Test prvočíselnosti:

- Malá Fermatova věta: Pro p prvočíslo a číslo $a < p$, vzájemně nesoudělná, $a^{(p-1)} \equiv 1 \pmod p$

→ Pokud pro nějaké a není splněn závěr, určitě to není prvočíslo. (a je svědek složenosti p)

→ Obrácení to ale neplatí vždy. Pro $a=2$ je nejmenší falešně pozitivní 341.

Problém:

- nevíme, kolik existuje falešných
- pro některá složená čísla n (Carmichaelova č.) platí $a^{(n-1)} \equiv 1 \pmod n$ pro $\forall a < n$ nesoudělná s n.

Tvrzení: Test složenosti čísla $\in NP$ (svědek: rozklad)

Test prvočíselnosti $\in NP$ (Nebudeme potřebovat, „jiný" ověř. alg.)

Od roku 2002 test prvočíselnosti $\in P$ (test složenosti $\in P$),

ale rozklad $\in NP$. (Využívá se proto v RSA)

Označme T jako množinu všech dvojic (k, n) : $k < n$ a platí jedna z podmínek:

1) $k^{n-1} \not\equiv 1 \pmod n$ → n porušuje malou Fermatovu

2) $\exists i$: $m = \frac{n-1}{2^i}$ je celé číslo a $1 < \gcd(k^{m}-1, n) < n$

- analyzujeme opakované druhé odmocniny z k^{n-1} pro zvyšující se i

dokud $k^m \equiv 1 \bmod n$, pokud $x^2 \equiv 1 \bmod n$, tak $x^2 - 1 \equiv (x+1)\cdot(x-1) \equiv 0 \bmod n$,

pro n prvočíslo nutně $x \equiv \pm 1 \bmod n$, pro n složené můžeme dostat

netriviální dělitele n (a k je svědek složenosti)

Tvrzení 1: Číslo n je složené právě tehdy, pokud $\exists k < n$ t.ž. $(k, n) \in T$.

Tvrzení 2: Nechť n složené. Pak existuje alespoň $\frac{n-1}{2}$ čísel $k < n$ t.ž. $(k, n) \in T$

Alg: Rabin-Millerův test.
Vstup: n testované číslo, $m \in N$ lib.

```
begin
  for i := 1 to m do
    k[i]  := Random(1,n-1);
    if T(k[i],n) then "n je složené"; konec fi
  od
  "n je prvočíslo"
end.
```

→ Uniform random dist.

↑ Algoritmus umí být jen falešně pozitivní. To je důležité. Nikdy není falešně negativní.

→ Hledá složená, protože pak to nemůže být prvočíslo

Pokud alg. rozhodne, že n je prvočíslo, pak se může jednat o chybu. V případě chyby všechny vybrané k_i byly "ne-svědci" pro n, a to se může stát podle T.2 s pravděpodobností $P(chyba) \leq (1/2)^m$, pro nezávislé výběry čísel k_i.

Složitost alg.: Polynomiální k $\log n$, tj. počtu bitů n. (Důkaz složitosti testu $(k, n) \in T$ je netriviální a využívá znalosti z teorie čísel.)

-> mohu si tedy pro zadání zvolit takový rozsah cyklu, abych splnil podmínku.

-> Lze škálovat výslednou chybu počtem iterací

-> Testy lze provádět paralelně.

Kryptografie:

$e()$ - encryption $\qquad e(): \{0\_M\} \to \{0\_N\}$

$d()$ - decryption $\qquad d: \{0\_N\} \to \{0\_M\}$

$d()$ je zleva inverzní k $e()$: $\forall m \; d(e(m)) = m$

Asymetrická šifra:

- Alice + Bob, each public + secret key P_X, S_X
- šifrujeme binárně --> většinou se použí blokové šifrování

$P_X(), S_X()$ jsou efektivně vyčíslitelné.

Platí: $\forall M \in D: P_X(S_X(M)) = M \wedge S_X(P_X(M)) = M$ tj funkce jsou vzájemně inverzní pro lib. M.

Bezpečnost: $S_X()$ nelze odvodit i s $P_X()$. Ve skutečnosti jsou funkce P_X, S_X známé.

Rozšířený Euklidův alg:

$a, b \geq 0$

$d = NSD(a,b) = $ nejmenší kladné $x \in \{ax+by \mid x,y \in \mathbb{Z}\}: d = ax+by$

Rozšířený navíc vrací i koeficienty x, y

```
RozšířenýEuklid(a,b)
  if b=0
    then return (a,1,0)
  (d',x',y') := RozšířenýEuklid(b, a mod b)
  (d, x, y ) := (d', y', x' - (a div b)*y')
  return (d,x,y)
```

Správnost:
Pro výsledek rekurze platí: $d' = bx' + (a \bmod b)y'$
Dále platí: $d = \mathrm{nsd}(a, b) = d'$
Chceme x a y, tž. $d = ax + by$ (1).

