Kryptografia

Lista nr 5, 13 V

1. Udowodnij, że dla dowolnego n istnieje liczba pierwsza $p > n$, która dzieli $\binom{2n}{n}$.
2. Pokaż, że dla $n \geq 2k$ istnieje liczba pierwsza $p > k$, która dzieli $\binom{n}{k}$.
3. Pokaż, że każda liczba pierwsza postaci $p = 4m + 1$ może być zapisana jako $p = x^2 + y^2$, dla pewnych liczb naturalnych x, y.
4. Udowodnij, że "książkowe" RSA nie jest CCA-secure, w szczególności mając kryptogram c napisz jak wybrać kryptogram $c' \neq c$ taki, że znajomość tekstu jawnego $x' = \mathsf{Dec}_K(c')$ pozwala na znalezienie x $(= \mathsf{Dec}_K(c))$.
5. O tekście jawnym x powiemy, że jest punktem stałym dla aszyfrowania jeżeli $\mathsf{Enc}_K(x) = x$. Pokaż, że dla "książkowego" RSA liczba punktów stałych $x \in Z_n^*$ jest równa: $\gcd(e-1, p-1) \cdot \gcd(e-1, q-1)$ (gdzie $n = pq, [N, e]$ - klucz publiczny).
6. Wykorzystaj metodę faktoryzacji $p-1$ do rozłożenia liczb 262063 i 9420457, wypróbuj różne ograniczenia na B.
7. Wykorzystaj metodę faktoryzacji $\rho - Pollard'a$ do rozłożenia liczb: $262063, 420457, 181937053$. Jako f przyjmij $f(x) = x^2 + 1$. Ile kroków wykonał algorytm w każdym z przypadków?
8. Pokaż, że jeżeli $n = pq$ oraz, że jeżeli dla pewnej małej liczby naturalnej d istnieje liczba k taka, że $k^2 = n + d^2$ to znajomość d może posłużyć do faktoryzacji n. Zaprezentuj technikę dla $n = 2189284635403183$.
9. Zaprezentuj działanie algorytmu Wiener'a (ułamek łańcuchowy) dla klucza publicznego $[n, e] = [317940011, 77537081$.