TEORIE ČÍSEL

- <u>složitost aritmetiky pro b-bit. čísla</u>: add/sub $\Theta(b)$
  mul $O(b^2)$, dokonce $O(b)$ [ale s obří konst.]
  div/mod ... o trochu horší než mul, rozhodně $O(b^2)$
  - modulární umocňování:
    $a^k \bmod N$ pomocí $O(\log k) \times$ mul
    $\rightarrow$ pro b-bit. čísla $O(b^3)$
- <u>Euklidův algoritmus</u>: $O(b)$ průchodů $\rightarrow$ celkem $O(b^3)$
  - lepší analýza / binární GCD $\rightarrow O(b^2)$
  - značení: $\gcd(x,y)$, $x \perp y \Leftrightarrow \gcd(x,y)=1$ (nesoudělnost)
  - rozšířený E.a.: spočte $\underbrace{u,v \in \mathbb{Z}}_{\text{Bézoutovy koeficienty}}$: $ux + vy = \gcd(x,y)$
- <u>počítání mod N</u>: $\mathbb{Z}_N$ je okruh ... kdy je prvek invertibilní?
  - řešíme kongruenci $ax \equiv b \pmod N$ ... a,b známe; x hledáme
  - ekvivalentní s: $\exists y \in \mathbb{Z}: ax - Ny = b$
    1. pokud $b = \gcd(a,N)$: Bézoutovy koef. dají x,y
    2. pokud $b = c \cdot \gcd(a,N)$: jako předtím, nakonec vynásobíme c
    3. jinak nemá řešení: levá strana je dělitelná $\gcd(a,N)$, pravá ne
  - a je invertibilní $\Leftrightarrow a \perp N$
    ↳ $\mathbb{Z}_N^*$: <u>multiplikativní grupa</u> mod N [je to grupa]
  - pokud N je prvočíslo, invertibilní je vše kromě $0 \Rightarrow \mathbb{Z}_p$ je těleso.
  - inverze umíme počítat efektivně
- <u>Malá Fermatova věta</u>: pokud $x \perp p$, pak $x^{p-1} \overset{p}{\equiv} 1$.
  (díky tomu x^{p-2} je inverze x, to dává jiný efektivní alg.)

↳ zobecnění: <u>Eulerova věta</u>: pokud $x \perp N$, pak $x^{\varphi(N)} \overset{N}{\equiv} 1$
  - zde $\varphi(N) = |\mathbb{Z}_N^*|$, tedy $\# a \in \mathbb{Z}_N : a \perp N$
  - Dk.: $x^0, x^1, x^2, \ldots x^k$ je nějaká podgrupa $\mathbb{Z}_N^*$, říkejme jí třeba H

↳ x^k bude první 1 kromě x^0

Lagrangeova věta: Je-li G konečná grupa a $H \leq G$, pak $|H| \backslash |G|$.
(nám stačí pro komutativní grupy)

$\rightarrow$ podle Lagrange: $|H| \setminus |\mathbb{Z}_N^*| = \varphi(N)$

tohle je k

$\rightarrow \varphi(N) = k \cdot c$ pro nějaké c

$\rightarrow x^{\varphi(N)} \equiv (x^k)^c \equiv 1^c = 1.$

- **Čínská zbytková věta** (CRT): Pokud $N_1 - N_k$ navzájem nesoudělné a $N = \prod_1^k N_i$, pak $\mathbb{Z}_{N_1} \times \_ \times \mathbb{Z}_{N_k} \cong \mathbb{Z}_N$

dokonce isomorfismus, navíc efektivní

Dk: BÚNO $k=2$, dál se pokračuje indukcí (triv.)

① Nekonstruktivně: $f(x) := (x \bmod N_1, x \bmod N_2)$

je zobrazení z $\mathbb{Z}_N$ do $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$

$\rightarrow$ je prosté $\Rightarrow$ je také na (vede mezi stejně velkými množinami)

② Konstruktivně: Chci vzor dvojice (a_1, a_2).

Najdu čísla u_1, u_2 t.ž. $f(u_1) = (1,0)$, $f(u_2) = (0,1)$

$\hookrightarrow$ pak stačí položit $x := a_1 u_1 + a_2 u_2$ (vše mod N)

$\hookrightarrow$ kde je vzít: $f(N_2) = (q, 0)$ ... pokud $q = 1$, vyhrál jsem a mám u_1

... jinak násobím N_2 inverzí q mod N_1 (vím, že $q \neq 0$)

$\rightarrow$ podobně u_2.

