Cvičení 12. 4. 2012

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 $C = M^e \pmod{n}$ a to pošle.
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 $e = 17$ čísla $n, \varphi(n)$ a d pro následující prvočísla:

1. $p = 7, q = 13$
2. $p = 11, q = 23$
3. $p = 113, q = 53$

Příklad 2. Proč není volba sudého e dobrý nápad?

Příklad 3. V případech 1, 2 a 3 z předchozího cvičení zašifrujte a dešifrujte zprávu 12 4 20 12 a digitálně podepište hash 60.

Příklad 4. Můj modul pro RSA je 33, veřejný klíč 7. Přišla mi zpráva $1, 2, 27, 10$. Dešifrujte ji.

Příklad 5. Buď $p = 13, q = 11, e = 7$. Pro která $0 \geq M < n$ bude zašifrovaná zpráva rovna M?

Příklad 6 (choosen-cryptotext attack)**.** Jsme útočníci, známe $n = 851, e = 7$ a chceme dešifrovat zprávu $C = 42$. Přesvědčili jsme Alici, aby dešifrovala (tj. umocnila na d-tou) nevinně se tvářící zprávu $M = 270 = 2^e C$ a sdělila nám výsledek $V = 603$. Jak teď spočítat C?

Příklad 7. Dokažte, že z $C = M^e$ a n je možné zjistit Jacobiho symbol $\left(\frac{M}{n}\right)$.

Příklad 8. 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 $\log n$, $\log d$, $\log e$).