Metoda Rabina, Metoda RSA

Zadanie 1. Czy istnieje $a \in Z$ takie, że

(a) $a \equiv 4 mod 6$ oraz $a \equiv 5 mod 35$

(b) $a \equiv 4 mod 7$ oraz $a \equiv 1 mod 19$

(c) $a \equiv 7 mod 8$ oraz $a \equiv 5 mod 12$

Zadanie 2. Dany jest kod: życie -24, infomatyka- 26,
królowa nauk -17, zmieniająca się pogoda -211, pudełko czekoladek- 30,
Stosując metodę Rabina dla $n = 19 \cdot 23$ odszyfruj hasło:
....139..... jest jak .....26.....

Zadanie 3. Dany jest kod: matematyka -279, nauka -180, zabawa- 26,
Stosując metodę Rabina dla $n = 19 \cdot 23$ odszyfruj hasło, które jest cytatem Alberta Einsteina:
"239 jest najdoskonalszą formą nauki"

Zadanie 4. Stosując metodę Rabina dla podanych p, q odszyfruj podane liczby

(a) $p = 11, q = 19, m = 45$ odp do 4 ukladów równań $\{65, 122, 87, 144\}$

(b) $p = 19, q = 31, m = 102$ odp$\{65, 369, 220, 524\}$

(c) $p = 43, q = 31, m = 273$ odp $\{201, 760, 1906, 1132\}$

(d) $p = 11, q = 23, m = 243$ odp $\{109, 98, 155, 144\}$

(e) $p = 23, q = 7, m = 105$ odp$\{63, 98, 63, 98\}$

(f) $p = 7, q = 11, m = 56$ odp $\{21, 56, 21, 56\}$

Zadanie 5. Stosując metodę RSA dla podanych p, q zaszyfruj l odszyfruj m

(a) $p = 5, q = 3, e = 7, l_1 = 10, l_2 = 7$ odp $m_1 = 10, m_2 = 13$

(b) $p = 17, q = 5, e = 13,$
$l_1 = 27(m_1 = 62), l_2 = 14(m_2 = 39), l_3 = 32(m_3 = 2) l_4 = 5, m_4 = 20$

(c) $p = 11, q = 23, e = 17,$
$l_1 = 16, l_2 = 8, l_3 = 32, (m_1 = 234, m_2 = 13, m_3 = 164)$

(d) $p = 11, q = 23, e = 31,$
$l_1 = 234, l_2 = 13, l_3 = 164, (m_1 = 36, m_2 = 233, m_3 = 87)$