e_K(x_1)e_K(x_2)\ldots$$

Takemu tajnopisu pravimo **bločni tajnopis** (block cipher).

Posplošitev: iz enega ključa $K \in \mathcal{K}$ napravimo zaporedje (tok) ključev. Naj bo f_i funkcija, ki generira i-ti ključ:

$$z_i = f_i(K, x_1, \ldots, x_{i-1}).$$

Z njim izračunamo:

$$y_i = e_{z_i}(x_i) \qquad \text{in} \qquad x_i = d_{z_i}(y_i).$$

Bločni tajnopis je poseben primer tokovnega tajnopisa (kjer je $z_i = K$ za vse $i \geq 1$).

Tokovni tajnopis je sedmerica $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{L},\mathcal{F},\mathcal{E},\mathcal{D})$ za katero velja:

1. $\mathcal{P}$ je končna množica možnih čistopisov
2. $\mathcal{C}$ je končna množica možnih tajnopisov
3. $\mathcal{K}$ je končna množica možnih ključev.
4. $\mathcal{L}$ je končna množica tokovne abecede.
5. $\mathcal{F} = (f_1, f_2, \ldots)$ je generator toka ključev:
$$f_i : \mathcal{K} \times \mathcal{P}^{i-1} \longrightarrow \mathcal{L} \quad \text{za } i \geq 1$$
6. Za vsak ključ $z \in \mathcal{L}$ imamo šifrirni ($e_z \in \mathcal{E}$) in dešifrirni ($d_z \in \mathcal{D}$) postopek, tako da je $d_z(e_z(x)) = x$ za vsak $x \in \mathcal{P}$.

Za šifriranje čistopisa $x_1 x_2 \ldots$ zaporedno računamo

$$z_1, y_1, z_2, y_2, \ldots,$$

za dešifriranje tajnopisa $y_1 y_2 \ldots$ pa zaporedno računamo

$$z_1, x_1, z_2, x_2, \ldots.$$

Tokovni tajnopis je **periodičen** s periodo d kadar, je $z_{i+d} = z_i$ za vsak $i \geq 1$ (poseben primer: Viginerejev tajnopis).

Začnimo s ključi $(k_1, \ldots, k_m)$ in naj bo $z_i = k_i$ za $i = 1, \ldots, m$. Definiramo linearno rekurzijo stopnje m:

$$z_{i+m} \;=\; z_i \;+\; \sum_{j=1}^{m-1} c_j \, z_{i+j} \text{ mod } 2,$$

kjer so $c_1, \ldots, c_{m-1} \in \mathbb{Z}_2$ vnaprej določene konstante.

Za ustrezno izbiro konstant $c_1, \ldots, c_{m-1} \in \mathbb{Z}_2$ in neničelen vektor $(k_1, \ldots, k_m)$ lahko dobimo tokovni tajnopis s periodo $2^m - 1$.

Hitro lahko generiramo tok ključev z uporabo LFSR (**Linear Feedback Shift Register**).
V zamičnem registru začnemo z vektorjem $(k_1, \ldots, k_m)$. Nato na vsakem koraku naredimo naslednje:

1. k_1 dodamo toku ključev (za XOR),
2. $k_2, \ldots, k_m$ pomaknemo za eno v levo,
3. 'nov' ključ k_m izračunamo z

$$\sum_{j=0}^{m-1} c_j \, k_{j+1} \quad \text{(to je ``linear feedback'')}.$$

Primer:

$c_0 = 1,\ c_1 = 1,\ c_2 = 0,\ c_3 = 0,$

torej je $k_{i+4} = k_i + k_{i+1}$.

Izberimo $k_0 = 1,\ k_1 = 0,\ k_2 = 1,\ k_3 = 0$.

Potem je $k_4 = 1,\ k_5 = 1,\ k_6 = 0,\ \ldots$.

Naj bo $\mathbf{k} = (k_0, k_1, k_2, k_3)^t$ in

$$A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Torej je $A(\mathbf{k}) = (k_1, k_2, k_3, k_4)^t$,
$A^2(\mathbf{k}) = A(k_1, k_2, k_3, k_4)^t = (k_2, k_3, k_4, k_5)^t$
...
$A^i(\mathbf{k}) = (k_i, k_{i+1}, k_{i+2}, k_{i+3})^t$.

Najdaljša možna perioda je 15.

Enkrat dobimo:

$$A^i(\mathbf{k}) = A^j(\mathbf{k})$$

in ker je A obrnljiva

$$A^{i-j}(\mathbf{k}) = \mathbf{k}$$

Karakteristični polinom matrike A je

$$f(x) = 1 + x + x^4.$$

Ker je $f(x)$ nerazcepen, je $f(x)$ tudi minimalni polinom matrike A.

