



Nesymetrická kryptografia

Stanislav Palúch

Fakula riadenia a informatiky, Žilinská univerzita

30. novembra 2010

$\mathbb{N} = \{1, 2, 3, \dots\}$ – množina prirodzených čísel

$\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, \dots\}$ – množina celých čísel

Hovoríme, že celé číslo a delí celé číslo b a píšeme $a|b$, ak existuje celé číslo k také, že $b = k.a$.

Poznámka:

Platí $\forall a \in \mathbb{Z} \quad 0 = 0.a$. Preto každé celé číslo a delí nulu, t. j. $a|0$.
0 nedelí žiadne nenulové číslo.

Relácia $|\cdot|$ je tranzitívna – ak $a|b$ a $b|c$ potom $a|c$.

$b = k_1.a, c = k_2.b \Rightarrow$ potom $c = k_2.b = k_2(k_1.a) = (k_1.k_2).a$

Nech $m \in \mathbb{Z}$. Triviálne delitele čísla m sú čísla $1, -1, m, -m$.

Číslo $m \in \mathbb{Z}$ nazveme prvočíslom, ak má len triviálne delitele. Inak je m zložené číslo.

Každé prirodzené číslo $m > 1$ sa dá jednoznačne napísať v tvare

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k},$$

kde p_1, p_2, \dots, p_k sú navzájom rôzne prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k$ sú prirodzené čísla.

Zisťovanie prvočíselnosti:

Eratostenovo sito

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24



Iný spôsob zisťovania prvočíselnosti čísla n je založený na skutočnosti, že ak $n = p \cdot q$, kde $p > 1$, $q > 1$ a $p \leq q$, potom $p \leq \sqrt{n}$.

Na zistenie takého p možno použiť niektorý z postupov:

Postupne vydeľ číslo n číslami $2, 3, \dots, [\sqrt{n}]$.

Alebo:

Vydeľ číslo n číslami $2, 3$ a potom postupne všetkými číslami tvaru $6k - 1$, $6k + 1$ menšími než \sqrt{n} .

Alebo:

Vydeľ číslo n postupne všetkými prvočíslami menšími než \sqrt{n} .



Najväčší spoločný deliteľ

Hovoríme, že prirodzené číslo $d \in \mathbb{N}$ je najväčším spoločným deliteľom celých čísel $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ a píšeme $d = NSD(a, b)$, ak platí

- 1 $d|a$ a tiež $d|b$.
- 2 Ak $d_1 \neq d$ a $d_1|a$, $d_1|b$, potom aj $d_1|d$.

Euklidov algoritmus pre výpočet $NSD(a, b)$ $r_0 = a, r_1 = b$

$$r_0 = r_1 \cdot q_1 + r_2, \quad r_2 < r_1$$

$$r_1 = r_2 \cdot q_2 + r_3, \quad r_3 < r_2$$

...

$$r_{i-1} = r_i \cdot q_i + r_{i+1}, \quad r_{i+1} < r_i$$

...

$$r_{m-1} = r_m \cdot q_m + 0$$

$$r_m = NSD(r_0, r_1) = NSD(a, b)$$



Kongruencie

Hovoríme, že a je kongruenté s b modulo n a píšeme $a \equiv b \pmod{n}$, ak $n \mid (a - b)$, t.j. ak rozdiel $(a - b)$ je deliteľný číslom n .

Platí: Relácia \equiv je reláciou ekvivalencie na množine \mathbb{Z} (resp \mathbb{N}) – relácia \equiv je reflexívna, symetrická a tranzitívna.

- 1 $a \equiv a \pmod{n} \forall a \in \mathbb{Z}$
- 2 Ak $a \equiv b \pmod{n}$ potom aj $b \equiv a \pmod{n}$
- 3 Ak $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, potom $a \equiv c \pmod{n}$

$a \equiv b \pmod{n}$ platí práve vtedy, keď obe čísla a , b dávajú po delení číslom n ten istý zvyšok.

