Kryptografia z elementami algebry

Laboratorium 2, algorytmy RSA i ElGamala oraz ich bezpieczeństwo

1. Zaimplementuj algorytm ElGamala. Wykorzystaj własną bibliotekę z arytmetyką na wielkich liczbach. Pamiętaj o efektywnej metodzie konstruowania grupy $\Phi(p)$ znajdowaniu jej generatora.

2. Zaimplementuj algorytm RSA. Wykorzystaj własną bibliotekę z arytmetyką na wielkich liczbach.

3. Zaimplementuj algorytm szybkiego szyfrowania RSA. Wykorzystaj Chińskie Twierdzenie o Resztach oraz własną bibliotekę z arytmetyką na wielkich liczbach. Porównaj czas metod szyfrowania RSA z zadania 2 i 3.

4. Niech $k_A = (n, d)$ będzie kluczem tajny Alice do algorytmu RSA. Załóżmy, że Mallet zna k_A. Czy Mallet potrafi faktoryzować n? Zapoznaj się z odpowiednim algorytmem oraz rozłóż na czynniki pierwsze n na podstawie klucza tajnego RSA podanego przez prowadzącego ćwiczenia.