

Príklad: Faktorizujte $n = 6683$, když znáte $\varphi(n) = 6480$

$$\begin{aligned} \pi &= p \cdot q = 6683 & \varphi(n) &= (p-1)(q-1) = p \cdot q - (p+q) + 1 = 6684 - (p+q) \\ \sigma &= p+q = 6684 - 6480 = 204 & & \end{aligned}$$

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

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

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

Přednáška Útoky na implementaci RSA

13.3.2019
14.3.2019

- Kocher: měří čas rozpočtu, který závisí na době brutální opakování číslic.
- Tipuje se, že bit po bitu a slouistikou vyhodnocuje, oda doba brutální záleží.
- říká chybouch kroků - Eva posílá Alice správu b ve formátu c·b pro kódování c a sleduje, jestli Alice vrátila číslo ("správa je ve správném formátu").

Další jsou v materiálech digitální podpisy, certifikáty a hashování funkce obecné, ale to připravil nebruder, nict se ke tomu stejně neříkalo.

Grupy a Abelovy grupy

připomínáme: Množina G s binární operací $*$ nazýváme grupu $(G, *)$, pokud je $*$ asociační, má neutrální prvek e a má i každou invertenci prvek. Pokud je množina $*$ komutativní, je $(G, *)$ Abelova grupa.

$(\mathbb{Z}_n, +)$ je Abelova grupa řádu n (\equiv má n prvků)

(\mathbb{Z}_n, \cdot) není grupa, protože nenajdeme invenci k 0: $0 \cdot x = 1$

(\mathbb{Z}_n^*, \cdot) je Abelova grupa řádu $\varphi(n)$, nula v ní vůbec není.

Tvrzení: Nechť (G, \cdot) je grupa. Pak

1) neutrální prvek je určen jednoznačně,

2) je-li b levý inverzní prvek k a a c je pravý inverzní prvek k a , pak $b=c$

3) $(ab)^{-1} = (b^{-1} \cdot a^{-1})$ socks and shoes lemma

Důkaz: 1) přepokládejme dvouřadé neutrální $e \neq f$. Pak

$e = e \cdot f = f$, tedy neutrálně se shodují, může být jen jeden

2) e je inverzní prvek v G , l je levá inverse, p je pravá inverse k a ($la=e$, $ap=e$). Pak:

$$l = l \cdot e = l(a \cdot p) = (l \cdot a) \cdot p = e \cdot p = p$$

platí to a následně jsme použili asociačnost. Znacíme $p=l=a^{-1}$

$$3) (ab)^{-1} \cdot (ab) = 1$$

$$(b^{-1}a^{-1}) \cdot (ab) = 1$$

$$b^{-1}(a^{-1} \cdot a)b = 1$$

$$b^{-1}e b = 1$$

$$b^{-1}b = 1$$

$$1 = 1$$

Tvrzení: Nechť (G, \cdot) je grupa. Pak

1) V grupě G je kladit libovolným pravem, když pro každé a platí:

je-li $a \cdot x = a \cdot y$, pak je $x=y$.

2) V grupě G mají každou lineární rovnici $ax=b$, $y \cdot a = b$ řešení a to je jediné.

Tato vlastnost grupy charakterizuje. Každá pologrupa, v níž mají každou lineární rovnici řešení, je vůbec grupou.

3) Levá transakce libovolným pravem $a \in G$, $la: G \rightarrow G: x \mapsto ax$ je vždy jednoznačně zobrazení.

Dоказ: 1) $ax = ay$ / násobením číslou

$$a^{-1}ax = a^{-1}ay$$

$$ex = ey$$

$$x = y$$

2) $ax = b$

$$a^{-1}ax = a^{-1}b$$

$$ex = a^{-1}b$$

$$x = a^{-1}b$$

$$ya = b$$

$$ya^{-1} = ba^{-1}$$

$$ye = ba^{-1}$$

$$y = ba^{-1}$$

3) $la(x) = ax$

$$a^{-1}la(x) = a^{-1}ax$$

$$a^{-1}la(x) = ex$$

$$x = a^{-1}la(x)$$

(G, \cdot) je pologrupa, proto platí asociativita

Důsledek: Nechť G je pologrupa, kde pro každou lineární rovnici $ax = b$ máme řešení, pak G je grupa.

