

Př: Alice chce doručit od Boba zašifrované správy, správy jsou přirozená čísla menší než  $N$ . Zvolí si dve prvočísla  $p, q$  tak, aby  $p \cdot q = n$ ,  $n > N$ . Pak spočítá  $\varphi(n) = (p-1)(q-1)$ , a zvolí  $e \in N$  tak, aby  $\gcd(e, \varphi(n)) = 1$ . Tzto znamená, že  $e$  má  $n$  mod  $\varphi(n)$  inverzi,  $e^{-1} = d \bmod \varphi(n)$ .

Veřejný klíč:  $(n, e)$   
Soukromý klíč:  $(n, d)$

Jak se správa zašifruje?

- vzdálej se na kroužek menší než  $N$ , vznikne správa  $a$
- spočítá se  $a^e = b \bmod n$ ,  $0 \leq b < n$
- $b$  je zašifrovaná správa

Jak se dešifruje?

- opočítánem  $b^d = a \bmod n$ ,  $0 \leq a < n$
- $a$  je otevřená správa.

TVrzení: Nechť  $n = p \cdot q$ , kde  $p \neq q$ ,  $p, q$  jsou prvočísla, a nechť  $e, d \in N$  splňují  $e \cdot d = 1 \bmod \varphi(n)$ . Potom pro každé  $a \in \mathbb{Z}_n$  platí:  $(a^e)^d = a \bmod \mathbb{Z}_n$

Důkaz: 1) pro  $a$  nesoudělné s  $n$

Z Euler-Fermatovy věty máme  $a^{\varphi(n)} = 1 \bmod \mathbb{Z}_n$ , tedy exponent může upravovat modulo  $\varphi(n)$ . O  $e, d$  víme, že  $e \cdot d = 1 \bmod \varphi(n)$ , což lze reprezentovat:  $e \cdot d = 1 + k \cdot \varphi(n)$   $\bmod \varphi(n)$ ,  $k \in N$ . Pak lze procházet RSA postupem jako:

$$(a^e)^d = a^{e \cdot d} = a^{1+k \cdot \varphi(n)} = a^1 = a \bmod \mathbb{Z}_n$$

2) pro  $a$  soudělné s  $n$ ,  $0 \leq a < n$

- $a = 0$

$$(a^e)^d = 0^{e \cdot d} = 0, \text{ rjvne platí}$$

- $a \neq 0$ , když  $a$  je soudělné s jedním z prvočísel (ne s oběma)

$p/a$ ,  $q \nmid a$ , nyní jsem činškou větu o slyšcích: dve čísla jsou shodná  $\bmod \mathbb{Z}_p$ , pokud mají stejný slyšek  $\bmod \mathbb{Z}_p$  a  $\mathbb{Z}_q$ ,  $n = p \cdot q$

Zbytky  $\bmod \mathbb{Z}_p$ :

$$a = 0 \bmod p \\ (a^e)^d = a^{e \cdot d} = 0^{e \cdot d} = 0 \bmod p \quad \} \text{ shodují se}$$

Zbytky  $\bmod \mathbb{Z}_q$ :

$$a \text{ je nesoudělné s } q, \text{ proto máme použít Euler-Fermatovu větu: } a^{\varphi(q)} = a^{q-1} = 1 \bmod \mathbb{Z}_q \\ (a^e)^d = a^{e \cdot d} = a^{1+k\varphi(n)} = a^{e \cdot d + k\varphi(n)} = a \cdot a^{e \cdot d + k(p-1) \cdot (q-1)} = a \cdot a^0 = a \cdot 1 = a \quad \} \text{ shodují se}$$

$$a = a \bmod q$$

Protože se shodují slyšky, jsou čísla shodná i  $\bmod \mathbb{Z}_n$ , tedy  $a = a^d \bmod \mathbb{Z}_n$

TVrzení: RSA lze rozložit: Nechť  $n = \prod_{i=1}^k p_i^{e_i}$ , kde  $p_i$  jsou prvočísla a  $e_i$  jsou exponenty. Pokud RSA funguje pro každé  $a \in \mathbb{Z}_n$  ( $a^d = a \bmod n$ ), pak lze dešifrovat, když  $\forall i: e_i = 1$ . Pokud je nějaký exponent větší než 1, pak se budou rozložitelně dešifrovat správy dělitelné  $p_i$ , ale nedělitelné  $p_i^{e_i}$ .

