Cvičení 15. 3. 2013

Základní idea algoritmu RSA (ne úplně bezpečná verze):

1. Alice vygeneruje dvě prvočísla p, q, spočte $n = pq, \varphi(n) = (p-1)(q-1)$.
2. Alice si vybere své oblíbené celé číslo $1 < e < \varphi(n)$, e nesoudělné s $\varphi(n)$.
3. Čísla (n, e) Alice zveřejní. Číslo n je *modul*, e *veřejný exponent*.
4. Alice najde d, že $ed \equiv 1 \pmod{\varphi(n)}$. Toto číslo je její *tajný exponent*.
5. Bob chce poslat Alici zprávu $0 < M < n$. Spočte a odešle $C = M^e \pmod{n}$.
6. Alice pohodlně spočte e-tou odmocninu z C jako $C^d = M^{ed} \pmod{n}$.
7. Má se za to, že odmocňování v $\mathbb{Z}_n^\star$ je typicky těžké, tedy pouze Alice může z C získat v rozumném čase M.

RSA lze také použít jako digitální podpis: Alice má hash M zprávy, co chce podepsat, spočte M^d a všichni si mohou spočíst, že $M^{de} = M$.

Počítání modulo n můžete urychlit pomocí Čínské zbytkové věty.

Příklad 1. Spočtěte pro $e = 7$ čísla $n, \varphi(n)$ a d pro následující prvočísla:

1. $p = 5, q = 7$
2. $p = 3, q = 13$

Příklad 2. V obou případech z předchozího cvičení zašifrujte a dešifrujte zprávu 15, 3, 20, 13.

Příklad 3. Proč není volba sudého e dobrý nápad?

Příklad 4. Může se při dešifování něco pokazit, pokud je náhodou M soudělné s n?

Příklad 5. Můj modul pro RSA je 33, veřejný klíč 7. Přišla mi zpráva $1, 2, 27, 10$. Dešifrujte ji.

Příklad 6. Buď $p = 13, q = 11, e = 7$. Pro která $0 \leq M < n$ bude zašifrovaná zpráva rovna M?

Kreativní příklad

Příklad 7. Navrhněte postup, jak ze znalosti n, d, e najít faktorizaci n (stačí nám pravděpodobnost úspěchu $1/2$, ale časová složitost by měla být polynomiální v $\log n$, $\log d$, $\log e$).