- **Výpočet $\varphi(N)$:**
  - $\varphi(p) = p - 1$ [už víme]
  - $\varphi(p^k) = (p-1) \cdot p^{k-1}$
  - pro $x \perp y$ máme $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ ... to je vidět z CRT

$\Rightarrow \varphi(N)$ umíme spočítat, pokud známe faktorizaci N

- **Faktorizace vs. prvočíselnost**

považuje se za těžkou:
- přímočaré alg. jsou exponenciální
- umí se různé subexponenciální (čím dál lepší)
- kvantové počítače umí polynomiálně [Shor]

snadná...
- rychlé pravděpodobnostní testy s 1strannou chybou
- poly alg. [Agarwal et al. 2002] ... zatím nepříliš praktické

- Pravděpodobnostní testy prvočíselnosti

  "Euklidův svědek"

  - Fermatův test: pro náhodné $x \in \mathbb{Z}_N$ spočítáme $x^{N-1} \bmod N$.
    - → pokud nevyjde 1, N je složené [x je Fermatův svědek]
      - ↳ buď proto, že $x \not\perp N$, nebo díky F. větě
    - Jaká je Pr, že složené číslo projde testem? Kolik je svědků?
      - bohužel existují Carmichaelova čísla (nejmenší je 561), pro než $\forall x \in \mathbb{Z}_N^*\ x^{N-1} \overset{N}{\equiv} 1$ ... mají jen Euklidovy svědky a těch je málo
        - → Carm. čísel je nekonečně mnoho [Alford et al. 1994]
      - pokud N není Carm., už to dopadne dobře:
        $H := \{ x \in \mathbb{Z}_N^* \mid x^{N-1} \overset{N}{\equiv} 1 \}$ je podgrupa $\mathbb{Z}_N^*$
        ... přitom $H \neq \mathbb{Z}_N^*$, takže podle Lagrangeovy věty $|H| \leq \frac{|\mathbb{Z}_N^*|}{2}$
        $\Rightarrow$ Pr[x je svědek] $\geq 1/2$.
  - Rabinův-Millerův test:
    1. $x \in_R \{1 \ldots N-1\}$
    2. pokud $\gcd(x,N) \neq 1$: SLOŽENÉ (Euklidův svědek)
    3. spočítáme [pozpátku]
       $x^{N-1} \bmod N$ ← pokud není 1: SLOŽENÉ (Fermatův svědek)
       $x^{\frac{N-1}{2}} \bmod N$
       ⋮
       $x^{\frac{N-1}{2^t}} \bmod N$
       Pokud jsou 1, pokračujeme. Pokud −1: PRVOČÍSLO. Jinak SLOŽENÉ (Riemannův svědek)

       zastavíme se, až bude exponent lichý → odpovím PRVOČÍSLO

    Pokud odpovím SLOŽENÉ, je to pravda

    Věta [Rabin]: Pr[PRVOČÍSLO | x složené] $\leq 1/4$

    Věta [Miller]: Pokud platí zobecněná Riemannova hypotéza, $\exists$ svědek $\in O(\log N)$.

- Generování velkých prvočísel: náhodně tipujeme a testujeme, hustota prvoč. kolem N je cca $1/\ln N$

- **Diskrétní logaritmy**
  - Věta: $\mathbb{Z}_p^*$ je cyklická grupa → $\exists g$ (generátor) t.ž. $\{g^0, g^1, \dots, g^{p-2}\} = \mathbb{Z}_p^*$
  - Jinými slovy $\mathbb{Z}_p^* \cong (\mathbb{Z}_{p-1}, +)$

    ↳ isomorfismus je v jednom směru umocňování, v druhém diskrétní log.

    umocňování ↓ poly. alg.

    diskrétní log. ↳ podobně těžké jako faktorizace – subexp. / kvantově poly.
  - Jak ověřit, zda g je generátor?

    Pokud není, pak $H := \{g^0, g^1, \dots\}$ je nějaká podgrupa $\mathbb{Z}_p^*$ ⇒ $|H| \backslash \varphi(p) = p-1$

    → $g^{\frac{p-1}{k}} \equiv 1$ pro nějaké přirozené k … dokonce stačí prvočíselné k.