Dоказ: Uvažme $a \in G$ a řešme $ax = a$, řešení označme $la = x$ ($a \cdot la = a$).

Ukážeme, že la je pravý neutralní, tj. $\forall g \in G: gla = g$.

Vypočtem řešení $ya = g$, o řešení víme, že $y \in G$, označme $y = c$.

$$g \cdot la = (ya) \cdot la = y(a \cdot la) = y \cdot a = g$$

Tedy $g \cdot la = g$, proto la je pravý neutralní.

Obdobně lze doložit, že fa je levý neutralní, a že $la = fa = 1$.

$\Rightarrow G$ má neutralní

Pro $a \in G$ řešme $ax = 1$ a $ya = 1$, kde x, y jsou prava a levá inverse. Tedy $x = y = a^{-1}$
jako předtím lze doložit, že obě inverse se komají a $x = y = a^{-1}$
 $\Rightarrow G$ má inverse

G je asociativní, má neutralní i inverse, tedy G je grupa.

Pozn. Platí-li krácení v G prvkem a (tedy G je monoid), tak $la: G \rightarrow G$ je injekce.

Platí-li řešení lin. rovnic $ax = b$ pro $b \in G$, pak $la: G \rightarrow G$ je surjekce. \hookrightarrow na prosté

Důsledek: Je-li monoid G s krácením a $|G| \in \mathbb{N}$ (je konečný), pak platí-li krácení pro $ta \in G$, tak lze řešit všechny lineární rovnice $ax = b$, $ya = b$.

Připomenutí:

Okrub: $(R, +, \cdot)$ je okrub, pokud $(R, +)$ je Abelova grupa a (R, \cdot) je pologrupa a platí oba distributivní zákony $(x(y+z)) = xy + xz$ a $((x+y)z) = xz + yz$.

Těleso: nebuďším okrub je těleso, pokud je $(R - \{0\}, \cdot)$ grupa

nebuďším okrub je těleso, pokud všechny lineární rovnice $ax = b$, $ya = b$ kde $a \neq 0$ mají řešení.

když konečný obor je těleso, mohouť prostí soubrazem la a konečné možnosti oboru lze využít jednoznačné

Obor: nebuďším okrub s jednotkou a neutrální obor, pokud v něm lze doložit libovolného nenulového prvku \hookrightarrow okrub sjednotka = okrub, kde $ab = b \cdot a$ a má násobku neutralní (1).

Def: Řeší-li G_1, G_2, \dots, G_k grupy, pak množina $G_1 \times G_2 \times \dots \times G_k$ všechna k-ticí součtu s operací, kterou provádíme po součinnicích (pro g_i jake v G_i) je také grupa nazývaná \otimes direktní součin grup G_1, \dots, G_k .

Řeší-li všechny grupy stejně, mluvíme o direktní mocnině, nazívané ko $G^{(k)}$.

Př: V direktním součinu jsou se setkali v reprezentacijském počítání:

$$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$$

Def: Podmnožina H grupy $(G, \cdot, 1, (-)^{-1})$ hovorí podgrupa, pokud pro každé $a, b \in H$:

- je-li $a, b \in H$, tak $a \cdot b \in H$

- je-li $a \in H$, pak $a^{-1} \in H$

Ak podgrupa je podmnožina uzavřená na operaci, neutrální prvek a invizi.

Tvrdění: Nechť G je grupa a $\emptyset \neq H \subseteq G$. Následující tvrzení jsou ekvivalentní:

- H je podgrupa v G

- pro všechny $a, b \in G$: je-li $a, b \in H$, pak $a \cdot b \in H$, $a^{-1} \in H$

- pro všechny $a, b \in G$: je-li $a, b \in H$, pak $a \cdot b^{-1} \in H$ ← tímto směrem myslíme ovlivnou podgrupy

Tvrdění: Nechť H_1, H_2 jsou podgrupy v G grupě G

- $H_1 \cap H_2$ je podgrupa v G

- Je-li G Abelova grupa, pak $H_1 \cdot H_2 = \{h_1 \cdot h_2 ; h_1 \in H_1, h_2 \in H_2\}$ je podgrupa v G

Příklady: Nechť G je grupa.

- všechny $\{a^k\}$ a $\langle a \rangle$ jsou podgrupy v G .

