Šifrování

Petr Šimeček

Na první přednášce si povíme něco o historii šifer, prodiskutujeme nejběžnější šifry (substituční, translační…) a ukážeme si jejich slabá místa. Nejzajímavější částí přednášky bude řešení ruzných netriviálních problémků (jak házet korunou po telefonu, jak „dokonale“ šifrovat, jak ukázat, že něco umíme dokázat, aniž bychom to dokázali…).

Druhá přednáška je na první zcela nezávislá. Budeme se bavit o systémech s veřejným klíčem (především o RSA).

Užitečné triky z kryptoanalýzy

- *Četnosti znaků + četnosti bigramů (dvojhlásek).*
  Viz tabulky na straně č. 24.
- *Odlišení náhodného a nenáhodného textu.*
  $\kappa = \sum_{i=1}^{k} ({p_i}^2)$, kde p_i je počet výskytu znaku i ku počtu znaků zkoumaného textu.
  $\kappa(\text{čeština}) = 0,0583$.
  $\kappa(\text{angličtina}) = 0,0661$.
  $\kappa(\text{němčina}) = 0,0762$.
  $\kappa(\text{náhodný text}) = \frac{1}{26} = 0,0385$.
- *Periodičnost* (posun podle hesla) - stačí uhádnout délku hesla.

$$r \cong \frac{0,0198 \cdot n}{\kappa \cdot (n-1) - 0,0385 \cdot n + 0,0583}$$

kde n je délka zkoumaného textu.
- *Další triky.*

Výrazně vám ulehčí práci, pokud znáte metodu šifrování, pokud uhádnete oslovení či podpis (nebo víte, že v textu je obsaženo nějaké slovo). Stojí za to zkoumat „zvláštní“ slova (krátká nebo se stejnými písmeny na začátku a na konci nebo slova s F,G,Q,W,X).

Substituční šifry

• *Posuvné o konstantu* - posouvám, až dostanu, co chci.
• *Proházená abeceda* - využiji četnosti písmen, bigramů, krátkých slov…
• *Posuvné o heslo* - uhádneme délku hesla (vzorec, opakující se skupiny), poté řešíme stejně jako v předchozím případě.

Translační šifry

• *Obyčejná* - odhalím délku hesla, potom text po „proužcích“ permutuji, ideální využití pravděpodobnosti bigramů.
• *Různá zesložitění* - metoda plukovníka Roche, dvě hesla…
• *Mřížka*.

Zajímavé problémky

• Jak chránit zprávu pomocí šumu?
• Existuje „dokonalá“ šifra?
• Jak házet korunou po telefonu?
• Jak šifrou reprezentovat trezor, jenž jde otevřít k lidmi z n?
• Jak funguje login v počítači?
• Jak ukázat, že něco umím dokázat, aniž bych to dokázal?

Tabulky a kódy

Do tabulky se zapíší hesla, hlásky, dvojhlásky a potom se odkazuje na řádek a sloupec.

Systémy s veřejným klíčem

„Odemykací“ klíč se liší od zamykacího klíče a nelze jej z něj odvodit. Obvykle bývá možné „odemknout a pak teprve zamknout“.

Výhody:

• Konec nebezpečí spojeného s dopravou klíče.
• Vyřešen problém autentifikace.

Matematické pozadí RSA

- $\binom{p}{a} \equiv 0 \pmod{p},\ a \notin \{0, a\}$.
- $(a+b)^p \equiv a^p + b^p \pmod{p}$.
- $c^{p-1} \equiv 1 \pmod{p},\ p$ nedělí c.
- $c^{\varphi(n)} \equiv 1 \pmod{n},\ (c, n) = 1$.

Algoritmus RSA

Podstata - pro dostatečně velké N je prakticky nemožné zjistit rozklad N na prvočísla. Naopak, pokud mám nějaké docela velké p, snadno zjistím, zda se jedná či nejdená o prvočíslo.

- Zvolíme p, q velká prvočísla, $N = p \cdot q$, $\varphi(N) = (p-1) \cdot (q-1)$.
- Nalezneme s nesoudělné s N.
- Spočítáme t: $s \cdot t \equiv 1 \pmod{\varphi(N)}$.
- Zašifrování bloku $W \equiv Z^s \pmod{N}, W < N$.
- Odšifrování bloku $Z \equiv W^t \equiv (Z^s)^t \equiv Z^{s \cdot t} \equiv Z \pmod{N}$.