Např:  $n = p^2 \cdot q$ ,  $\{p^2, q\}$  je nesoudělná sada. Zvolím správu  $a = p$ .

$$a = p \bmod p^2 \\ a^{ed} = p^{ed} = p^{1 + \varphi(n) \cdot k} = p^{2 + ((q-1)(p-1))k} = p^2 \cdot p^k = 0 \quad p^k = 0 \quad \} \text{ zbytky se tiší}$$

Pro regenerování klíče RSA potřebujeme:

- vygenerovat k-místné prvočíslo: Miller-Rabinov test,  $O(k^4)$
- spočítat inverzi  $k^{-1} \bmod \varphi(n)$  rozšířeným Euklidem,  $O(\log(n)^2)$

Při řešení a dešifrování potřebujeme:

- rychle umocňovat v  $\mathbb{Z}_n$ , alg. opakovacích čtvrticí to umí  $O(\text{len}(n)^3)$
- při dešifrování musíme počítat residuálně v  $\mathbb{Z}_p$  a  $\mathbb{Z}_q$ , použijeme Euler-Fermatova větu a tímto větu a slydeček,  $O(\frac{1}{4} \text{len}(n)^3)$

Casová náročnost algoritmu RSA: (hledáním  $p \neq q$ )

- dělení větší pravdělky do  $\mathbb{Z}_n$  trvá  $O(2^{\frac{1}{2} \text{len}(n)})$

- celkový nejrychlejší algoritmus je  $O(2^{(c+o)} \cdot (\text{len}(n)^{13} \cdot \text{len}(\text{len}(n))^{2/3}))$ ,  $c < 2$

Pr.: Máme RSA s veřejným klíčem  $(1469, 5)$ , zadejte jsme správné  $b = 1314$

1) hromadou silou najdeme  $p, q$ , dělíme  $1469$  čísly až do  $1469 \div 38$ :

$$\begin{array}{r} 2 \\ 2871 \\ \hline 1719 \end{array}$$

$$\rightarrow 1469 \div 13 = 113$$

$$p=13, q=113, m=p \cdot q = 1469$$

2) spočítáme soukromý klíč:

$$\varphi(n) = (p-1)(q-1) = 12 \cdot 112 = 1344$$

$$d = e^{-1} = 5^{-1} \text{ v } \mathbb{Z}_{1344}$$

$$5d + 1344k = 1$$

$$\downarrow \text{Euklid } (1344, 5)$$

$$1344 = 268 \cdot 5 + 4$$

$$5 = 4 + 1$$

$$\begin{array}{r} \varphi(n) \\ \hline 4 = 1344 - 268 \cdot e \\ 1 = 1344 + 268 \cdot e \\ \hline k = -1 \quad d \end{array}$$

$$d = 269$$

3) dešifrujeme správu: (residuálně)

$$a = b^d = 1314^{269} \text{ v } \mathbb{Z}_{1469}$$

$$\text{v, } \mathbb{Z}_{13}: a_{13} = 1314^{269} \equiv 1^{269} \equiv 1$$

$$\text{v, } \mathbb{Z}_{113}: a_{113} = 1314^{269} \equiv 71^{269}, \text{ protože } \text{gcd}(113, 71) = 1, \text{ použijeme E-F: } \varphi(113) = 112$$

$$a = 71^{269} = 71^{45}. \text{ Sed' použijeme opakování čtvrtice: } 45 = 32 + 8 + 4 + 1 \approx 101101$$

$\approx XSSXSSXSSX$

$$71^{45} = 1XSSXSSXSSX = 71 SSXSSXSSX = 69SXSSXSSX = 15XSXSSX = 48SXSSX =$$

$$= 44XSSX = 73SSX = 18SX = 98X = 65$$

$$q_{13} = 113 \cdot 1, \text{ až } 113 \cdot 1 = 1 \text{ v } \mathbb{Z}_{13}, 1 = 3, q_{13} = 339$$

$$q_{113} = 13 \cdot 4, \text{ až } 13 \cdot 4 = 1 \text{ mod } 113, 4 = 87, q_{113} = 1131$$

$$a = a_{13} \cdot q_{13} + a_{113} \cdot q_{113} = 1 \cdot 339 + 65 \cdot 1131 = 339 + 73515 = 73854 = \underline{404} \text{ v } \mathbb{Z}_{1469}$$

Úkol na RSA odmocněním (znamí  $a^e, e$ , chceme  $a$ )

Funkce  $\mathbb{Z}_n \rightarrow \mathbb{Z}_n: x \mapsto x^e$  je jednoznačná.