- množina všech celých mocnin prvku $a \in G$, $M = \{a^{k^2} ; k \in \mathbb{Z}\}$ je podgrupa grupy G . Naopak je cyklická podgrupa generovaná prvkem a , snadno $\langle a \rangle$.

Tvrdění: Každá podgrupa v $(\mathbb{Z}, +)$ je tvaru $m\mathbb{Z}$ pro nějaké $m \in \mathbb{Z}$.

Nauč se $m\mathbb{Z} = m_2\mathbb{Z}$ právě tehdy, když m_2/m_1 . $\rightarrow = \{m\mathbb{Z} ; z \in \mathbb{Z}\}$

Důkaz: $m\mathbb{Z}$ je podgrupa

$$m \cdot z_1 + m \cdot z_2 = m(z_1 + z_2), \text{ a protože } z_1 + z_2 \in \mathbb{Z}, \text{ bude}$$

platit i $m(z_1 + z_2) \in m\mathbb{Z}$. (násobení nevyloučí)

$$z=0: mz = m \cdot 0 = 0 \in m\mathbb{Z} \quad (m\mathbb{Z} \text{ má neutrální})$$

$$-(m \cdot z) = m(-z) \in m\mathbb{Z} \quad (m\mathbb{Z} \text{ má invese})$$

podgrupa vždy může zapsat jíko $m\mathbb{Z}$

Nechť P je podgrupa v $(\mathbb{Z}, +)$. Zvolíme $m = \text{nejmenší kladné číslo v } \mathbb{Z}$. Pokud takové m nenajdu, nazavenu to, že $P = \{0\}$, což je $0 \cdot \mathbb{Z}$.

Libovolné $a \in P$ podélím m -hem se slyšet $a \in P$

$a = qm + r$, $0 \leq r < m$, slyšete je $r = \underline{\circ} a - qm \circ$, q reprezíme:

$q \leq m$

$$qm = \overbrace{m \cdot m \dots \cdot m}^{q \text{ krát}}, \text{ a je toho je vidět, že } i q \cdot m \in P$$

Díky dělení se slyšet většinu, že $r < m$ a $r \geq 0$, ale m je minimální, proto $r=0$.

Máme $a = qm$, tedy libovolný prvek v P může jíko násobek m .

Tvrdění: Každá podgrupa v $(\mathbb{Z}_n, +)$ je tvaru $d\mathbb{Z}_n = \{d \cdot z ; z \in \mathbb{Z}_n\}$ pro nějaké $d \in \mathbb{Z}$, kde d/n . Nauč se $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$ iff. d_2/d_1 .

Důkaz: Všechny podgrupy v $(\mathbb{Z}_n, +)$ jsou cyklické a pro každého děliteli d čísla n je ade právě jedna podgrupa tvaru $d\mathbb{Z}_n$. Tato podgrupa má $\frac{n}{d}$ prvků.

Příklad: $(\mathbb{Z}_{15}^*, \cdot)$ $\Psi(15) = \Psi(3 \cdot 5) = 2 \cdot 4 = 8$, \mathbb{Z}_{15}^* má 8 prvků: $\{1, 2, 4, 7, 8, 11, 13, 14\}$

příklady podgrup: $P_1 = \{1\}$

$P_2 = \{1, 14\} = \{1, -1\}$

$P_3 = \langle 2 \rangle = \{2, 4, 8, 16=1, 2, \dots\} = \{1, 2, 4, 8\}$

$$P_2 \cdot P_3 = \{\pm 1\} \{1, 2, 4, 8\} = \{\pm 1, \pm 2, \pm 4, \pm 8\} = \{1, 2, 4, 7, 8, 11, 13, 14\} = \mathbb{Z}_{15}^* \subseteq \mathbb{Z}_{15}^*$$

$$P_2 \cap P_3 = \{1\} = P_1 \subseteq \mathbb{Z}_{15}^*$$

$\forall \mathbb{Z}_n = \mathbb{Z}/\mathbb{Z} \text{ mod } n$ jsou podgrupy také novou m. \mathbb{Z}_n .