    → jakmile známe faktorizaci $p-1$, umíme to otestovat (dost rychle, protože faktorů je $O(\log p)$).
- Jak najít generátor? Náhodně vybíráme a testujeme…

  Kolik je generátorů?

  → pokud g je gen., pak g^k je gen. ⇔ $k \perp p-1$

  → # generátorů $= \varphi(p-1)$ … to je dost (nepočítáme přesnou Pr…)

- **Diskrétní odmocniny**
  - v $\mathbb{Z}_5$: $1^2 = 4^2 = 1$, $2^2 = 3^2 = 4$ ⇒ 1, 4 mají 2 odmocniny "kvadratické zbytky" (QR)

    2, 3 nemá žádnou

    0 má právě 1
  - Obecně mod p: kromě 0 má polovina čísel 2 odmocniny, zbytek žádnou.
    - nejvýše 2: jsou to kořeny kvad. polynomu
    - pokud $x^2 = a$, pak také $(-x)^2 = a$

      … kromě $x = -x$ (jen pro $x = 0$) ~~jsou vždy~~ je odmocnin sudý počet
    - nechť g je generátor $\mathbb{Z}_p^*$: g^{2k} má 2 odmocniny } takových čísel je $\frac{p-1}{2}$

      ↳ na čísla g^{2k+1} už žádné odmocniny nezbyly

  ⇒ sudost/lichost $\mathrm{dlog}(x)$ prozradí, zda x je QR.

- Množina všech QR tvoří podgrupu $\mathbb{Z}_p^*$. (1 je QR, QR·QR je QR)
- Testování QR: x je QR $\Leftrightarrow$ $x^{\frac{p-1}{2}} \overset{p}{\equiv} 1$. (Eulerovo kriterium)

  Dk: $(g^{2k})^{\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1^k \equiv 1$

  $(g^{2k+1})^{\frac{p-1}{2}} \equiv g^{k(p-1)} \cdot \underbrace{g^{\frac{p-1}{2}}}_{\text{tohle je } \sqrt{1}\text{, takže } -1} \equiv -1$

  } $x^{\frac{p-1}{2}}$ je tedy homomorfismus $\mathbb{Z}_p^* \to (\{-1,1\},\cdot)$ indikující QR (Legendreův symbol)

- Jak počítat $\sqrt{x}$?
  - pokud $p = 4t+3$: $\left(x^{\frac{p+1}{4}}\right)^2 \equiv x^{\frac{p+1}{2}} \equiv \underbrace{x^{\frac{p-1}{2}}}_{1 \text{ dle Eul. kriteria}} \cdot x \equiv x$
  - pro $p = 4t+1$: randomizovaný alg. [Tonelli 1891, Shanks 1973]
- Odmocniny mod složené N: Pokud umíme N faktorizovat, použijeme CRT, jinak těžké.

RSA [Rivest, Shamir, Adleman 1978 ; GCHQ 1973, but public 1997]

Klíč: $n = p \cdot q$ — p, q dvě různá velká prvočísla [modulus]

$\varphi(n) = (p-1)(q-1)$

e t.ž. $e \perp \varphi(n)$ [šifrovací exponent]

d t.ž. $ed \equiv 1 \pmod{\varphi(n)}$ [dešifrovací exponent]

$\to$ šifrovací klíč (e,n), dešifrovací klíč (d,n).

$\to$ 1 veřejný, 2. tajný

} idea: bez faktorizace n je těžké z jednoho klíče spočítat druhý

Šifra: $E(x) = x^e \bmod n$

$D(x) = x^d \bmod n$

} zprávy jsou prvky $\mathbb{Z}_n$

Korektnost: $(x^e)^d \equiv x^{ed} \equiv x^{k\cdot\varphi(n)+1} \equiv \underbrace{\left(x^{\varphi(n)}\right)^k}_{1} \cdot x \equiv x$.

