

Samostatná úloha na RSA

Zadáno: 12.1.2009

Odevzdat do: 23.1.2009 12:00

Příjmení a jméno:

Skupina:

Algoritmus RSA s parametry $p = 16777199$, $q = 16777213$ a $e = 65537$ šifruje otevřený text

Příliš žluťoučký kůň úpěl ďábelské ódy.

doplněný na konci mezerami na délku $3m$ osmibitových znaků (délka zpracovávaného řetězce textu je tedy vždy dělitelná třemi). Text se zpracovává ve skupinách po třech znacích na šifrovaný text, jenž má v hexadecimálním zápisu tvar

```
dc2444aa4953 3c7061337cf0 9891b19bf647 1a61c1c9f117 7eedbdfddd0b
098a73781a85 9539e8384ae3 c3f96ac3188b f413abb358cc 5cf93de289e2
2284aa47a926 b40a23e994f7 a2243725f1da
```

Tento text lze dešifrovat exponentem $d = 189623958995321$.

Šifrování probíhá takto:

- doplníme do textu mezery tak, aby počet znaků byl dělitelný třemi
- vezmeme vždy trojici znaků
- převedeme jejich reprezentace na celá čísla
- modulárně umocníme
- uložíme v šestnáctkovém zápisu jako jeden blok

Čili v tom úvodním vzorovém příkladu:

- první dešifrovaný blok je `dc2444aa4953` šestnáctkově
- jeho dekadický ekvivalent je 242048328943955
- dešifruju

$$m = 242048328943955^{189623958995321} \mod (16777199 \cdot 16777213)$$

- vyjde mi 5306605 což jsou tři osmibitová čísla (šestnáctkově `50f8ed`) za sebou $\Rightarrow$
 $0x50 = 80$ ('P'), $0xf8 = 248$ ('ř'), $0xed = 237$ ('í')

- a tak dále

Toto zadání má číslo . Neexistují dvě zadání se stejným číslem.

Na adrese <http://euler.fd.cvut.cz/predmety/ma/files/rsa2008ks.html> naleznete seznam očíslovaných zadání s veřejným klíčem (n, e) , příslušnou šifrovanou zprávou a případná errata či doplnění tohoto zadání. Vaším úkolem je

1. Faktorizovat n na p a q a zvolený postup faktorizace popsat (googlete, podívejte se na loňské přednášky).
2. Určit odpovídající $\phi(n)$ a d a opět popsat zvolený postup.
3. Dešifrovat zprávu.
4. Přijít na to, odkud je ten text opsán (stačí autor)

Odpovědi

$p =$

$q =$

$\phi(n) =$

$d =$

Dešifrovaný text: