Eulerova funkcia φ, Eulerova veta, malá Fermatova veta, modulárne umocňovanie, RSA

Eulerova funkcia φ

• $\varphi : \mathbb{N} \to \mathbb{N}$
$n \mapsto$ počet čísel medzi 1 až n nesúdeliteľných s n, t.j.
$\varphi(n) = |\{k \in \mathbb{N} : (1 \le k \le n) \wedge (k, n) = 1\}|$
• Pre $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ je

$$\begin{aligned}\varphi(n) =& \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = \\ =& (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = \\ =& n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).\end{aligned}$$

Odvodenie:
• Pre p^α, $\alpha > 0$, p-prvočíslo: $d | p^\alpha \Leftrightarrow p | d$
Označme $X = \{1, 2, \ldots, p^\alpha\}$ a X_p množinu násobkov p v X. Potom
$\varphi(p^\alpha) = |X| - |X_p| = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$.
• Pre $p^\alpha q^\beta$, $\alpha, \beta > 0$, p, q-prvočísla: $d | p^\alpha q^\beta \Leftrightarrow p | d \vee q | d$.
Označme X čísla od 1 do $p^\alpha q^\beta$, X_p čísla z X deliteľné p a X_q čísla z X deliteľné q.
Potom $\varphi(p^\alpha q^\beta) = |X| - |X_p \cup X_q|$.
Z princípu zapojenia a vypojenia (inklúzie-exklúzie) dostávame, že
$|X_p \cup X_q| = |X_p| + |X_q| - |X_p \cap X_q| = \frac{|X|}{p} + \frac{|X|}{q} - \frac{|X|}{pq}|$.
$\varphi(p^\alpha q^\beta) = |X| - \frac{|X|}{p} - \frac{|X|}{q} + \frac{|X|}{pq} = |X|(1 - \frac{1}{p})(1 - \frac{1}{q})$.
• Pre $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $\alpha_i > 0$, p_i-prvočísla:

$$d | p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \Leftrightarrow p_1 | d \vee p_2 | d \vee \ldots \vee p_k | d.$$

Označme X čísla od 1 po n, X_{p_i} čísla z X deliteľné p_i, $i = 1, 2, \ldots, k$.
$\varphi(n) = |X| - |X_{p_1} \cup X_{p_2} \cup \ldots \cup X_{p_k}|$.
$|X| - |X_{p_1} \cup X_{p_2} \cup \ldots \cup X_{p_k}| = |X| - |(X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}) \cup X_{p_k}| = |X| - |X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}| - |X_p| + |(X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}) \cap X_p| = |X| - |X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}| - \frac{|X|}{p_k} - \frac{|X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}|}{p_k} = (1 - \frac{1}{p_k})(|X| - |X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}|) = |X|(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$.

Eulerova a malá Fermatova veta

• **Eulerova veta:** Ak $(a, n) = 1$, tak $a^{\varphi(n)} \equiv 1 \pmod{n}$.
• **Malá Fermatova veta:** - ak p je prvočíslo, tak $a^p \equiv a \pmod{p}$
- ak p je prvočíslo, $(a, p) = 1$, tak $a^{p-1} \equiv 1 \pmod{p}$

• Využitie: $a^{b^{c^{\cdots}}} \equiv (a \mod n)^{(b \mod \varphi(n))^{(c \mod \varphi(\varphi(n)))^{\cdots}}} \pmod{n}$ za predpokladu, že $(a, n) = (b, \varphi(n)) = (c, \varphi(\varphi(n))) = \ldots = 1$

Modulárne mocniny

- **Výpočet** $x^k \pmod{n}$:
  - Prevod do dvojkovej sústavy: $k = (b_m b_{m-1} \dots b_1 b_0)_2$
  - Výpočet $y_k := x^{2^k} \pmod{n}$ rekurentne pre $k = 0, 1, \dots, m$
  - $y_0 := x \mod n$, $y_k := y_{k-1}^2 \mod n$, $k > 0$
  - Nech $b_{i_1}, \dots, b_{i_m}$ sú jednotky v binárnom zápise k, potom $x^k \mod n = y_{i_1} y_{i_2} \dots y_{i_m} \mod n$
  - Algoritmus:

  Vstup: `x, k`
  Výstup: `result`

```
result:=1;
y:=x (mod n);
while (k>0)
   if (k je nepárne) then
      result:=result * y (mod n);
   y:=y*y (mod n);
   k:=k div 2;
```

- Ešte pred aplikáciou predošlého algoritmu je vhodné, čo najviac zjednodušiť základ i exponent.
  (1) $x^k \mod n = (x \mod n)^k \mod n$
  (2) ak $(x, n) = 1$, tak $x^k \mod n = x^{k \mod \varphi(n)} \mod n$
  (3) $x^k \mod n = (x - u \cdot n)^k \mod n$ (prechod k záporným základom)

