Nesymetrická kryptografia

Stanislav Palúch

Fakulta riadenia a informatiky, Žilinská univerzita

30. novembra 2010

Základy teórie čísel

$\mathbb{N} = \{1, 2, 3, \dots\}$ – 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 $\forall a \in \mathbb{Z} \;\; 0 = 0.a$. Preto každé celé číslo a delí nulu, t. j. $a|0$.
0 nedelí žiadne nenulové číslo.

Relácia .|. 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.

Základná veta aritmetiky

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

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

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

$\cancel{1}\ {\color{red}2}\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ 9\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ 15\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ 21\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ {\color{red}5}\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ {\color{red}5}\ \cancel{6}\ {\color{red}7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ {\color{red}5}\ \cancel{6}\ {\color{red}7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ {\color{red}11}\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ {\color{red}5}\ \cancel{6}\ {\color{red}7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ {\color{red}11}\ \cancel{12}\ {\color{red}13}\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ {\color{red}5}\ \cancel{6}\ {\color{red}7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ {\color{red}11}\ \cancel{12}\ {\color{red}13}\ \cancel{14}\ \cancel{15}\ \cancel{16}\ {\color{red}17}\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

$\cancel{1}\ {\color{red}2}\ {\color{red}3}\ \cancel{4}\ {\color{red}5}\ \cancel{6}\ {\color{red}7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ {\color{red}11}\ \cancel{12}\ {\color{red}13}\ \cancel{14}\ \cancel{15}\ \cancel{16}\ {\color{red}17}\ \cancel{18}\ {\color{red}19}\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}$

Zisťovanie prvočíselnosti

Iný spôsob zisťovania prvočíslenosti čísla n je založený na skutočnosti, že ak $n = p.q$, 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 $2, 3, \ldots, [\sqrt{n}]$.

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 $NSD(a, b)$ $\qquad r_0 = a,\ r_1 = b$

$$
\begin{array}{rcll}
r_0 & = & r_1.q_1 + r_2, & r_2 < r_1 \\
r_1 & = & r_2.q_2 + r_3, & r_3 < r_2 \\
 & \dots & & \\
r_{i-1} & = & r_i.q_i + r_{i+1}, & r_{i+1} < r_i \\
 & \dots & & \\
r_{m-1} & = & r_m.q_m + 0 &
\end{array}
$$

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

Kongruencie

Hovoríme, že a je kongruenté s b modulo n a píšeme $a \equiv b \mod n$, ak $n|(a-b)$, 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. $a \equiv a \mod n \ \forall a \in \mathbb{Z}$
2. Ak $a \equiv b \mod n$ potom aj $b \equiv a \mod n$
3. Ak $a \equiv b \mod n$, $b \equiv c \mod n$, potom $a \equiv c \mod n$

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

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

Ak $a \equiv b \mod n$, $c \equiv d \mod n$, potom $a + c \equiv b + d \mod n$.

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

Rozšírený Euklidov algoritmus

$$
\begin{aligned}
r_0 &= r_1.q_1 + r_2 & t_2 &= (-q_1) \mod r_0 \\
r_1 &= r_2.q_2 + r_3 & t_3 &= (1 - q_2.t_2) \mod r_0 \\
r_2 &= r_3.q_3 + r_4 & t_4 &= (t_2 - q_3.t_3) \mod r_0 \\
& \dots \\
r_{i-1} &= r_i.q_i + r_{i+1} & t_{i+1} &= (t_{i-1} - q_i.t_i) \mod r_0 \\
r_i &= r_{i+1}.q_{i+1} + r_{i+2} \\
& \dots \\
r_{m-3} &= r_{m-2}.q_{m-2} + r_{m-1} & t_{m-1} &= (t_{m-3} - q_{m-2}.t_{m-2}) \mod r_0 \\
r_{m-2} &= r_{m-1}.q_{m-1} + r_m & t_m &= (t_{m-2} - q_{m-1}.t_{m-1}) \mod r_0 \\
r_{m-1} &= r_m.q_m + 0 & t_{m+1} &= (t_{m-1} - q_m.t_m) \mod r_0
\end{aligned}
$$

Rozšírený Euklidov algoritmus

Tvrdenie: $t_m r_1 \equiv r_m \mod r_0$.
Dokážeme indukciou pre $i = 2, 3, \ldots, m$ $t_i r_1 \equiv r_i \mod r_0$.

Pre $i = 2$:
Keďže $r_0 = r_1.q_1 + r_2$ je $r_2 = r_0 - r_1.q_1$.
Ďalej je $t_2 = (-q_1) \mod r_0$ čo je ekvivalentné s $q_1 + t_2 \equiv 0 \mod r_0$.

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

Pre $i = 3$:

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

Predpokladajme že: $t_i r_1 \equiv r_i \mod r_0$, $t_{i-1} r_1 \equiv r_{i-1} \mod r_0$.
Použijeme rekurzívne vzťahy $r_{i+1} = r_{i-1} - r_i q_i$, $t_{i+1} = t_{i-1} - q_i.t_i$

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

Rozšírený 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 $1, 2, \ldots, p-1$ sú neúdeliteľné s p.

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

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

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

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

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

Dôsledok.

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

Vlastnosti Eulerovej funkcie

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

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

Dôsledok.

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

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

Vlastnosti Eulerovej funkcie

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

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

Dôsledok.

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

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

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

Vlastnosti Eulerovej funkcie

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

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

Dôsledok.

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

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

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

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

Vlastnosti Eulerovej funkcie

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

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

Dôsledok.