! Tohle sedí, pokud $x \perp n$

$\to$ mohu důkaz opravit pomocí CRT (dokáži zvlášť mod p a mod q)

$\to$ ale pokud se do takového x trefím, mám jiné problémy

Efektivita: Poly, ale pomalé... často stavíme hybridní šifru z RSA a sym. šifry

Triky na zrychlení:
- volím malý veřejný e (třeba 3 nebo 17)
- dešifrování pomocí CRT (menší čísla ⇒ rychlejší aritmetika) (to v tajném směru mohu)

Důležité vlastnosti:
- komutuje: $D_{k_1}(D_{k_2}(E_{k_1}(E_{k_2}(x)))) = x$ (pro klíče se stejným modulem)
- klíče lze prohodit (ale nebývá bezpečné používat oba směry v jednom protokolu)
- **homomorfní šifra**: $E(x \cdot y) \equiv E(x) \cdot E(y)$

↳ to je většinou spíš k vzteku, ale má to i hezké aplikace:

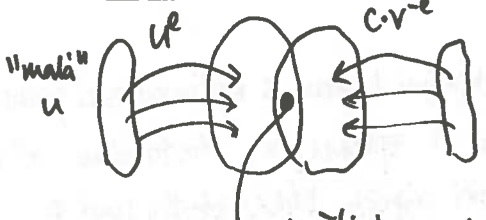
Slepé podpisy
- Alice podepisuje libovolné zprávy (šifruje je tajným e)
- Bob si chce nechat podepsat x, ale nechce, aby ho A. znala
- Bob vygeneruje $r \in_R \mathbb{Z}_N^*$, pošle Alici $x \cdot r^d \bmod n$.
- Alice spočítá $(x \cdot r^d)^e \equiv x^e \cdot r^{ed} \equiv x^e \cdot r$
- Bob výsledek vynásobí inverzí r a získá x^e.
- Alice (až na případy $x \notin \mathbb{Z}_n^*$) nezjistí o x nic.

(viz protokoly na digitální peníze)

Útoky:
- pokud $x < n^{1/e}$, stačí spočítat odmocninu v $\mathbb{Z}$, což je poly.
- známe-li $\varphi(n)$, můžeme faktorizovat n:
$$\left.\begin{array}{l} n = pq \\ \varphi(n) = \underbrace{(p-1)(q-1)}_{pq-p-q+1} \end{array}\right\} \text{soustava rovnic, snadno řešitelná}$$
- je-li $d < n^{1/4}$, lze ho spočítat z e [Wiener 1990]

  ⇒ malý si můžeme dovolit jen veřejný exponent
- z d, e lze spočítat $\varphi(n)$ randomizovaným alg. (viz Stinson & Paterson)
- **Meet in the middle**:

... máme $c = m^e$ (c známe, m neznáme)



↳ našli jsme u,v: $u^e \equiv c \cdot v^{-e}$

Jak velká u,v potřebujeme?

$$u^e \cdot v^e \equiv c$$
$$(uv)^e \equiv c$$
$$uv \equiv m$$

$$\Pr[\exists u,v \le n^{\frac{1}{2}+\varepsilon} : uv \equiv m] \ge \text{const.}$$

⇒ útok hrubou silou stihneme za $\sim\sqrt{n}$ pokusů!

- Podobné zprávy: Pokud známe $c \equiv m^e$, $c' \equiv (m+\delta)^e$
  ... m je spol. kořen polynomů $p(x) = x^e - c$, $p'(x) = (x+\delta)^e - c'$
  → pokud $\underbrace{\text{je } \gcd(p, p') \text{ lineární}}_{\text{nastane s velkou psti}}$, známe m.
  potřebuji malé e
- Částečně známé zprávy: stačí hádat neznámé bity (netriviální!)
- p, q blízko u sebe → faktorizace:
  Nechť $q = p + 2d$. Potom $n = pq = p(p+2d) = p^2 + 2dp$,
  takže $n + d^2 = p^2 + 2dp + d^2 = (p+d)^2$
  ⇒ mohu zkoušet různá d a odmocňovat $n + d^2$.
- Více klíčů používá stejný modul: Jednak může každý majitel priv. klíče faktorizovat n, jednak při poslání téže zprávy více příjemcům může Eva dešifrovat. [bez důkazu, viz Stinson, Cvič. 6.17]
- Tatáž zpráva zašifrovaná klíči s různými moduly:
  ukážeme pro $e=3$ a 3 odchycené zprávy.
  toto je lepší

  Víme: $x^3 \equiv c_1 \pmod{n_1}$
  $x^3 \equiv c_2 \pmod{n_2}$
  $x^3 \equiv c_3 \pmod{n_3}$

  Nyní: $N := n_1 \cdot n_2 \cdot n_3$
  jistě $x^3 < N$
  ... ale díky CRT je toto x^3 jednoznačně určeno zbytky c_1, c_2, c_3
  → umíme najít x^3 v $\mathbb{Z}$
  → stačí odmocnit v $\mathbb{R}$.