Chceme-li počítat odmocniny, musíme snad faktorizaci  $n$ , nebo  $d$  takové, že  $e \cdot d = 1 \text{ v } \mathbb{Z}_{\varphi(n)}$ . Bez toho se máme počítat  $\sqrt[n]{x}$  hromadou silou, opět  $O(2^{\text{len}(n)})$ .

Úkol na RSA svištěním  $\varphi(n)$  nebo  $d$ :

Tvrzení: Nechť  $n = p \cdot q$ ,  $p \neq q$ ,  $p, q$  jsou větší pravdělosti. Znalost klíče provádí je ekvivalentní smyslu  $\varphi(n)$ .

Důkaz:  $\varphi(n) = (p-1)(q-1) = p \cdot q + 1 - (p+q) = n+1 - (p+q)$

Zámeček:  $n$  a  $\varphi(n)$  mají společný dělitel  $\pi = p \cdot q = n$  a  $\sigma = p+q = n - \varphi(n) + 1$ , a je dělitel vztahu  $\pi \mid \sigma$  smyslo vypočítat vztahem rovnice  $x^2 - \sigma x + \pi = 0$

Tvrzení: Nechť  $(n, e)$  je veřejný RSA klíč. Znalost  $d$  umožňuje faktorizaci  $n$ .

Lemma: Pokud naleznete v  $\mathbb{Z}_n$  nekrátkou druhou odmocninu  $a^1$ , tj.  $b^2 \neq 1 \text{ v } \mathbb{Z}_n$ , tak můžete faktorizovat  $n$ .

Důkaz lemma:  $b^2 = 1 \text{ v } \mathbb{Z}_n, b \neq \pm 1$ . Pak  $(b+1)(b-1) = b^2 - 1 = 0 \text{ v } \mathbb{Z}_n$ .

Tedy  $b+1$  a  $b-1$  jsou děliteli nuly v  $\mathbb{Z}_n$ , když jsou oddílné s  $n$  a nejsou invertibilní. Pak  $\text{gcd}(b+1, n) = p$ ,  $\text{gcd}(b-1, n) = q$ .  $\rightarrow$  protože  $a$  má jenom  $\text{gcd}(d, \varphi(n)) = 1$ .

Důkaz tvrzení: Užíváme, že  $e \cdot d = 1 \text{ v } \mathbb{Z}_{\varphi(n)}$ , tedy  $e \cdot d - 1 = k \cdot \varphi(n) = k(p-1)(q-1)$ ,

kde  $p-1$  a  $q-1$  jsou sudá. Zároveň  $a \in \mathbb{Z}_n^*$ , pak  $a^{\varphi(n)} = 1 \text{ v } \mathbb{Z}_n = a^{(e \cdot d - 1)}$ .

Pak bude  $b = a^{\frac{1}{2}(e+d-1)}$  splňovat  $b^2 = 1$ , protože dělitel je exponent užší čísla.

J. li  $b \neq \pm 1$ , můžeme faktorizovat  $n$ . V opačném případě zvolíme jiné  $a \in \mathbb{Z}_n^*$ .

Pr:  $n = 1469$ ,  $\varphi(n) = 1344$ . Najděte  $p \cdot q$ .