RSA

- Rivest, Shamir, Adleman
  - Zvolia sa 2 dostatočne veľké prvočísla p, q
  - Vypočíta sa $n = pq$, $\varphi(n) = (p-1)(q-1)$
  - Zvolí sa veľké $1 < e < \varphi(n)$ také, že $(e, \varphi(n)) = 1$
  - Vypočíta sa $d = e^{-1} \pmod{\varphi(n)}$, t.j. $ed \equiv 1 \pmod{\varphi(n)}$
  - Zverejní sa n, e (Public key)
  - V tajnosti ostáva p, q, d (Secret key)

  Šifrovanie: $x \mapsto x^e \pmod{n}$
  Dešifrovanie: $y \mapsto y^d \pmod{n}$

Korektnosť RSA - po dešifrovaní zašifrovaného dostávame pôvodný text.
Pre $(a, n) = 1$ platí:
$(a^e \mod n)^d \mod n = (a^{ed}) \mod n = a^{ed \mod \varphi(n)} \mod n = a^1 \mod n = a.$

- Podmienka $(a, n) = 1$ je v praxi splnená, pretože sa šifrujú znaky kódované nejakým kódovaním (číselne < 256, či < 65536) a prvočísla sú veľmi veľké (1024, 2048 a viac bitové), čo zodpovedá hodnotám 10^{308} ($10^{1024 \log_{10} 2}$), či 10^{616} ($10^{2048 \log_{10} 2}$).

Cvičenia

- 1. Vypočítajte hodnoty:
  (a) $\varphi(48)$, (b) $\varphi(468)$, (c) $\varphi(63)$, (d) $\varphi(196)$
- 2. Vypočítajte:
  (a) $59^{375} \mod 63$, (b) $127^{78} \mod 37$, (c) $57^{857} \mod 43$, (d) $12^{37} \mod 77$
- 3. Určte parametre RSA a zakódujte správu 5, 10, 66, 37 (následne tú zakódovanú odkódujte) pre
  (a) $p = 11$, $q = 17$, $e = 79$
  (b) $p = 73$, $q = 109$, $e = 343$
  (c) $p = 17$, $q = 23$, $e = 169$
  (d) $p = 11$, $q = 19$, $e = 91$

Riešené príklady

- Určte $\varphi(576)$.

Riešenie:

Rozložíme do kanonického tvaru (na súčin prvočísel) a dosadíme do vzorca. $576 = 4 \cdot 144 = 2^6 \cdot 3^2$. Preto $\varphi(576) = \varphi(2^6)\varphi(3^2) = (2^6 - 2^5)(3^2 - 3) = 32 \cdot 6 = 192$. Alebo $\varphi(576) = 576 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 576 \cdot \frac{1}{3} = 192$.

- Určte $147^{573} \mod 68$.

Riešenie:

Najprv sa pokúsime zjednodušiť počítanú mocninu:

$147^{573} \equiv 11^{573} \mod 68$, $(11, 68) = 1$, preto

$11^{573} \equiv 11^{573 \mod \varphi(68)} = 11^{573 \mod 32} = 11^{29} \mod 68$

Prevod do dvojkovej sústavy.

$29 : 2 = 14$ zv. 1, $14 : 2 = 7$ zv. 0, $7 : 2 = 3$ zv. 1, $3 : 2 = 1$ zv. 1, $1 : 2 = 0$ zv. 1.

$29_{10} = (11101)_2$, treba počítať od 0 do 4 (od 1 do 5).

Samotné výpočty mocnín $y_i = a^{2^i}$ modulo 68.

$y_0 = 11 \mod 68 = 11$

$y_1 = y_0^2 \mod 68 = 121 \mod 68 = -15 \mod 68 = 53$

$y_2 = y_1^2 \mod 68 = (-15)^2 \mod = 225 \mod 68 = 21$

$y_3 = y_2^2 \mod 68 = 13^2 \mod 68 = 169 \mod 68 = 33$

$y_4 = y_3^2 \mod 68 = 33^2 \mod 68 = 1089 \mod 68 = 1$

Dosadenie tých hodnôt y_i pre ktoré je na pozícii pri 2^i, či $(i+1)$.pozícii jednotka.

$147^{573} \mod 68 = 11^{29} \mod 68 = y_0 \cdot y_2 \cdot y_3 \cdot y_4 \mod 68 = 11 \cdot 21 \cdot 33 \cdot 1 \mod 68 = 7623 \mod 68 = 7$.