- Chyba při výpočtu
  - Nechť Alice podepisuje tajným klíčem s optimalizací pomocí CRT
  - Opakovaně podepisujeme 1 zprávu, x, dostáváme $x^e \bmod n$.
  - Pokud A. udělá chybu při výpočtu BÚNO zbytku mod p, vydá výsledek lišící se o násobek q: $\gcd(\text{výsledek} - x^e \bmod n, n)$ prozradí q!

⇒ útočník se může snažit chyby uměle vyvolávat.

Sémantická bezpečnost RSA

↳ žádná vlastnost plaintextu (efektivně testovatelná) nemá jít efektivně zjistit z ciphertextu

- RSA zachovává Jacobiho symbol (to je cca 1 bit informace)

Df: • Legenderův symbol $\left(\frac{a}{p}\right)$ pro p prvočíslo $:= a^{\frac{p-1}{2}} \bmod p$

☼ +1 pokud a je QR, −1 není-li QR, 0 pro $p \mid a$

• Jacobiho symbol to generalizuje pro liché složené $n = \prod_{i=1}^{k} p_i^{\alpha_i}$:

↳ $\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}$

⇒ pro $a \perp n$ je $Pr\left[\left(\frac{a}{n}\right) = 1\right] = 1/2$

⇒ $\left(\frac{a}{n}\right)$ nese $1 \pm \varepsilon$ bitů informace

☼ 0 pokud gcd(a,n)>1, jinak je to ±1 → −1 ⇒ a není QR
+1 ⇒ může, ale nemusí

- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$ [nejprve dokážeme pro L. symbol]
- existuje poly alg. pro výpočet $\left(\frac{a}{n}\right)$, který nepotřebuje faktorizaci n

využívá $\left(\frac{a}{n}\right) = \left(\frac{a'}{n}\right)$ pro $a' \equiv a \pmod n$

$\left(\frac{a}{n}\right) \cdot \left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}} \cdot (-1)^{\frac{n-1}{2}}$ [Gaussův zákon kvadratické reciprocity – netriviální]

a pak je podoben Euklidovu alg.

... ale to je jediné známé prosakování informace!

- Def. $half(x) := [D(x) > n/2]$, $parity(x) := D(x) \bmod 2$

↑ indikátor 0/1

Věta: Umíme-li $\underbrace{\text{spočítat } half(x)}_{\text{máme-li na to orákulum}}$, umíme i ~~...~~ počítat $D(\ldots)$.
tedy invertovat RSA

Dk: ~~zapíšeme x jako n·α, kde α∈[0,1), mějme~~
~~half(Mějme ... c = m~~

Mějme $y = x^e$. Známe y, chceme zjistit x.
Jistě je $x = n \cdot \alpha$ pro nějaké $\alpha \in [0,1)$, které zapíšeme binárně.
half(y) nám řekne nejvyšší bit α
half($y \cdot 2^e$) nám řekne nejvyšší bit $2\alpha \bmod 1$,
$D(y \cdot 2^e) = 2x$ což je 2. nejvyšší bit α

... atd. a za $\log n$ pokusů známe α': $|\alpha - \alpha'| < \frac{1}{2n}$

⇒ $\alpha' \cdot n$ po zaokrouhlení dá x.

Analogicky pro parity(x). Ono totiž platí:

- $half(x) = parity(x \cdot 2^e)$ $\Rightarrow$ pomocí orákula pro paritu můžeme počítat half v předchozím důkazu.

Padding – nechceme pomocí RSA šifrovat surovou informaci (hrozí, že bude moc malá apod., stejně tak RSA je deterministické $\Rightarrow$ není CPA-bezpečné)
↳ a hrozí multi-modulový útok

PKCS #1 v1.5
↑ Public-key Crypto. Std. od RSA Security Inc.