Úpravou dostaneme:
$d = d' = bx' + (a \bmod b)y'$
$= bx' + (a - \lfloor a/b \rfloor \cdot b)y'$
$= ay' + b(x' - \lfloor a/b \rfloor y')$

Proto volba $x = y'$ a $y = x' - \lfloor a/b \rfloor y'$ zaručuje splnění (1).
Použití: pro počítání inverzních prvků v Z_n

Tvrzení: Pro n-bitová čísla potřebuje RozšířenýEuklid $O(n^3)$ bitových operací.
Idea dk.: Nejmenší čísla (tj. nejhorší případ) při daném počtu kroků jsou Fibonacciho čísla.

Df: Eulerova funkce $\phi(n)$ je pro $n > 1$ # kladných čísel menších než n, nesoudělných s n.

Věta: Pokud je n prvočíslo, pak $\phi(n) = n-1$. Pokud $n = p \cdot q$, kde p, q jsou různá prvočísla, pak $\phi(n) = \phi(p) \cdot \phi(q) = (p-1)\cdot(q-1)$.

Věta: (Eulerova) Pro a, n nesoudělná, tj. $nsd(a,n) = 1$, platí: $a^{\phi(n)} \equiv 1 \pmod{n}$

↳ **Důsl:** Pokud $nsd(a,n) = 1$, potom multiplikativní inverzní prvek $\langle a \rangle_n^{-1} = \langle a^{\phi(n)-1} \rangle_n$

$\langle a \rangle_n := a \bmod n$

Malá Fermatova: Je-li p prvočíslo, pak pro $a < p$ vzájemně nesoudělná: $a^{p-1} \equiv 1 \pmod{n}$.

Eulerova věta: pro prvočíslo p je $\phi(p) = p-1$.

Princip RSA:

RSA šifra (Rivest, Shamir, Adelman)

1. Vyber dvě velká prvočísla p a q (každé má stovky bitů)
2. Spočítej $n = pq$. Spočítej $r = \phi(n) = (p-1)(q-1)$
3. Vyber malé liché číslo e, nesoudělné s r, tj. s $(p-1)(q-1)$.
4. Spočítej multiplikativní inverzní prvek d k e modulo r. !
5. Zveřejni (e, n) jako veřejný RSA klíč a uschovej (d, n) jako soukromý RSA klíč.

šifrování

dešifr. Věta (korektnost RSA): Funkce $P(M) = M^e \pmod{n}$ a $S(M) = M^d \pmod{n}$ definují dvojici inverzních transformací na $Z_n = \{0, 1, \ldots, n-1\}$.

Důkaz: Pro všechny $M \in Z_n$ platí: $P(S(M)) = S(P(M)) = M^{ed} \pmod{n}$.

Protože e a d jsou inverzní prvky modulo r, můžeme upravovat (pro vhodné c)

$M^{ed} \pmod{n} \equiv M^{1+cr} \pmod{n}$

$\equiv M \cdot M^{c \cdot \phi(n)} \pmod{n}$

$\equiv M \cdot 1 \pmod{n}$

$\equiv M \pmod{n}$. Q.E.D

Příklad (ověřeno):

Volíme $p = 47$, $q = 71$.

Spočítáme $n = 3337$, $r = (p-1)(q-1) = 3220$.

Volíme $e = 79$, spočítáme $d = \langle 79 \rangle_{3220}^{-1} = 1019$.

Klíč P je $(79, 3337)$.

Bob posílá $M = 688$.

$P(M) = \langle M^e \rangle_n = \langle 688^{79} \rangle_{3337} = 1570 = C$

My dešifrujeme:

$S(C) = \langle C^d \rangle_n = \langle 1570^{1019} \rangle_{3337} = 688 = M$

Proč je RSA bezpečná?
Na základě (e, n) není (zatím) nikdo schopen rychle spočítat d, aniž by znal rozklad $n = p \cdot q$ a teda $\phi(n) = (p-1)(q-1)$. Faktorizace velkých čísel je výpočetně těžký problém.

Pozn.: Jsou i jiné (vhodné) těžké problémy, např. diskrétní logaritmus (v Z_n), na kterých jsou založené kryptografické algoritmy.

Je to asymetrická šifra (která není rychlostně) optimální, takže se většinou používá na zahájení komunikace.

Konvexní obal v množině:

Df. Množina bodů $A \in R^n$ je *konvexní* iff (právě když) pro $\forall a, b \in A$ a $\forall t, 0 \le t \le 1$, platí $ta + (1-t)b \in A$.

Konvexní obal množiny A je průnik všech konvexních množin v R^n, které obsahují A. (!Nekonstruktivní def.)

Pozn. Konvexní obal je dobře definovaný, protože průnik lib. systému konvexních množin je konvexní a celý prostor R^n je konvexní.