Př: Podgrupy $\langle (\mathbb{Z}_{12}, +) \rangle$, podgrupy obsahující posle děliteli ohromátek.

$$\begin{aligned} P_1 &= \{0\} \\ P_2 &= \{0, 6\} \\ P_3 &= \{0, 4, 8\} \\ P_4 &= \{0, 3, 6, 9\} \\ P_6 &= \{0, 2, 4, 6, 8, 10\} \end{aligned}$$

$$\begin{array}{c} P_4 \subseteq P_{12} \\ P_6 \subseteq P_{12} \\ P_2 \supseteq P_1 \\ P_3 \subseteq P_1 \end{array} \quad P_{12} \subseteq \mathbb{Z}_{12}$$

Def: Nechť G je grupa, H je podgrupa v G , $a \in G$. Levá třída podle podgrupy H nazývána prvkem a je množina $aH = \{ah \mid h \in H\}$, analogicky se definuje prava třída Ha .

Pozn: Je-li G Abelova grupa, pak $aH = Ha$ pro každé $a \in G$. Počet různých (levých) tříd se nazývá index podgrupy H v grupě G , značí se $[G : H]$.

Tvrzení: Pro každé $a \in G$ je $|aH| = |H|$.

Všechny levé třídy jsou rozklad na množinu G , tj. $G = \bigcup_{a \in G} aH$ a třídy aH, bH jsou buď stejné, nebo disjunktní.

Lagrangeova věta: Nechť G je konečná grupa a H je podgrupa grupy G . Pak rád podgrupy H dělí rád grupy G , tj. $|G| = [G : H] \cdot |H|$.

Dk: $(G, *)$ je grupa s neutrálem 1 , H je podgrupa G .

1) $\lambda: G \rightarrow G: x \mapsto ax$, robařem λ je bijekce

$aH = \{a \cdot h \mid h \in H\} = \lambda(H)$ je levá třída podle podgrupy H reprezentovaná prvkem a . Protože λ je bijekce, platí $|H| = |aH|$.

2) Ukažeme, že $\{aH \mid a \in G\}$ tvorí rozklad množiny G na třídy, když je sjednocen třídou po celou G , a třídy lze doložit po chování disjunktnosti

- $\bigcup_{a \in G} aH = G$ (tj. $\forall 1 \in H$. Pak o každém $a \in G$ můžeme říct $a = a \cdot 1 \in aH$)

- třídy jsou disjunktní, když: $aH \cap bH \neq \emptyset \Rightarrow aH = bH$ (to chci ukažat)

Když $c \in aH \cap bH$, tak $c = ah = bh$, kde $h, h^{-1} \in H$

$$ah = bh \Leftrightarrow h^{-1}a = b$$

$$a = bhh^{-1}$$

Protože $h \in H$ i $h^{-1} \in H$, můžeme $h^{-1} \in H$ a taky $h^{-1}h \in H$. Tidíme, že nemáme podarilo najít $a = bh$, $h \in H$, proto $a \in bH$, obecněji $aH \subseteq bH$. Obdobně bychom ukažali, že $bH \subseteq aH$, když vidíme, že $aH = bH$.

Tidíme, že aH skutečně tvorí rozklad G na třídy.

3) Ukažeme velikost $|G|$:

$$|G| = \sum |aH| = \sum |H| = [G : H] \cdot |H|$$

↑ pás všechny různé aH , celkem pás $[G : H]$ různých tříd

Pozn: Lagrangeova věta neplatí pro pologrupy a podpologrupy, protože v nich nemají inverze, která je potřeba k důkazu.

Př: $(\mathbb{Z}_{12}, +)$, $H = 4 \cdot \mathbb{Z}_{12} = \{0, 4, 8\}$ $\mathbb{Z}_{12} = \{0, 1, 2, 3, \dots, 10, 11\}$

Třídy podle H : $0+H = H = \{0, 4, 8\}$

$$1+H = \{1, 5, 9\}$$

$$2+H = \{2, 6, 10\}$$

$$3+H = \{3, 7, 11\}$$

$$U = \{0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7, 11\} = \mathbb{Z}_{12}$$

a třídy jsou disjunktní.

Cvičení
14.3.2019

Útok insidéra: Bobův RSA veřejný klíč je $(n, e) = (533, 17)$ a jeho klíč je $(n, d) = (533, 113)$. Faktorizuje n na ráhodné malosti r, d.