Ak $a \equiv b \pmod{n}$, potom $a * c \equiv b * c \pmod{n}$ pre ľubovoľné celé číslo c .

Ak $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, potom $a + c \equiv b + d \pmod{n}$.

Ak $a * c \equiv b * c \pmod{n}$ a $NSD(c, n) = 1$, potom $a \equiv b \pmod{n}$.



Rozšířený Euklidov algoritmus

$$r_0 = r_1 \cdot q_1 + r_2 \quad t_2 = (-q_1) \bmod r_0$$

$$r_1 = r_2 \cdot q_2 + r_3 \quad t_3 = (1 - q_2 \cdot t_2) \bmod r_0$$

$$r_2 = r_3 \cdot q_3 + r_4 \quad t_4 = (t_2 - q_3 \cdot t_3) \bmod r_0$$

...

$$r_{i-1} = r_i \cdot q_i + r_{i+1} \quad t_{i+1} = (t_{i-1} - q_i \cdot t_i) \bmod r_0$$

$$r_i = r_{i+1} \cdot q_{i+1} + r_{i+2}$$

...

$$r_{m-3} = r_{m-2} \cdot q_{m-2} + r_{m-1} \quad t_{m-1} = (t_{m-3} - q_{m-2} \cdot t_{m-2}) \bmod r_0$$

$$r_{m-2} = r_{m-1} \cdot q_{m-1} + r_m \quad t_m = (t_{m-2} - q_{m-1} \cdot t_{m-1}) \bmod r_0$$

$$r_{m-1} = r_m \cdot q_m + 0 \quad t_{m+1} = (t_{m-1} - q_m \cdot t_m) \bmod r_0$$

Rozšířený Euklidov algoritmus

Tvrdenie: $t_m r_1 \equiv r_m \pmod{r_0}$.

Dokážeme indukciou pre $i = 2, 3, \dots, m$ $t_i r_1 \equiv r_i \pmod{r_0}$.

Pre $i = 2$:

Keďže $r_0 = r_1 \cdot q_1 + r_2$ je $r_2 = r_0 - r_1 \cdot q_1$.

Ďalej je $t_2 = (-q_1) \pmod{r_0}$ čo je ekvivalentné s $q_1 + t_2 \equiv 0 \pmod{r_0}$.

$$r_2 - t_2 r_1 \equiv r_0 - r_1 q_1 - t_2 r_1 \equiv r_0 - r_1 \underbrace{(q_1 + t_2)}_{\equiv 0 \pmod{r_0}} \equiv 0 \pmod{r_0}$$

Pre $i = 3$:

$$r_3 - t_3 r_1 \equiv r_1 - r_2 q_2 - t_3 r_1 \equiv r_1 - r_2 q_2 - (1 - q_2 t_2) r_1 \equiv q_2 t_2 r_1 - r_2 q_2 = \underbrace{q_2 (t_2 r_1 - r_2)}_{\equiv 0 \pmod{r_0}} \equiv 0 \pmod{r_0}$$

Predpokladajme že: $t_i r_1 \equiv r_i \pmod{r_0}$, $t_{i-1} r_1 \equiv r_{i-1} \pmod{r_0}$.

Použijeme rekurzívne vzťahy $r_{i+1} = r_{i-1} - r_i q_i$, $t_{i+1} = t_{i-1} - q_i \cdot t_i$

$$r_{i+1} - t_{i+1} r_1 \equiv r_{i-1} - r_i q_i - (t_{i-1} - q_i \cdot t_i) r_1 \equiv r_{i-1} - r_i q_i - t_{i-1} r_1 + q_i \cdot t_i r_1 \equiv \underbrace{r_{i-1} - t_{i-1} r_1}_{\equiv 0 \pmod{r_0}} + q_i \underbrace{(t_i r_1 - r_i)}_{\equiv 0 \pmod{r_0}} \equiv 0 \pmod{r_0}$$