$$p \cdot q = 1469$$

$$\varphi(n) = (p-1)(q-1) = p \cdot q - (p+q) + 1 = n - (p+q) + 1 = 1469 + 1 - (p+q) = 1470 - (p+q)$$

$$p+q = 1470 - \varphi(n) = 1470 - 1344 = 126$$

$$\pi = p \cdot q = 1469$$

$$o = p+q = 126$$

$$D = b^2 - 4ac = (-o)^2 - 4\pi = 126^2 - 4 \cdot 1469 = 10000, \sqrt{D} = 100$$

$$p, q = \frac{126 \pm 100}{2} = \frac{226/2}{26/2} = \frac{113}{13} = 113$$

Pr: Faktorizujte  $n=15$ ,  $b=\pm 4$   $\rightarrow -4 = 11 \cdot 15$

$$\sim \mathbb{Z}_{15}, 4 = 16 = 1, (-4)^2 = 16 = 1, \text{tedy } \sqrt{1} \text{ má nekrivitelný kořen } 4, -4.$$

$$\gcd(11-1, 15) = \gcd(15, 10) = 5$$

$$\gcd(11+1, 15) = \gcd(15, 12) = 3$$

$$\gcd(15, 4-1) = \gcd(15, 3) = 3$$

$$\gcd(15, 4+1) = \gcd(15, 5) = 5$$

$$5 \cdot 3 = 15 \leftarrow \text{Náš faktorizace} \rightarrow 5 \cdot 3 = 15$$

Pr: U RSA máme  $n=15$ ,  $e=5$ ,  $d=5$ . Faktorizujte  $n$ .

$$\varphi(n) = \varphi(15) = 8, 5 \cdot 5 = 1 \sim \mathbb{Z}_8, e \cdot d - 1 = 5 \cdot 5 - 1 = 24, \text{tedy } a^{24} = 1 \sim \mathbb{Z}_{15}$$

Pak  $b = a^{\frac{ed-1}{2}}$  by měl splňovat  $b^2 = 1 \sim \mathbb{Z}_n$ .

$$\text{Kvadrát } a=2: b = 2^{12} = 2^{4 \cdot 3} = (16)^3 = 1^3 = 1 \quad b=1, \text{ moždu } \sqrt{b} = 1.$$

$$\sqrt{b} = 2^{\frac{1}{2}} = 2^{\frac{1}{2} \cdot 12} = 2^6 = 64 = 4$$

$$\text{Máme } b=4, b^2=1. \text{ Faktorizace } n \text{ je } \gcd(15, 4+1) = 3, \gcd(15, 4-1) = 5.$$

Prádnáška Pr: Znaleť  $e, d, n$  umožní faktorizaci,  $n = 1469$ ,  $e=5$ ,  $d=269$   
7.3.2019  $e \cdot d - 1 = 5 \cdot 269 - 1 = 1344, a^{1344} = 1 \sim \mathbb{Z}_{1469}, 1344 = 2^6 \cdot 21$

$$\text{Kvadrát } a=2: b = 2^{2^6 \cdot 21} = (2^{21})^{2^6} = (889)^{2^6} = (1468)^{2^5} = (-1)^{2^5}$$

- Nám rádem se dál budou opakovat jednichky, ale my nechceme  $b=1$ .

$$a=3: b = (3^{21})^{2^6} = (833)^{2^6} = (521)^{2^5} = (1145)^{2^4} = (677)^{2^3} = 1^4$$

- máme  $\sqrt{1} = 677$ , to jsme chtěli

$$\gcd(1469, 678) = ? = 113$$

$$\gcd(1469, 678) = ?$$

$$= 1469 / 113 = 13$$

$$1469 = 678 \cdot 2 + 113$$

$$678 = 113 \cdot 6 + 0$$

$$1469 = 13 \cdot 113$$

Útok oshidra: Upráve přidělovařem k klíčů s modulom  $n$ . Eva všechna správy zasílá s vlastním klíčem, jejichž verejné klíče jsou resoudělné. Eva náleží, že se jedná o správy vzniklé se stejným obecněho obecněho řešením.

Pokud  $\gcd(e_1, \dots, e_s) = 1$ , tedy verejné části jsou resoudělné, náleží, že díky Bezoutovi je dokazovat využíváním jeho  $1 = e_1 A_1 + e_2 A_2 + \dots + e_s A_s$ . Eva si svedla  $\frac{1}{e_i}$  a pak upravila  $b_1^{t_1} \cdot b_2^{t_2} \cdots b_s^{t_s} = a^{e_1 t_1 + e_2 t_2 + \dots + e_s t_s} = a^1 = a \sim \mathbb{Z}_n$

Pokud to bude

Pr: Eva má verejné klíče  $(703, 11)$  a  $(703, 7)$  a jimi založené upravily  $694, 78$ .  
Najděte správu OT.