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

$$e \cdot d - 1 = 1921 - 1 = 1920 = 2^7 \cdot 3 \cdot 5$$

- algoritmus na faktorizaci n se malostí veřejného i soukromého klíče

1) spočti r takové, že $e \cdot d - 1 = 2^r \cdot l$, kde l je liché

2) nájdě a $\in \mathbb{Z}_n$ náhodně

$$\uparrow d = \gcd(a, n)$$

if $d > 1$:

return d

else:

$$c = a^2 \pmod{n}$$

dokud $c^2 \neq 1$, počítej $c = c^2$

if $\sqrt{c} \neq -1$:

return $\gcd(\sqrt{c} \pm 1, n)$

else]

Už máme $r = 7$, $l = 15$ je liché, nájdeme $a = 2$. Ráhodné neplatí $\gcd(2, 533) > 1$, proto jdeme počítat $c = a^l$

$$c = a^l = 2^{15}, 15 = 8 + 4 + 2 + 1 = 1111 = XSXSXSX$$

$$2XSXSXSX \rightarrow 4XSXSX = 8SX = 64SX = 128SX = 16384X = 394X = 255 = c$$

$$255^2 = 532 = -1, -1^2 = 1 \quad \text{Takže najde, že } b^2 = 1, \text{ ale } b \neq \pm 1$$

Nášli jsme $a = 3$

$$c = a^l = 3^{15}$$

$$3XSXSXSX \rightarrow 9XSXSX \rightarrow 27XSX \rightarrow 729XSX \rightarrow 196XSX \rightarrow 588SX \rightarrow 55SX \rightarrow$$

$$\rightarrow 3025X \rightarrow 360X = 1080 = 14, 3^{15} = 14 \pmod{n} \quad \text{R} 533$$

$$14^2 = 196, 196^2 = 38416 = 40, 40^2 = 1600 = 1$$

Nášli jsme b, kde $b^2 = 1$ a $b \neq \pm 1$, tedy $b = 40$

Máme $b = 40, b^2 = 1, a \in \mathbb{Z}_{533}$ a vlastností b platí $(b+1) \cdot (b-1) = b^2 - 1 = 0 \pmod{n}$

Vyjádříme ale platí $0 = l, p \cdot l, q = k \cdot p \cdot q = k \cdot n$

A toho vidíme, že $\gcd(b \pm 1, n) = p$ nebo q:

$$\gcd(41, 533) \Rightarrow (\text{luktidem}) \dots 533 = 13 \cdot 41 + 0, \gcd(41, 533) = 41 = p$$

$$q = 533 / 41 = 13$$

Nášli jsme faktory $p = 41, q = 13$

asouběžný (91, 29)

Př: Bob má veřejný klíč $(91, 11)$, Cecília má veřejný klíč $(91, 5)$. Alice poslala Bobovi správu $b = 31$. Cecília provede číslo insidéra a správu vypočítá:

$$e \cdot d - 1 = 29 \cdot 5 - 1 = 145 - 1 = 144 = 12^2 = 3^2 \cdot 4^2 = 3^2 \cdot 2^4 \approx 2^4 \cdot 9$$

$$\Rightarrow r = 4, l = 9$$

$$a = 2? \quad 2^l = 2^9 = 512 = 57 \pmod{91} \quad 57^2 = 64, 64^2 = 4096 = 1 \pmod{91} \Rightarrow b = 64$$

$$\gcd(65, 91)^2$$

$$\begin{pmatrix} 1 & 0 & 65 \\ 0 & 1 & 91 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 65 \\ -1 & 1 & 26 \end{pmatrix} \sim \begin{pmatrix} 3 & -2 & 13 \\ -1 & 1 & 26 \end{pmatrix} \sim \begin{pmatrix} 3 & -2 & 13 \\ -7 & 5 & 0 \end{pmatrix}$$

$$\gcd(65, 91) = 13 \quad 13 \mid 91 \quad \text{a} \quad q = 7$$

$$n = 7 \cdot 13 = 91$$

$$\varphi(n) = 6 \cdot 12 = 72$$

Závěr: sítka je a $\varphi(n)$ spočítáme Bobův d

$$e \cdot d = 1 \pmod{72}$$

$$11d - 1 = 0 \pmod{72}$$

$$11d + 72k = 1$$

d k

$$\left(\begin{array}{cc|c} 1 & 0 & 11 \\ 0 & 1 & 72 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 0 & 11 \\ -6 & 1 & 6 \end{array} \right) \sim \left(\begin{array}{cc|c} 13 & -2 & -1 \\ -6 & 1 & 6 \end{array} \right) \sim \left(\begin{array}{cc|c} -13 & 2 & 1 \\ -6 & 1 & 6 \end{array} \right) \approx \frac{-13 \cdot 11}{d} + 2 \cdot 72 = 1$$