Rozšířený Euklidov – algoritmus program v C

```
#include <stdio.h>
#include <string.h>
int main()
{int a,b,i,nsd,inv,q[100],r[100],t[100];
 printf("Zadaj a: \n");
 scanf("%d", &a);
 printf("Zadaj b:\n ");
 scanf("%d", &b);
 for(i=0;i<100;i++) r[i]=0,q[i]=0,t[i]=0;
 i=0; r[0]=a, r[1]=b, t[0]=0, t[1]=1;

 while (r[i+1]!=0)
   {q[i+1]=r[i]/r[i+1];
    r[i+2]=r[i]%r[i+1];
    t[i+2]=(t[i]-q[i+1]*t[i+1])%a;
    if(t[i+2]<0)t[i+2]=t[i+2]+a;
    i++;}

 nsd=r[i], inv=t[i];
 printf("nsd(%d,%d) = %d \n", a, b, nsd);
 printf("(%d)^ -1 mod %d = %d \n", b, a, inv);
 return 0;
}
```



Eulerova funkcia $\phi(n)$

Definícia. Nech $n \in \mathbb{N}$. Eulerova funkcia $\phi(n)$ je počet prirodzených čísel menších alebo rovných než n nesúdeliteľných s n .

n	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	...

Ak p je prvočíslo, potom všetky čísla $1, 2, \dots, p - 1$ sú neúdeliteľné s p .

Ak p je prvočíslo, potom všetky súdeliteľné čísla s p menšie alebo rovné než p sú $1p, 2p, 3p, \dots, p^{n-1} \cdot p$ – je ich presne p^{n-1} .

Tvrdenie. Nech $p \in \mathbb{N}$ je prvočíslo, $n \in \mathbb{N}$, $n \geq 1$. Potom platí:

$$\begin{aligned}\phi(p) &= p - 1 \\ \phi(p^n) &= p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)\end{aligned}$$



Vlastnosti Eulerovej funkcie

Tvrdenie. Nech $a, b \in \mathbb{N}$, a, b nesúdeliteľné. Potom

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Dôsledok.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \dots \cdot \phi(p_k^{\alpha_k}) =$$

Vlastnosti Eulerovej funkcie

Tvrdenie. Nech $a, b \in \mathbb{N}$, a, b nesúdeliteľné. Potom

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Dôsledok.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \dots \cdot \phi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$$

Vlastnosti Eulerovej funkcie

Tvrdenie. Nech $a, b \in \mathbb{N}$, a, b nesúdeliteľné. Potom

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Dôsledok.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \dots \cdot \phi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$$

$$p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) =$$

Vlastnosti Eulerovej funkcie

Tvrdenie. Nech $a, b \in \mathbb{N}$, a, b nesúdeliteľné. Potom

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Dôsledok.

$$\begin{aligned}\phi(n) &= \phi(\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \dots \cdot \phi(p_k^{\alpha_k}) = \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = \\ &= \underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n} \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right) =\end{aligned}$$

Vlastnosti Eulerovej funkcie

Tvrdenie. Nech $a, b \in \mathbb{N}$, a, b nesúdeliteľné. Potom

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Dôsledok.

$$\phi(n) = \phi(\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \dots \cdot \phi(p_k^{\alpha_k}) =$$


$$(p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$$

$$p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) =$$

$$\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_{=n} \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right) =$$

$$n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

Špeciálne: Pre $p, q \in \mathbb{N}$ obe prvočísla je $\phi(p \cdot q) = (p - 1) \cdot (q - 1)$.



Umocňovanie $(a + b)^p \equiv a^p + b^p \pmod p$

Binomická veta:

$$(a + b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} b^1 + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{i} a^{p-i} b^i + \dots + \binom{p}{p-1} a^1 b^{p-1}}_{\text{ak je } p \text{ prvočíslo, tento súčet je deliteľný } p} + b^p$$

Ak je p prvočíslo, $1 \leq i < p$, potom

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1.2.\dots.i} = p \cdot \underbrace{\left[\frac{(p-1)\dots(p-i+1)}{1.2.\dots.i} \right]}_{\text{toto je celé číslo, lebo } p \text{ sa nemá s čím skrátiť}} = p \cdot k$$

Dôsledok. Ak je p prvočíslo,

$$(a + b)^p \equiv a^p + b^p \pmod p.$$



Malá Fermatova veta

Nech p je prvočíslo.