$$\gcd(11, 7) = 1 = 2 \cdot 11 - 3 \cdot 7, t_1 = 2, t_2 = -3$$

$$a = a^1 = a^{b_1 t_1 + b_2 t_2} = a^{11 \cdot 2 + 7 \cdot (-3)} = (a^1)^2 \cdot (a^7)^{-3} = 694^2 \cdot 78^{-3} = 694^2 \cdot (78^{-1})^3 =$$

$$[zpovídání k 78^{-1} = -9 = 694]$$

$$= 694^2 \cdot (-9)^3 = (-9)^2 \cdot (-9)^3 = 81 \cdot (-531441) = 81 \cdot 27 = 78$$

\* Chceme nahoru vymazat jednichky, takže rádi vložíme nějaké náporové li. Proto budeme rádi vložit počítat nějakou inverzi (exponenty ejson kladné)

Holc insidera: Uprávce přidělí vývratelům klíče se odkazujím modulom  $n$ . Jeden z vývratelů si se snadností sámho  $e_i$  a díl faktorizuje  $n$ . Pak si můžeme spočítat díl ostatních vývratelů a čist jejich upravy.

$\rightarrow$  malé nějaké  $e_i$ ,  $e \leq k$ , rachyhli jsme k správ

Hastadův útok: počítá s kym, že stejná správa se rozšírá až lidem, ale lidé mají různé moduly a malejší výpočty klíče. Pak může nastat situace, když se výpočty exponenty shodují, a moduly jsou nezádělné! Eva má výpočty klíče  $(n_i, b_i)$ , a zároveň  $b_i \cdot b_j \equiv e \pmod{n_i \cdot n_j}$ .

Z čínské věty o sítých uželovém soustavu:  $b_i = a^e \pmod{n_i}$ , spočítáme  $n = \prod n_k$  a pak můžeme  $a \pmod{Z_n}$ . Protože  $e < n$ , můžeme správu odmocnit  $\pmod{Z_n}$  stejně jako  $\pmod{\mathbb{Z}}$ , když už uželové soustavy.

- když  $n_i$  nelyže nezádělná, můžeme faktor nějakého  $n_i$ , a můžeme si pro tento klíč doporučit něčeho jiného.

Obrana: Neponívat oddělené moduly, používat do足akně velká  $e$  (aby bylo ležkejší mít  $k \geq e$  sítých), doporučuje se  $e > 2^{16}$ . Do správy lze přidat náhodné kódování, aby nelyly zašifrovane správy výjevit.

Příklad: Hastadův útok, možné klíče  $(77, 3)$ ,  $(51, 3)$ ,  $(65, 3)$  a rachyhli jsme správy 64, 9, 60. Uspořejte původní správy.

$a < \min(n_i) = 51$ , správa bude mít výsledek 51. Měli bychom ověřit nezádělnost  $n_i$  pomocí gcd, ale protože to jsou malá čísla, vidíme ho primu s faktorisací (na nepřijetí).

Soustava pro čínskou větu:

$$a^3 \equiv 64 \pmod{77}$$

$$q_{77} = 192270$$

$$a^3 \equiv 9 \pmod{51}$$

$$q_{51} = 110110$$

$$a^3 \equiv 60 \pmod{65}$$

$$q_{65} = 208131$$

$$a^3 = 64 \cdot 192270 + 9 \cdot 110110 + 60 \cdot 208131 = 510511 = 63040 + 225225 + 235620 = \\ = 513885 = 3375 \pmod{255255}$$

$$\text{Protože } a^3 < 255255, \text{ můžeme spočítat } a = \sqrt[3]{a^3} = \sqrt[3]{3375} = 15.$$

Wienerův útok: Nechť  $n = p \cdot q$ , kde  $q < p < c \cdot q$  pro nějaké malé  $c \in \mathbb{N}$ , díle  $e < \varphi(n)$ ,  $d < \frac{1}{c+1} n^{\frac{1}{4}}$ . Pak lze  $a (n, e)$  efektivně spočítat  $(n, d)$ .

Využívají se k tomu řetězové zlomky.

