Kryptografia
przykładowe zadania na Minikolokwium 1

Tematy na minikolokwium 1: Liczba cyfr binarnych n. Złożoność dodawania/mnożenia/dzielenia liczb. Grupy, w szczególności $\mathbb{Z}/n$ oraz $\Phi(n)$. Działanie i elementy odwrotne w tych grupach. Reszty kwadratowe $(\mathrm{mod}\ p)$. Rząd elementu w grupie.

1. Ile cyfr binarnych ma w przybliżeniu n?
2. Jaką złożoność obliczeniową ma dodawanie/odejmowanie/mnożenie/dzielenie dwóch liczb mniejszych od n?
3. Czy $(\mathbb{N}, +)$ jest grupą? Czy $(\mathbb{Z}, \cdot)$ jest grupą?
4. Jakie elementy ma $\mathbb{Z}/10$? A $\Phi(10)$? Oblicz $3 \cdot 9$ w $\Phi(10)$.
5. Znajdź $7^{-1} \pmod{10}$.
6. Czy 2 jest resztą kwadratową mod 7?
7. Znajdź rząd elementu 4 w $\Phi(7)$.
8. Znajdź rząd elementu 4 w $(\mathbb{Z}_7, +)$.