00 02 [random] 00 [zpráva]

- random: aspoň 8 náhodných bytů různých od 00
- 00: část se nevyužije, pokud $\lceil \log n \rceil$ není násobek 8
- 02: typ paddingu (00 a 01 jsou deterministické)

Bleichenbacherův útok [1998]: zneužití paddingového orákula (řekne, zda dešifrovaná zpráva má správný formát paddingu – to může být třeba časový postranní kanál)

Nechť x je správně opadovaná zpráva, známe $y = x^e$.
↳ $2B \le x < 3B$ pro nějakou mocninu dvojky B (danou pozicí 02 v paddingu)

Ptáme se orákula na $y \cdot s^e$ pro různá s … tedy zda $x \cdot s$ je správná.
Odhadněme Pr, že to tak bude (heuristicky - předpokládáme náhodnost D)

① $Pr[\underbrace{2B \le xs \bmod n < 3B}] \ge 2^{-16}$
nejvyšších max. 16 bitů má správný tvar

② Pr[za 00 02 je 8 nenul a pak aspoň 1 nula]
$= \left(\frac{255}{256}\right)^8 \cdot \left(1 - \left(\frac{255}{256}\right)^{k-10}\right) \ge 0.18$
k: # bytů; ≥ 0.18 pro $k \ge 64$ (aspoň 512b klíč)

} Pr[obojí najednou] $\ge 2.8 \cdot 10^{-6}$
$\Downarrow$
cca za průměrně 10^6 pokusů se to povede

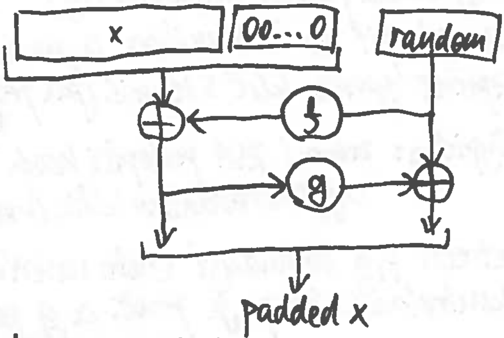
Co se dozvíme o x?

- $2B \le xs \bmod n < 3B \Rightarrow \exists r: 2B \le xs - rn < 3B$
$\Rightarrow \exists r: \left\lceil \frac{2B + rn}{s} \right\rceil \le x \le \left\lfloor \frac{3B - 1 + rn}{s} \right\rfloor$

To je nějaký interval … ale my neznáme r $\Rightarrow$ spousta intervalů $(\sim 2^{16})$

Velmi zhruba: začneme intervalem $[2B, 3B)$, každý další pokus ho protne se sjednocením intervalů.
Heuristicky: intervalů dlouhodobě ubývá a zkracují se
⇒ časem je x jednoznačně určeno.

PKCS #1 v2.0 – protokol OAEP, netrpí těmito neduhy
– v podstatě je to Feistelova síť se 2 rundami



díky tomu je reverzibilní

f, g jsou hešovací funkce

Obecně k bezpečnosti RSA

- spoléhá na obtížnost faktorizace (ale není s ní ekvivalentní?)
- má algebraickou strukturu ⇒ randomizujeme, hešujeme apod.
- je potřeba používat ho velmi opatrně

$\boxed{\text{Rabinův kryptosystém}}$ – založený na diskrétních odmocninách

Tajný klíč: prvočísla p, q
Veřejný klíč: $n = p \cdot q$
$E(x) = x^2 \bmod n$
$D(y)$ počítá diskrétní odmocninu
- to jde se znalostí faktorizace lehko (zvlášť mod p, mod q, pak CRT)
- pozor, vyjdou 4 možná řešení, je nutno nějak zjednoznačnit (hash?)

To bohužel také ukazuje, že CCA faktorizuje n!

Bezpečnost: Pokud umíme dešifrovat, umíme i faktorizovat modul (aspoň randomizovaně):
$a \leftarrow$ náhodně ze $\mathbb{Z}_n$
$b \leftarrow D(a^2)$
Pokud $a = \pm b \Rightarrow$ FAIL
Jinak $\Rightarrow \gcd(a-b, n)$ je faktor n

b je s pstí aspoň 3/4 jiná odmocnina než a
-- s pstí 1/2 to není ani $-a$
⇒ liší se o násobek p nebo q