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}$$



Malá Fermatova veta

Nech p je prvočíslo.

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}$$

$$3^p = (2 + 1)^p \equiv 2^p + 1^p \equiv 3 \pmod{p}$$



Malá Fermatova veta

Nech p je prvočíslo.

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}$$

$$3^p = (2 + 1)^p \equiv 2^p + 1^p \equiv 3 \pmod{p}$$

$$4^p = (3 + 1)^p \equiv 3^p + 1^p \equiv 4 \pmod{p}$$



Malá Fermatova veta

Nech p je prvočíslo.

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}$$

$$3^p = (2 + 1)^p \equiv 2^p + 1^p \equiv 3 \pmod{p}$$

$$4^p = (3 + 1)^p \equiv 3^p + 1^p \equiv 4 \pmod{p}$$

...

$$c^p = ((c - 1) + 1)^p \equiv (c - 1)^p + 1^p \equiv (c - 1) + 1 \equiv c \pmod{p}$$



Malá Fermatova veta

Nech p je prvočíslo.

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}$$

$$3^p = (2 + 1)^p \equiv 2^p + 1^p \equiv 3 \pmod{p}$$

$$4^p = (3 + 1)^p \equiv 3^p + 1^p \equiv 4 \pmod{p}$$

...

$$c^p = ((c - 1) + 1)^p \equiv (c - 1)^p + 1^p \equiv (c - 1) + 1 \equiv c \pmod{p}$$

Malá Fermatova veta. Nech p je prvočíslo, nech c je ľubovoľné prirodzené číslo. Potom

$$c^p \equiv c \pmod{p}.$$



Malá Fermatova veta

Nech p je prvočíslo.

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}$$

$$3^p = (2 + 1)^p \equiv 2^p + 1^p \equiv 3 \pmod{p}$$

$$4^p = (3 + 1)^p \equiv 3^p + 1^p \equiv 4 \pmod{p}$$

...

$$c^p = ((c - 1) + 1)^p \equiv (c - 1)^p + 1^p \equiv (c - 1) + 1 \equiv c \pmod{p}$$

Malá Fermatova veta. Nech p je prvočíslo, nech c je ľubovoľné prirodzené číslo. Potom

$$c^p \equiv c \pmod{p}.$$

Ak navyše $c \in \{1, 2, \dots, p - 1\}$, potom

$$c^{p-1} \equiv 1 \pmod{p}.$$



Eulerova veta – zovšeobecnenie malej Fermatovej vety

Nech a_1, a_2, \dots, a_k sú všetky navzájom rôzne nesúdeliteľné čísla s číslom m menšie než m , kde m je ľubovoľné číslo, $k = \phi(m)$.

Vezmime x nesúdeliteľné s m a skúmame množinu čísel $\{a_1x, a_2x, \dots, a_kx\}$. Sú to zase všetko čísla nesúdeliteľné s m .

Pre každú dvojicu i, j , $i \neq j$ platí $a_ix \not\equiv a_jx \pmod{m}$

– inak by muselo byť $a_i \equiv a_j \pmod{m}$ (a keďže $1 \leq a_i, a_j \leq m-1$) aj $a_i = a_j$.

Pre každé a_ix existuje práve jedno $a_{\pi[x]}$ také, že $a_ix \equiv a_{\pi[x]} \pmod{m}$. Preto je

$$x^{\phi(m)} \cdot \prod_{i=1}^{\phi(m)} a_i \equiv \prod_{i=1}^{\phi(m)} (a_ix) \equiv \prod_{i=1}^{\phi(m)} a_{\pi[i]} \equiv \prod_{i=1}^{\phi(m)} a_i \pmod{m}$$

Keďže súčin $\prod_{i=1}^{\phi(m)} a_i$ je nesúdeliteľný s m , obe strany poslednej kongruencie možno týmto súčinom vydeliť, čím dostávame nasledujúcu vetu:

Eulerova veta. Pre ľubovoľné číslo x nesúdeliteľné s číslom m platí

$$x^{\phi(m)} \equiv 1 \pmod{m}.$$



Okruhy a polia typu \mathbb{Z}_p

$\mathbb{Z}_p = (\{0, 1, 2, \dots, p-1\}, \oplus, \otimes)$, kde

$$a \oplus b = a + b \pmod{p}$$

$$a \otimes b = a \cdot b \pmod{p}$$

Štruktúra \mathbb{Z}_p je pole práve vtedy, keď p je prvočíslo.

Platí tam:

1. $a \oplus b = b \oplus a$
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. $a \oplus 0 = 0 \oplus a = a$
4. $\forall a \exists b (a \oplus b = b \oplus a = 0)$
5. $a \otimes b = b \otimes a$
6. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
7. $a \otimes 1 = 1 \otimes a = a$
8. $\forall (a \neq 0) \exists b (a \otimes b = b \otimes a = 0)$
9. $a \otimes 0 = 0 \otimes a = 0$
10. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Nech p je prvočíslo.

Riešime rovnicu $a \otimes x = 1$, t.j. hľadáme také x , že $ax \equiv 1 \pmod{p}$.

Vieme že platí

$$\begin{aligned}a^{\phi(p)} &\equiv 1 \pmod{p} \\ a \cdot a^{\phi(p)-1} &\equiv 1 \pmod{p} \\ x &\equiv a^{\phi(p)-1} \pmod{p} \\ a^{-1} &\equiv a^{\phi(p)-1} \pmod{p}\end{aligned}$$

Keďže p je prvočíslo, $\phi(p) = p - 1$, v \mathbb{Z}_p je $x = a^{-1} = a^{p-2}$.

Rovnica $a \otimes x = b$ má v \mathbb{Z}_p riešenie $x = a^{-1} \otimes b = a^{p-2} \otimes b$.

Zisťovanie prvočíselnosti veľkých čísel

Nech M je veľké číslo. Ak je M prvočíslo, podľa Fermatovej vety platí pre každé prirodzené c , $c < M$

$$c^{M-1} \equiv 1 \pmod{M}.$$

Ak sa teda nájde také prirodzené číslo $c < M$, že

$$c^{M-1} \not\equiv 1 \pmod{M},$$

potom je M zložené číslo.

Fermatov test prvočíselnosti.

1. Ak pre niektoré $c < M$ je $c^{M-1} \not\equiv 1 \pmod{M}$, potom je c určite zložené číslo.
2. Ak pre dostatočne veľa čísel $c < M$ platí $c^{M-1} \equiv 1 \pmod{M}$, potom c je pravdepodobne prvočíslo.

Phill Zimmermann v PGP použil túto procedúru na zisťovanie prvočíselnosti M :

- Vylúčil M ak neprešlo testom vydelením všetkými 16-bitovými prvočíslami
- Aplikoval Fermatov test pre štyri hodnoty c .



Carmichaelove čísla

Carmichaelove číslo – také zložené číslo M , že pre všetky $c < M$, c nesúdeliteľné s M platí $c^{M-1} \equiv 1 \pmod{M}$.

561 = 3 · 11 · 17	Vlastnosti Carmichaelovho čísla M :
1105 = 5 · 13 · 17	• M je zložené z aspoň troch prvočísel
1729 = 7 · 13 · 19	• Žiadne prvočíslo sa v rozklade M neopakuje
2465 = 5 · 17 · 29	• Carmichaelove čísla sú zriedkavé – medzi 1 a 10^{21} je
2821 = 7 · 13 · 31	ich najviac 20,138,200. Pravdepodobnosť, že číslo
6601 = 7 · 23 · 41	z intervalu $\langle 1, 10^{21} \rangle$ je Carmichaelovo je
8911 = 7 · 19 · 67	$\frac{10^{21}}{2 \cdot 10^7} = 5 \cdot \frac{1}{10^{13}}$

$$9746347772161 = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641$$

$C(N)$ počet Carmichaelových čísel medzi 1 a N

$$N^{0.332} < C(N) < N \cdot \exp\left(-\frac{\ln N \ln \ln \ln N}{\ln \ln N}\right)$$