\Rightarrow Bobův soukromý klíč je $(91, 59)$

$$-13 = 59 \pmod{72}$$

Rámcem řešení:

$$31^d, d=59 = 32+16+8+2+1 = 111011 \approx XSXSXSSXSX$$

Tobž muselo dojít, abělámlo to pro čínskou větu

$$31^{59} \pmod{7} = (31^5 \pmod{7}) \cdot q_7 + (31^{59} \pmod{13}) \cdot q_3$$

$$\pmod{7}: 31^{59} = (28+3)^{(54+5)} = 3^5 = 27 \cdot 9 = (-1) \cdot 2 = -2 = 5$$

$$\pmod{13}: 31^{59} = (26+5)^{(48+11)} = (5)^{11} = (5)^{4+4+3} = 625 \cdot 625 \cdot 125 = 1 \cdot 1 \cdot 8 = 8$$

$$q_7 = 13+ = 1 \pmod{7} \quad A = 6 \Rightarrow 13 \cdot 6 = 78 \pmod{91}$$

$$q_{13} = 7+ = 1 \pmod{13} \quad 4 = 2 \Rightarrow 7 \cdot 2 = 14 \pmod{91}$$

$$31^{59} = 5 \cdot q_7 + 8 \cdot q_{13} = 5 \cdot 78 + 8 \cdot 14 = 390 + 112 = \underline{\underline{502}}$$

Zpráva pro Bota je 47.

Alici $(91, 5)$ a Bobovi s veřejným klíčem $(91, 11)$ přišla stejná zpráva a, zašifrována jako $b_a = 32, b_b = 46$. Proveďte útok outsidera a našlete a.

Veřejné klíče jsou nesoudelné, proto je dokážeme Bezoutovm vyjádřit jako $1 = 1_1 \cdot 5 + 1_2 \cdot 11$

$$\left(\begin{array}{cc|c} 1 & 0 & 5 \\ 0 & 1 & 11 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 0 & 5 \\ -2 & 1 & 1 \end{array} \right) \sim \left(\begin{array}{cc|c} 11-5 & 0 \\ -2 & 1 & 1 \end{array} \right) \Rightarrow -2 \cdot 5 + 1 \cdot 11 = 1 \quad \begin{matrix} 1_1 = -2 \\ 1_2 = 1 \end{matrix}$$

$$\text{Využijeme toho, že } b_a^{1_1} \cdot b_b^{1_2} = a^{e_a \cdot 1_1} \cdot a^{e_b \cdot 1_2} = a^{e_a \cdot 1_1 + e_b \cdot 1_2} = a^1$$

$$a = b_a^{1_1} \cdot b_b^{1_2} = 32^{-2} \cdot 46^1 = (32^2)^{-1} \cdot 46 = (1024)^{-1} \cdot 46 = (23)^{-1} \cdot 46 = 4 \cdot 46 = 184 = 2$$

Zpráva pro Alici a Boba je 2.

Alici a Bobovi přišla shodnými klíči zašifrována správa $b_a = b_b = 65$. Spočítejte a.

Veřejné klíče jsou nesoudelné a víme, že $-2 \cdot 5 + 1 \cdot 11 = 1$.

$$a = b_a^{1_1} \cdot b_b^{1_2} = 65^{-2} \cdot 65 = 65^{-1}$$

Odejmme malit x, aby $65x + 91k = 1$

$$\left(\begin{array}{cc|c} 1 & 0 & 65 \\ 0 & 1 & 91 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 0 & 65 \\ -1 & 1 & 26 \end{array} \right) \sim \left(\begin{array}{cc|c} 3 & -2 & 13 \\ -1 & 1 & 26 \end{array} \right) \sim \left(\begin{array}{cc|c} 3 & -2 & 13 \\ -7 & 5 & 0 \end{array} \right)$$

