1 RM test

Zistite s pomocou RM testu, či nasledujúce čísla sú prvočísla (jednotlivé kroky počítajte s kalkulačkou).

1. $n = 252601, n-1 = 2^3 * 31575, a = 85132$. Výsledok: n je zložené, 184829 je netriviálna odmocnina z 1 mod$n$
2. $n = 3057601, n-1 = 2^6 * 47775, a = 99908$. Výsledok: n je zložené, 235899 je netriviálna odmocnina z 1 mod$n$
3. $n = 104717, n-1 = 2^2 * 26179, a = 96152$. Výsledok: n je pravdepodobne prvočíslo
4. $n = 577757, n-1 = 2^2 * 144439, a = 314997$. Výsledok: n je pravdepodobne prvočíslo
5. $n = 101089, n-1 = 2^5 * 3159, a = 5$. Výsledok: n je pravdepodobne prvočíslo
6. $n = 280001, n-1 = 2^6 * 4375, a = 105532$. Výsledok: n je pravdepodobne prvočíslo

2 Fermatova faktorizácia

Faktorizujte $91, 187$

3 Kraitchikova faktorizácia

Faktorizujte $91, 95, 115$

4 Generovanie silného prvočísla

Nájdi 10 bit strong prime.

1. $t = 11, s = 13, b = 4$
2. $2it + 1 = 23$ pre $i = 1$
3. $p_0 = 2(13^{21}) \bmod 23 * 13 - 1 = 415$
4. $p = 415 + 2j23 * 13 = 1023, j = 1, b = 10$

Nájdi 15 bit strong prime.... volte $b = 5, t = 17, s = 19$ ... $p =$?

5 Rabinov KS

Dešifrujte správu $y = 2$ ak $7 * 19 = 133, B = 1, 4^{-1} \bmod 133 = 100$,

6 ElGamalov KS

$p = 11, a = 2, c = 2^3, x = 5, k = 4$
$y_1 = 2^4 = 5 \bmod 11, y_2 = 9 \bmod 11, y_2(y_1^3)^{-1} \bmod 11 = 5$

7 ElGamalov EC

Nájdite všetky body krivky $y^2 = x^3+x+1 \bmod 5$ aj tabulku... $(2,1),(2,4),(3,1),(3,4),(4,2),(4,3)$.

Nájdite všetky body krivky $y^2 = x^3 + 3x + 2 \bmod 13$ aj tabulku... POZOR NA $p \bmod 4$! Najpr $Q_1 3 = \{4, 9, 3, 12, 10, 1\}$, 5 bodov $x = 11, 9, 4, 12$.

Nech $y^2 = x^3 + x + 6 \bmod 11$.

Nájdite súčet bodov.

1. $(2,7) + (5,9) = (2,4), \lambda = 8$
2. $(2,7) + (2,7) = (5,2), \lambda = 8$

Nájdite body EC

1. volte $x = 4$ nie je bod EC
2. volte $x = 2$ je bod EC

8 Menezes Vanstoneho KS

$y^2 = x^3 + x + 6 \bmod 11$
Tajná hodnota je $b = 7$, náhodne zvolená hodnota $k = 6$, verejný kľúč je $P = (2,7), Q = bP = (7,2)$. Nech správa je $x = (9,1)$. (Uvedomte si, že $x \notin E$.)
Šifrovanie:

- $R = kP = 6(2,7) = (7,9), kQ = 6(7,2) = (8,3) = (c_1, c_2)$
- $y_1 = c_1 x_1 \bmod 11 = 8 * 9 \bmod 11 = 6$
- $y_2 = c_2 x_2 \bmod 11 = 3 * 1 \bmod 11 = 3$
- $y = (R, y_1, y_2) = ((7,9), 6, 3)$.

Dešifrovanie:

- $bR = bkP = k(bP) = kQ = (c_1, c_2) = (8,3)$
- $x_1 = y_1 c_1^{-1} \bmod 11 = 9$
- $x_2 = y_2 c_2^{-1} \bmod 11 = 1$