1. Vyjadri p v tvare $p = 1 + 2^s \cdot r$, r nepárne
2. For $i = 1$ to t urob
 - 2.1 Vyber náhodné číslo a také, že $2 \leq a \leq p - 2$
 - 2.2 Polož $y = a^r \pmod{p}$
 - 2.3 Ak $y \neq 1$ and $y \neq p - 1$ urob:

$$\left[\begin{array}{l} j=1 \\ \text{WHILE } (j \leq s - 1) \text{ and } (y \neq p - 1) \\ \quad \left\{ \begin{array}{l} y = y^2 \pmod{p} \\ \text{Ak } y = 1, \text{ RETURN ZLOŽENÉ} \\ j = j + 1 \end{array} \right. \\ \text{Ak } y \neq p - 1 \text{ RETURN ZLOŽENÉ} \end{array} \right.$$

3. RETURN PRVOČÍSLO S PRAVDEPODOBNOŠŤOU $1 - \left(\frac{1}{4}\right)^t$

Nevýhody symetrickej kryptografie:

- Každá dvojica účastníkov musí udržiavať svoj kľúč.
- Kľúčov je teda veľmi veľa a všetky sa musia udržať v tajnosti.

Princíp kryptografie s verejným kľúčom:

- Každý účastník A má jednu dvojicu kľúčov – Verejný kľúč $KV(A)$ a tajný kľúč $KT(A)$.
Kľúč $KV(A)$ zverejní, kľúč $KT(A)$ utají.
- Účastník A šifruje správu x účastníkovi B tak, že nájde verejný kľúč $KV(B)$ a pošle správu $y = E_{KV(B)}(x)$.
- Účastník B dešifruje správu y predpisom $x = D_{KT(B)}(y)$.

1. Účastník A zvolí dve veľké tajné prvočísla p, q .
2. $n = p \cdot q$
3. $\phi(n) = (p - 1)(q - 1)$
4. Ďalej zvolí dve čísla $0 < e < \phi(n)$, $0 < d < \phi(n)$ také, že

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

5. Verejný kľúč účastníka A je dvojica (e, n) , jeho tajný kľúč je dvojica (d, n)
6. Účastník B bude správu $x < n$ pre účastníka A šifrovať predpisom

$$y = x^e \pmod{n}.$$

7. Účastník A dešifruje správu y predpisom

$$x = y^d \pmod{n}.$$

Problém voľby prvočísel p, q .

- Dostatočná veľkosť – aspoň 512 – 1024 bitov.
- Zisťovanie prvočíselnosti – použiť niektorý pravdepodobnostný test.
- Je ich dosť? Počet prvočísel menších než $n \approx \frac{n}{\ln n}$.

Niekedy sa požaduje, aby p, q boli silné prvočísla (strong prime).

Prvočíslo p je silné prvočíslo, ak

1. p je veľké
2. $p - 1$ má veľký prvočíselný faktor, t.j. $p - 1 = a_1 p_1 + 1$ pre niektoré veľké prvočíslo p_1
3. $p_1 - 1$ má veľký prvočíselný faktor, t.j. $p_1 - 1 = a_2 p_2 + 1$ pre niektoré veľké prvočíslo p_2
4. $p + 1$ má veľký prvočíselný faktor, t.j. $p + 1 = a_3 p_3 + 1$ pre niektoré veľké prvočíslo p_3

Voľba silných prvočísel bola motivovaná sťažiením niektorých metód faktorizácie. Objavenie ďalších faktorizačných metód ukázalo, že pre ne silné prvočísla nepredstavujú problém.

Bruce Schneier ani Philip Zimmerman neodporúčajú silné prvočísla.

Problém voľby čísel e , d .