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

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

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

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

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

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

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

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

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

Dôsledok. Ak je p prvočíslo,

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

Malá Fermatova veta

Nech p je prvočíslo.

$$2^p \quad = \quad (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p$$

Malá Fermatova veta

Nech p je prvočíslo.

$$
\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p
\end{aligned}
$$

Malá Fermatova veta

Nech p je prvočíslo.

$$
\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\
4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p
\end{aligned}
$$

Malá Fermatova veta

Nech p je prvočíslo.

$$\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\
4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p \\
&\dots \\
c^p &= ((c-1)+1)^p \equiv (c-1)^p + 1^p \equiv (c-1)+1 \equiv c \mod p
\end{aligned}$$

Malá Fermatova veta

Nech p je prvočíslo.

$$
\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p\\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p\\
4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p\\
&\dots\\
c^p &= ((c-1)+1)^p \equiv (c-1)^p + 1^p \equiv (c-1)+1 \equiv c \mod p
\end{aligned}
$$

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

$$c^p \equiv c \mod p.$$

Malá Fermatova veta

Nech p je prvočíslo.

$$\begin{aligned}
2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \mod p \\
3^p &= (2+1)^p \equiv 2^p + 1^p \equiv 3 \mod p \\
4^p &= (3+1)^p \equiv 3^p + 1^p \equiv 4 \mod p \\
&\dots \\
c^p &= ((c-1)+1)^p \equiv (c-1)^p + 1^p \equiv (c-1)+1 \equiv c \mod p
\end{aligned}$$

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

$$c^p \equiv c \mod p.$$

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

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

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 skúmajme 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 $\quad a_ix \not\equiv a_jx \mod m$
– inak by muselo byt $a_i \equiv a_j \mod m \quad$ (a keďže $1 \le a_i,\ a_j \le m-1$) aj $a_i = a_j$.

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

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

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

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

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

Okruhy a polia typu $\mathbb{Z}_p$

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

$$\begin{aligned} a \oplus b &= a + b \mod p \\ a \otimes b &= a.b \mod p \end{aligned}$$

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. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Ďalšie vlastnosti poľa Z_p

Nech p je prvočíslo.
Riešime rovnicu $a \otimes x = 1$, t.j. hľadáme také x, že $ax \equiv 1 \mod p$.
Vieme že platí

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

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, $c < M$

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

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

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

potom je M zložené číslo.

Fermatov test prvočíselnosti.

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

$$
\begin{aligned}
561 &= 3 \cdot 11 \cdot 17 \\
1105 &= 5 \cdot 13 \cdot 17 \\
1729 &= 7 \cdot 13 \cdot 19 \\
2465 &= 5 \cdot 17 \cdot 29 \\
2821 &= 7 \cdot 13 \cdot 31 \\
6601 &= 7 \cdot 23 \cdot 41 \\
8911 &= 7 \cdot 19 \cdot 67
\end{aligned}
$$

Vlastnosti Carmichaelovho čísla M:

- M je zložené z aspoň troch prvočísel
- Žiadne prvočíslo sa v rozklade M neopakuje
- Carmichaelove čísla sú zriedkavé – medzi 1 a 10^{21} je ich najviac 20,138,200. Pravdepodobnosť, že číslo z intervalu $\langle 1, 10^{21} \rangle$ je Carmichaelovo je

$$\frac{10^{21}}{2.10^7} = 5.\frac{1}{10^{13}}$$

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

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

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

Pravdepodobnostný test prvočíselnosti - RABIN – MILLER

1. Vyjadri p v tvare $p = 1 + 2^s.r$, 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 $y = a^r \mod p$
   2.3 Ak $y \neq 1$ and $y \neq p - 1$ urob:

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

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

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 šfiruje 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 $x = D_{KT(B)}(y)$.

RSA algoritmus

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
$$e \cdot d \equiv 1 \mod \phi(n)$$
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
$$y = x^e \mod n.$$
7. Účastník A dešifruje správu y predpisom
$$x = y^d \mod n.$$

RSA algoritmus – voľba prvočísel p, q

Problém voľby prvočísel p, q.

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

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

Voľba silných prvočísel bola motivovaná sťažením 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 $e \cdot d \equiv 1 \mod \phi(n)$ sa nájde rozšíreným Euklidovým algoritmom.

Umocňovanie $x^d \mod n$ pre veľké d.

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

```
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 $x < n$, $y = E(x) = x^e \mod n$.
Platí skutočne, že $D(y) = y^d \mod n = x$?

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

Čísla e, d boli vyberané tak aby $e.d \equiv 1 \mod \phi(n)$, t.j. aby $e.d = k.\phi(n) + 1$ pre nejaké prirodzené číslo k.

1. Ak x je nesúdeliteľné s n potom

$$\begin{aligned}
x^{\phi}(n) &\equiv 1 \mod n \\
(x^{\phi(n)})^k &\equiv 1^k \mod n \\
x^{k.\phi(n)} &\equiv 1 \mod n \\
x \cdot x^{k.\phi(n)} &\equiv x \mod n \\
y^d \equiv x^{e.d} \equiv x^{k.\phi(n)+1} &\equiv x \mod n
\end{aligned}$$

RSA algoritmus – prečo to funguje 2.

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

Nech $p|x$ potom $q \not| x$. (Inak by muselo byť $x = k.pq \geq n$.)

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

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

Máme teda

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

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

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

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

Nebezpečenstvo spoločného n

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

$$\begin{aligned} c_1 &\equiv m^{e_1} \mod n \\ c_2 &\equiv m^{e_2} \mod n \end{aligned}$$

Ak sú e_1, e_2 nesúdeliteľné nájdeme r také, že $r \cdot e_1 \equiv 1 \mod e_2$. 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 $c_2.c_3 \equiv 1 \mod n$, t.j $c_3 = c_2^{-1}$. Potom

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

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