Red matrike A je najmanjše naravno število s, tako da je $A^s = I$. Naj bo e najmanjše naravno število, tako da $f(x)|(x^e - 1)$.
Potem je $e = s$.

$$\begin{aligned} 1 + x^{15} &= (x+1)(x^2+x+1)(x^4+x+1) \\ &\quad (x^4+x^3+1)(x^4+x^3+x^2+x+1). \end{aligned}$$

Splošno: če hočemo, da nam rekurzija stopnje m da periodo $2^m - 1$, potem si izberemo nerazcepen f.
Analiza je neodvisna od začetnega neničelnega vektorja.

Ponovimo od zadnjič:

Dokler niste razbili (rešili) nobenega kripto-sistema ne sestavljajte novega.

Dešifriranje klasičnih tajnopisov

Držali se bomo **Kerckhoffovega principa**, ki pravi da “nasprotnik”

pozna kriptosistem, ki ga uporabljamo.

Ločimo naslednje nivoje napadov na kriptosisteme:

1. **samo tajnopis:** nasprotnik ima del tajnopisa
2. **poznani čistopis:** nasprotnik ima del čistopisa ter ustrezen tajnopis
3. **izbrani čistopis:** nasprotnik ima začasno na voljo šifrirno mašinerijo ter za izbrani $x \in \mathcal{P}$ konstruira $e(x)$
4. **izbrani tajnopis:** nasprotnik ima začasno na voljo dešifrirno mašinerijo ter za izbrani $y \in \mathcal{C}$ konstruira $d(y)$

Hillov tajnopis (1929):

Naj bo m neko naravno število in naj bo

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m.$$

Za K vzemimo obrnljivo $m \times m$ matriko in definirajmo

$$e_K(x) = xK \quad \text{in} \quad d_K(y) = yK^{-1},$$

pri čemer so vse operacije opravljene v $\mathbb{Z}_{26}$.

Dešifriranje Hillovega tajnopisa:

Predpostavimo, da je nasprotnik določil m, ki ga uporabljamo, ter se dokopal do m različnih parov m-teric (2. stopnja – poznan čistopis):

$$x_j = (x_{1,j}, x_{2,j}, ..., x_{m,j}), \;\; y_j = (y_{1,j}, y_{2,j}, ..., y_{m,j}),$$

tako da je $y_j = e_K(x_j)$ za $1 \leq j \leq m$.

Za matriki $X = (x_{i,j})$ in $Y = (y_{i,j})$ dobimo matrično enačbo $Y = XK$.

Če je matrika X obrnljiva, je $K = YX^{-1}$.

Za Hillov tajnopis lahko uporabimo tudi 1. stopnjo napada (samo tajnopis), glej nalogo 1.6.

Koliko ključev imamo na voljo v primeru Hillovega tajnopisa? Glej nalogo 1.2.

Za afino-Hillov tajnopis glej nalogo 1.5.

Kriptoanaliza LFSR tokovnega tajnopisa: zopet lahko uporabimo poznan čistopis, glej nalogo 1.9.

Anglija: Sir John dobi sporočilo: Worthie Sir John:- Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honor, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command. - R.T.

"Med vrsticami" vam uspe prebrati:
"PANEL AT EAST END OF CHAPEL SLIDES"
če berete samo tretje znake za ločili.

Rešitev naloge iz Preseka:
glej Presek V/3, str. 144.

Ali se v besedilu skriva beseda "sporočilo"? Na misel nam pride najprej beseda, ki se je ponovila dvakrat: 03CWC%J(-. Vidimo, da njena samoglasniška razporeditev ustreza samoglasniški razporeditvi v besedi "sporočilo". Od tod takoj izpeljemo, da je:

J+ ?H = in je

saj je lahko le tako beseda D-?+- smiselna:

D-?+- = tajna

Od tu naprej ni težko razvozlati sporočilo, ki pravi:

VERJETNO STE ŽE SAMI UGOTOVILI
DA JE LAŽJE RAZVOZLJATI DALJŠA
SPOROČILA ZATO MORAJO BITI
TAJNA SPOROČILA KRAJŠA IN
JE TREBA POGOSTO MENJATI
TAJNO PISAVO

Do naslednjega tedna

- začnite brati 3. poglavje (str. 70)
(2. poglavje bomo zaenkrat izpustili),

- končajte z reševanjem nalog iz 1. poglavja
(str. 39-43),

Stinsonovega učbenika
Cryptography, Theory and Practice