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{\dots}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = q_1 + \frac{1}{q_2 + \frac{r_1}{r_2}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_2}{r_3}}} \dots$$

$$\frac{10733}{27161} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \dots}}} = 0.395$$

Získá se Euklidem:

$$10733 = 0 \cdot 27161 + 10733$$

$$27161 = 2 \cdot 10733 + 5695$$

$$10733 = 1 \cdot 5695 + 5083$$

$$5695 = 1 \cdot 5083 + 612$$

$$5083 = 7 \cdot 612 + 439$$

$$612 = 1 \cdot 439 + 218$$

$$439 = 2 \cdot 218 + 3$$

$$218 = 72 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$\uparrow q_i$

Pro racionalní číslo  $\frac{a}{b}$  je slomek konečný a má délku  $\lambda < 2 \cdot \min(\text{len}(a), \text{len}(b))$

S řetězovými slomeky užce souvisejí pojmem konvergentsa

$$i\text{-t\'a konvergenta} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_i}}}, \text{ d\'ale budeme zapisovat jako } (q_0, q_1, \dots, q_i)$$

postupnost

Konvergentsy nebo předchůdci p\'ukladek:

$$0: (0) = 0$$

$$1: (0, 2) = 0 + \frac{1}{2} = 1/2 = 0.5$$

$$2: (0, 2, 1) = 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3} = 0.\overline{3}$$

$$3: (0, 2, 1, 1) = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1}}} = \frac{1}{2 + \frac{1}{2}} = \frac{1}{\frac{5}{2}} = \frac{2}{5} = 0.4$$

$$4: (0, 2, 1, 1, 7) = 0 + 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{7}}} = 2 + \frac{1}{1 + \frac{8}{7}} = 2 + \frac{1}{\frac{15}{8}} = 2 + \frac{8}{15} = \frac{1}{2 + \frac{8}{15}} = \frac{1}{\frac{38}{15}} = \frac{15}{38} = 0.3947\dots$$

= slomek už m\'eje n\'e sk\'ratit

**Tvrzen\'i:** Ještě pro slomek  $\frac{c}{d}$ ,  $\text{gcd}(c, d) = 1$ , který approximuje č\'slo  $r \in \mathbb{R}$  s přesností  $|r - \frac{c}{d}| < \frac{1}{2d^2}$ , pak je slomek  $\frac{c}{d}$  některou konvergentou řetězového slomku pro  $r$ .  
→ d\'ukaz je v Thoupov\'i

spíš názv\'a d\'ukaz

**D\'ukaz Wienerova útoku:** ( $n = p \cdot q$ ,  $q < p < c \cdot q$ ,  $e < \varphi(n)$ ,  $d < \frac{1}{c+1} \cdot n^{\frac{1}{2}}$ )

$$e \cdot d = 1 \Leftrightarrow \exists \varphi(n) \quad (\text{l} \text{ a } d \text{ jsou si inverzn\'e } \Leftrightarrow \exists \varphi(n), \text{ t} \text{o v\'ime z vlastnosti RSA})$$

$$e \cdot d - k \cdot \varphi(n) = 1 \Leftrightarrow \exists \quad 1: (d, \varphi(n))$$

$$\frac{e}{\varphi(n)} - \frac{k}{d} = \frac{1}{d \varphi(n)} \quad (\varphi(n) \text{ nezm\'ame, ale l\'e\'iva o trochu menší m\'eru } n)$$

Wiener approximuje  $\varphi(n)$  n\'akem a uyužije vztahy pro  $n, p, q, c, d$ , aby s\'iskal nov\'y vztah:

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{2d^2}$$

Následně se použije korek\'n\'e n\'yže, v\'ime tedy, \\'ze  $\frac{e}{n}$  (kter\'e s\'ame) je konvergentou  $\frac{k}{d}$ , kter\'e cheme.

Budeme p\'ejdat všechny konvergentsy a skouset, jestli je  $d$  správný kl\'ic.

