

SKÚŠKA Z KRYPTOLÓGIE 21.5.2007

ZDARMA NÁZNAKY RIEŠENÍ

spísal Lukáš Poláček

1. Nech $n = pq$ je verejný modul, e je verejný kľúč a d je súkromný kľúč RSA inštancie. Platí $e \mid (p-1)(q-1) - 1$ a $d = \frac{(p-1)(q-1)(e-1)+1}{e}$. Dokážte, že dešifrovanie bude korektné.

Riešenie: Stačí ukázať, že $ed \equiv 1 \pmod{\phi(n)}$ a že d je celé (na to veľa ľudí zabudlo).

2. Nech $n = pq$ a y_1, y_2, y_3, y_4 tvoria verejný kľúč. Uvažujme dokazovací protokol, kde sa dokazovateľ snaží presvedčiť overovateľa, že pozná x_i také, že $x_i^2 \equiv y_i \pmod{n}$. Protokol má k krokov, v každom dokazovateľ vygeneruje v_i náhodne zo Z_n^* . Nech H je hašovacia funkcia a b_1, b_2, b_3, b_4 sú posledné štyri bity výstupu $H(n, v^2, y_1, y_2, y_3, y_4)$. Potom dokazovateľ pošle overovateľovi dvojicu $(v^2, v \cdot x_1^{b_1} \cdots x_4^{b_4})$. Navrhните, ako má overovateľ overovať dokazovateľove správy a zistite, prečo tento protokol nie je v poriadku.

Riešenie:

3. Nech $n = pq$ a e sú verejne známe konštanty inštancie RSA (d nikto nepozná). Definujme $E(m) = m^e \pmod{n}$. Definujme hašovaciu funkciu $HRSA(m)$ takto: správu m najprv rozdelíme na l blokov $m_1, \dots, m_l; \forall i, m_i < n$. Potom $HRSA(m) = E(\cdots E(E(m_1) \oplus m_2) \oplus \cdots \oplus m_l)$. Preskúmajte jednosmernosť a slabú odolnosť voči kolíziám takejto hašovacej funkcie za predpokladu, že d nijakým spôsobom nemáme šancu zistiť.

Riešenie:

- (a) Jednosmernosť. Keby nebola jednosmerná, vieme ku každému y nájsť efektívne m také, že $HRSA(m) = y$. To znamená, že $E(\cdots E(m_1) \cdots) = y$, teda vieme nájsť také $x \equiv E(\cdots E(m_1) \oplus m_2 \cdots \oplus m_l) \pmod{n}$, že $E(x) = y$. Teda vieme dešifrovať RSA bez toho, aby sme poznali d . A to efektívne nevieme. Teda HRSA je jednosmerná.
- (b) Ukážeme, ako ku každej správe hľadať kolíziu dĺžky 2. Nech $m = m_1 \dots m_l$ je správa a chceme k nej nájsť $p = p_1 p_2$ také, že $E(E(p_1) \oplus p_2) = E(\cdots E(m_1) \oplus m_2 \oplus \cdots \oplus m_l)$. Označme $x = E(\cdots E(m_1) \oplus m_2 \oplus \cdots \oplus m_l)$. Teda $E(E(p_1) \oplus p_2) = E(x)$. RSA je bijekcia, teda musí platiť aj $E(p_1) \oplus p_2 \equiv x \pmod{n}$. Teraz dáme do predchádzajúcej kongruencie na chvíľu rovnosť. Potom $E(p_1) \oplus p_2 = x$ a $p_2 = E(p_1) \oplus x$. Teda postup bude vyzeráť tak, že si tipneme p_1 a dorátame p_2 . Môže sa stať, že $p_2 \geq n$, v tom prípade tipneme znova. Môžu nastať dva prípady – buď $E(p_1) \oplus x < n$ alebo $n \leq E(p_1) \oplus x < 2n$ (prenechávam čitateľovi ako cvičenie :-)) – stačí si všimnúť najvyššie bity x a $E(p_1)$). Teda pravdepodobnosť úspešného tipu je aspoň $1/2$, takže bude hádať v priemere najviac dvakrát.

4. Uvažujme takýto mód blokovej šifry: $C_i = E_k(P_i) \oplus C_{i-1} \oplus P_{i-1}$. P_0 a C_0 sú inicializačné vektory. Napíšte a dokážte, ako funguje dešifrovanie. Zistite, ako ovplyvní zmena bitu šifrovaného textu otvorený text. Zistite, čo spraví s otvoreným textom výmena C_i a C_{i+1} .

Riešenie: Toto je také ľahké, že sa mi to sem nechce písať. Ale aj tak som mal za to len 3 body, lebo som to odflákol.

5. Protokol... Pribudne neskôr