- Určte parametre RSA pre $p = 11$, $q = 23$, $e = 81$ a zašifrujte správu 15 a aj ju dešifrujte.

Riešenie:

Parametre RSA:

$n = 11 \cdot 23 = 253$, $\varphi(n) = \varphi(11)\varphi(23) = 10 \cdot 22 = 220$

$d = 81^{-1} \mod 220$

Zovšeobecnený Euklidov algoritmus pre dvojicu $(81, 220)$.

$220 : 81 = 2$ zv. 58

$81 : 58 = 1$ zv. 23

$58 : 23 = 2$ zv. 12

$23 : 12 = 1$ zv. 11

$12 : 11 = 1$ zv. 1

$11 : 1 = 11$ zv. 0

$1 = 1 \cdot \mathbf{12} - 1 \cdot \underline{\mathbf{11}} = 1 \cdot 12 - 1 \cdot (1 \cdot \mathbf{23} - 1 \cdot \mathbf{12}) = 2 \cdot \underline{\mathbf{12}} - 1 \cdot \mathbf{23} = 2 \cdot (1 \cdot \mathbf{58} - 2 \cdot \mathbf{23}) - 1 \cdot \mathbf{23} = 2 \cdot \mathbf{58} - 5 \cdot \underline{\mathbf{23}} = 2 \cdot \mathbf{58} - 5 \cdot (1 \cdot \mathbf{81} - 1 \cdot \mathbf{58}) = 7 \cdot \underline{\mathbf{58}} - 5 \cdot \mathbf{81} = 7 \cdot (1 \cdot \mathbf{220} - 2 \cdot \mathbf{81}) - 5 \cdot \mathbf{81} = 7 \cdot \mathbf{220} - 19 \cdot \mathbf{81}$

Preto $d = -19 \mod 220 = 201$.

Verejný kľúč: $n = 253$, $e = 81$

Tajný kľúč: $p = 11$, $q = 23$, $d = 201$.

Šifrovanie:

$15 \mapsto 15^{81} \mod 253$

$81 : 2 = 40$ zv. 1, $40 : 2 = 20$ zv. 0, $20 : 2 = 10$ zv. 0, $10 : 2 = 5$ zv. 0, $5 : 2 = 2$ zv. 1, $2 : 2 = 1$ zv. 0, $1 : 2 = 0$ zv. 1.

$81_{10} = 1010001_2$. Treba počítať y_0 - y_6.

$y_0 = 15 \mod 253 = 15$

$y_1 = y_0^2 \mod 253 = 15^2 \mod 253 = 225 \mod 253 = -28$

$y_2 = y_1^2 \mod 253 = (-28)^2 \mod 253 = 784 \mod 253 = 25$

$y_3 = y_2^2 \mod 253 = 25^2 \mod 253 = 625 \mod 253 = 119$

$y_4 = y_3^2 \mod 253 = 119^2 \mod 253 = 14161 \mod 253 = 246 = -7$

$y_5 = y_4^2 \mod 253 = (-7)^2 \mod 253 = 49$

$y_6 = y_5^2 \mod 253 = 49^2 \mod 253 = 2401 \mod 253 = 124$

$15^{81} \mod 253 = y_6 \cdot y_4 \cdot y_0 \mod 253 = 124 \cdot (-7) \cdot 15 \mod 253 = -13020 \mod 253 = -117 \mod 253 = 136$.

Dešifrovanie:

$136 \mapsto 136^{201} \mod 253$

Výpočet 136^{201}:

$201_{10} = 11001001_2$, preto treba počítať y_0-y_7.

$y_0 = 136 \mod 253 = 136$

$y_1 = y_0^2 \mod 253 = 136^2 \mod 253 = 18496 \mod 253 = 27$

$y_2 = y_1^2 \mod 253 = 27^2 \mod 253 = 729 \mod 253 = 223 = -30$

$y_3 = y_2^2 \mod 253 = (-30)^2 \mod 253 = 900 \mod 253 = 141$

$y_4 = y_3^2 \mod 253 = 141^2 \mod 253 = 19881 \mod 253 = 147$

$y_5 = y_4^2 \mod 253 = 147^2 \mod 253 = 21609 \mod 253 = 104$

$y_6 = y_5^2 \mod 253 = 104^2 \mod 253 = 10816 \mod 253 = 190 = -63$

$y_7 = y_6^2 \mod 253 = (-63)^2 \mod 253 = 3969 \mod 253 = 174 = -79$

$136^{201} \mod 253 = y_7 \cdot y_6 \cdot y_3 \cdot y_0 \mod 253 = (-79) \cdot (-63) \cdot 141 \cdot 136 \mod 253 = 170 \cdot 201 \mod 253 = 15$.