**Př:** Máme neřešený kl\'ic  $(n, e) = (27161, 10733)$ . Najděte  $d$ .

$$\frac{e}{n} = \frac{10733}{27161}, \text{ slomek i konvergentsy v\'iž m\'ame spočítan\'e, stač\'i skouset konvergentsy:}$$

$$e \cdot d - k \cdot \varphi(n) = 1 \Rightarrow \varphi(n) = (e \cdot d - 1)/k$$

$$1: \frac{k}{d} = \frac{1}{2} \quad \varphi(n) = \frac{2 \cdot 10733 - 1}{k-1} = 21465$$

NE,  $\varphi(n)$  je sud\'e a d\'elikeln\'e  $\varphi(n)$

$$2: \frac{k}{d} = \frac{1}{3} \quad \varphi(n) = \frac{3 \cdot 10733 - 1}{1} = 32198$$

NE, musí být  $\varphi(n) < n$

$$3: \frac{k}{d} = \frac{2}{5} \quad \varphi(n) = \frac{5 \cdot 10733 - 1}{2} = \frac{53664}{2} = 26832$$

MOŽNÁ'

$$4: \frac{k}{d} = \frac{15}{38} \quad \varphi(n) = \frac{38 \cdot 10733 - 1}{15} = \frac{407853}{15} = 27190.2$$

NE, musí být  $\varphi(n) \in \mathbb{N}$

Ověříme  $k=2$ ,  $d=5$ ,  $n=27161$ ,  $\varphi(n)=26832$

$$n = p \cdot q = 27161$$

$$\varphi(n) = (p-1)(q-1) = p \cdot q + 1 - (p+q) = 27162 - (p+q)$$

$$\pi = p \cdot q = 27161$$

$$\sigma = p+q = 27162 - 26832 = 330$$

$$p = \frac{27161}{q} = 330 - q \quad | 27161 = 330q - q^2 \quad | q^2 - 330q + 27161 = 0$$

...

$p = 173$ ,  $q = 157$ , to jsou prvočísla, když j\'sme m\'alek\'i p\'rijateln\'e RSA, souhlasn\'y kl\'ic je 5

Příklad: Nařízněte RSA protokol pro šifrování sítěvku  $a < 2^8 = 256$

$$\left. \begin{array}{l} p=41 \\ q=7 \end{array} \right\} n=41 \cdot 7 = 287, \varphi(n)=40 \cdot 6 = 240$$

$$e=11, d=e^{-1} \bmod 240 \quad d \text{ k}$$

$$11d=1 \bmod 240$$

$$11d+240k=1$$

$$-109 \cdot 11 + 5 \cdot 240 = 1$$

$$\hookrightarrow d = -109 = 131$$

verejný klíč je  $(287, 11)$ , soukromý klíč je  $(287, 131)$

Příklad: Alice má veřejný klíč  $(517, 11)$ . Jaký z následujících klíčů je správný soukromý?

$$-(571, 67)$$

ten to nemá, má jiné  $n$  ( $517 \neq 571$ )

$$-(517, 301)$$

mohlo, ověříme posleží

$$-(517, 251)$$

mohlo, ověříme posleží

$$n=517=11 \cdot 47, \varphi(n)=460$$

$$e=11, d \cdot e = 1 \bmod 460$$

$$d=301? \quad 301 \cdot 11 = 3311 = 91 \bmod 460 \quad \times$$

$$d=251? \quad 251 \cdot 11 = 2761 = 1 \bmod 460 \quad \checkmark$$

Správný soukromý klíč je  $(517, 251)$

Příklad: Alice má klíče  $(517, 11)$  a  $\text{PRIK} = (517, 251)$ , Bob má klíče  $\text{PRIK} = (533, 113)$ ,  $\text{PUK} = (533, 17)$ . Bob posílá Alice správu  $a=10$ . Jak ji zašifruje?

Bob použije Alicin veřejný klíč  $(517, 11)$ .  $b=a^e = 10^{11} \bmod 517$

Opatkování číslice:  $11 = 8+2+1 = 1011 = XSSXSX$

$$10^{11} = 10SSXSX = 100SX SX = 10000SX = 177SX = 1770SX = 219SX = 47961X = 397X = 3970 = \underline{\underline{351}}$$

Příklad: Alice má klíč  $\text{PUB} = (551, 11)$ . Bob posílá Alice správu, ale Eva ji zachytila a hrubou silou přečetla. Jak?