- Veľmi často sa volí $e = 65537 = 2^{16} + 1$. e je prvočíslo.
- Číslo d také, že $e \cdot d \equiv 1 \pmod{\phi(n)}$ sa nájde rozšíreným Euklidovým algoritmom.

Umocňovanie $x^d \pmod n$ pre veľké d .

Bitová reprezentácia čísla d nech je $d[k-1] \dots d[1]d[0]$.

```
temp=x;
y=1;
for(i=0; i<k; i++)
{if(d[i]==1) y=mod(y*temp,n);
  temp=mod(temp*temp,n);
}
return y;
```




RSA algoritmus – prečo to funguje 1.

Nech $x < n$, $y = E(x) = x^e \pmod n$.

Platí skutočne, že $D(y) = y^d \pmod n = x$?

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{k\phi(n)+1} \pmod n$$

Čísla e , d boli vybrané tak aby $e \cdot d \equiv 1 \pmod{\phi(n)}$, t.j. aby $e \cdot d = k \cdot \phi(n) + 1$ pre nejaké prirodzené číslo k .

1. Ak x je nesúdeliteľné s n potom

$$x^{\phi(n)} \equiv 1 \pmod n$$

$$(x^{\phi(n)})^k \equiv 1^k \pmod n$$

$$x^{k \cdot \phi(n)} \equiv 1 \pmod n$$

$$x \cdot x^{k \cdot \phi(n)} \equiv x \pmod n$$

$$y^d \equiv x^{e \cdot d} \equiv x^{k \cdot \phi(n)+1} \equiv x \pmod n$$



RSA algoritmus – prečo to funguje 2.

2. Ak x a n sú súdeliteľné potom musí byť $p|x$ alebo $q|x$.

Nech $p|x$ potom $q \nmid x$. (Inak by muselo byť $x = k \cdot pq \geq n$.)

Eulerova veta ($x^{\phi(q)} \equiv 1 \pmod{q}$) platí aj pre $x^{\phi(p)}$.

$$\begin{aligned}(x^{\phi(p)})^{\phi(q)} &\equiv 1 \pmod{q} \\ (x^{\phi(p)})^{k \cdot \phi(q)} &\equiv 1 \pmod{q} \\ x^{k \cdot \phi(p) \cdot \phi(q)} &\equiv 1 \pmod{q} \\ x \cdot x^{k \cdot \phi(n)} &\equiv x \pmod{q}\end{aligned}$$

Máme teda

$$x^{k \cdot \phi(n) + 1} - x = L \cdot q.$$

Keďže $p|x$, musí byť aj $p|L$, t.j. $L = M \cdot p$. Preto je

$$x^{k \cdot \phi(n) + 1} - x = L \cdot q = M \cdot p \cdot q = M \cdot n$$

$$x^{k \cdot \phi(n) + 1} \equiv x \pmod{n}.$$

Nech dvaja účastníci majú kľúče so spoločným modulom n . Obidvom pošleme tú istú správu m , ktorú zašifrujeme na šifrované texty c_1, c_2 .

$$c_1 \equiv m^{e_1} \pmod{n}$$

$$c_2 \equiv m^{e_2} \pmod{n}$$

Ak sú, e_1, e_2 nesúdeliteľné nájdeme r také, že $r \cdot e_1 \equiv 1 \pmod{e_2}$.
Potom platí

$$\begin{aligned} r \cdot e_1 - 1 &= s \cdot e_2 \quad \text{pre niektoré } s \geq 1 \\ r \cdot e_1 - s \cdot e_2 &= 1 \end{aligned}$$

Vypočítajme c_3 také že $c_2 \cdot c_3 \equiv 1 \pmod{n}$, t.j. $c_3 = c_2^{-1}$.
Potom

$$c_1^r \cdot c_3^s \equiv c_1^r \cdot (c_2^{-1})^s \equiv m^{re_1} \cdot m^{-se_2} \equiv m^{re_1 - se_2} \equiv m^1 \equiv m \pmod{n}.$$

Poučenie: Nešifrovať viackrát tú istú správu.
Nepoužívať spoločný modulus n .