Vidíme, že $\gcd(91, 65) = 13$, takže rovnice nás nejdá řešit a my neumíme límo spůsobem spočítat a. Ale protože jsme našli delitele 91, když 13, můžeme faktorizovat $91 = 13 \cdot 7$, a majit správu jiným spůsobem:

$$\varphi(n) = 12 \cdot 6 = 72, \quad e \cdot d_a = 1 \pmod{72} \Rightarrow 5d_a + 72k = 1$$

$$\left(\begin{array}{cc|c} 1 & 0 & 5 \\ 0 & 1 & 72 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 0 & 5 \\ -14 & 1 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 29 & -2 & 1 \\ -14 & 1 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 29 & -2 & 1 \\ 72 & 5 & 0 \end{array} \right) \quad d_a = 29, \quad a = b_a^{d_a} = 65^{29}$$

Využijeme hodnoty $q_7 = 78$ a $q_{13} = 14$, které jsme počítali následně na slouunce.

$$\pmod{7}: 65^{29} = 2^5 = 32 = 4$$

$$\pmod{13}: 65^{29} = 0^{29} = 0$$

$$a = q_7 \cdot 4 + q_{13} \cdot 0 = 78 \cdot 4 = \underline{\underline{312}}$$

Zpráva byla $a = 39$.

Práce: Najděte řetězový zlomek pro $\frac{73}{15}$ a spočtěte řečeny konvergenty.

$$\frac{73}{15} = 4 + \frac{13}{15} = 4 + \frac{1}{\frac{15}{13}} = 4 + \frac{1}{1 + \frac{2}{13}} = 4 + \frac{1}{1 + \frac{1}{\frac{13}{2}}} = 4 + \frac{1}{1 + \frac{1}{6 + \frac{1}{2}}}$$

$$0: (4) = 4$$

$$1: (4, 1) = 4 + \frac{1}{1} = 5$$

$$2: (4, 1, 6) = 4 + \frac{1}{1 + \frac{1}{6}} = 4 + \frac{1}{7/6} = 4 + \frac{6}{7} = \frac{34}{7} \approx 4.86$$

$$3: (4, 1, 6, 2) = \frac{32}{15}$$

Práce: Proveďte Wienerův útok na RSA s nejedním klíčem (55751, 22109)

Pokud se p a q lze rozložit na jeden bit, takže $q < p < 2q$, $d < \frac{1}{3}\sqrt{n}$, pak by měl $\frac{e}{d}$ byl jehož je konvergentským členem $\frac{k}{d}$

$$\text{Euklid: } 22109 = 0 \cdot 55751 + 22109$$

$$55751 = 2 \cdot 22109 + 11533$$

$$22109 = 1 \cdot 11533 + 10576$$

$$11533 = 1 \cdot 10576 + 957$$

$$10576 = 11 \cdot 957 + 49$$

$$957 = 19 \cdot 49 + 26$$

$$49 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

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

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

$$= \frac{1}{\frac{5}{2}} = \frac{2}{5}$$

$$k=2, d=5, \varphi(n) = \frac{22109 \cdot 5 - 1}{2} = 55272, \text{ kde by možná šlo:}$$

$$\varphi(n) = (p-1)(q-1) = p \cdot q - (p+q) + 1 = 55751 + 1 - (p+q) = 55752 - (p+q)$$

$$p+q = 55752 - 55272 = 480$$

$$p \cdot q = 55751$$

$$x^2 - 480x + 55751 = 0 \quad D = b^2 - 4ac = 7396 = 86^2$$

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a} = \frac{480 \pm 86}{2} < 283$$

$$< 197$$

Následujeme použitáho $p = 197, q = 283$ příslušné klíče (55751, 22109).

$$\Rightarrow \varphi(n) = (0, 2, 1, 1, 11, 19, 2, 1, 7, 1, 2)$$

$$\text{Konvergenty: } \begin{aligned} (0, 2) &= 0 + \frac{1}{2} = \frac{1}{2} \quad (= lisy má \frac{k}{d}, \varphi(n) = \frac{ed-1}{k}) \\ (0, 2, 1) &= 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3} \end{aligned}$$

$$k=1, d=2, \varphi(n) = \frac{22109 \cdot 2 - 1}{1} = 44217$$

Totéž $\varphi(n)$ je opatrně, protože je liché

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

$$k=1, d=2, \varphi(n) = \frac{22109 \cdot 3 - 1}{2} = 66326$$

Také ne, nemá dělitelné 4 a návíc je menší než n .

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