Eva říká, že  $551 = 19 \cdot 29, \varphi(n) = 504$

$$e \cdot d = 1 \bmod 504 \quad d \text{ k}$$

$$11d = 1 \bmod 504$$

$$11d + 504k = 1$$

$$d = -229 = 275 \bmod 504$$

$$b=169$$

$$\left( \begin{array}{c|cc} 1 & 0 & 11 \\ 0 & 1 & 504 \end{array} \right) \approx \left( \begin{array}{c|cc} 1 & 0 & 11 \\ -451 & 1 & 9 \end{array} \right) \approx \left( \begin{array}{c|cc} 46 & -1 & 2 \\ -45 & 1 & 9 \end{array} \right) \approx \left( \begin{array}{c|cc} 46 & -1 & 2 \\ -229 & 5 & 1 \end{array} \right) \approx \left( \begin{array}{c|cc} 504 & -11 & 0 \\ -229 & 5 & 1 \end{array} \right)$$

$$\begin{aligned} a = b^d &= 169^{275}, 275 = 256 + 16 + 2 + 1 = 100010011 \approx XSSXSXSSSX \\ 169^{275} &= 169SSXSXSSSX = 28561SSSXSSSX = -91SSSXSSSX = 8281SSSXSSSX = \\ &= 16SSXSSSX = 256SXSSSX = 65536XSSSX = -33XSSSX = -5577SSSX = \\ &= -67SSSX = 4489SSSX = 81SSSX = 6561SX = -51SX = 2601SX = -154SX = \\ &= -26026SX = -129SX = 16641X = 111X = 18759 = \underline{\underline{25}} \end{aligned}$$

Nebudu moci ráno udělat lépe čínskou větou a shodit, protože snášíme  $p$  a  $q$

$$-\sim \mathbb{Z}_p = \mathbb{Z}_{19}$$

$$\varphi(19) = 18$$

$$169^{275} = -2^5 = -32 = 6$$

$$\varphi_{19} = 19 \cdot 1 = 1 \bmod 19$$

$$29_1 + 19k = 1$$

$$-\sim \mathbb{Z}_q = \mathbb{Z}_{29}$$

můžu ho řešit přes číslice, nebo jít do

$$\varphi(29) = 28$$

egzponent a moží se inverzi

$$169^{275} = -5^{23} = (-5)^{-5} = (-5^{-1})^5 = (-6)^5 = -7776 = 25$$

$$\varphi_{29} = 19 \cdot 1 = 1 \bmod 29$$

$$19n + 29l = 1$$

$$\left( \begin{array}{c|cc} 1 & 0 & 29 \\ 0 & 1 & 19 \end{array} \right) \approx \left( \begin{array}{c|cc} 1 & -1 & 10 \\ 0 & 1 & 19 \end{array} \right) \approx \left( \begin{array}{c|cc} 1 & -1 & 10 \\ -1 & 2 & 9 \end{array} \right) \approx \left( \begin{array}{c|cc} 2 & -3 & 1 \\ -1 & 2 & 9 \end{array} \right)$$

$$l=2$$

$$n=-3$$

$$\left| \begin{array}{l} \varphi_{19} = 58 \\ \varphi_{29} = -57 \end{array} \right.$$

$$a = b^d = \varphi_{19} \cdot b_{19}^d + \varphi_{29} \cdot b_{29}^d = 58 \cdot 6 - 57 \cdot 25 = -1077 = \underline{\underline{25}}$$

Príklad: Faktorizujte  $n = 6683$ , kdežto máme  $\varphi(n) = 6480$

$$\pi = p \cdot q = 6683 \quad \varphi(n) = (p-1)(q-1) = p \cdot q - (p+q) + 1 = 6684 - (p+q)$$

$$\sigma = p+q = 6684 - 6480 = 204$$

$$p = \frac{\pi}{q}, p = \sigma - q \quad \left| \frac{\pi}{q} = \sigma - q \right. \quad \left| \pi = \sigma q - q^2 \right. \quad \left| q^2 - \sigma q + \pi = 0 \right. \quad \left| q^2 - 204q + 6683 \right.$$

$$D = b^2 - 4ac = 204^2 - 4 \cdot 6683 = 41616 - 26732 = 14884 = 122^2$$

$$p, q = \frac{-b \pm \sqrt{D}}{2a} = \frac{204 \pm 122}{2} = \begin{cases} 163 \\ 41 \end{cases} \quad \underline{p=41, q=163}$$