Kryptografia z elementami algebry

RSA, ElGamal

1. Zapoznaj się z algorytmem RSA. Wygeneruj klucz publiczny i tajny dla danych $p = 7$ i $q = 11$. Zaszyfruj $M = 15$.

2. Bob posiada $K_A = (n, e)$ klucz publiczny Alice do algorytmu RSA. Wybiera w sposób losowy wiadomość M, $1 < M < n$ i szyfruje kluczem K_A. Oblicz prawdopodobieństwo wylosowania $(M, n) > 1$. Jaki wpływ na bezpieczeństwo ma wylosowania takiego M?

3. W pewnej sieci komputerowej wygenerowano wszystkim użytkownikom sieci wspólny moduł $n = pq$ algorytmu RSA. By zapewnić bezpieczeństwo kryptosystemu RSA każdemu i-temu użytkownikowi wygenerowano losowe komponenty kluczy d_i, e_i, gdzie $k_i = (d_i, n)$ oraz $K_i = (e_i, n)$ oznaczają odpowiednio klucz prywatny i publiczny RSA i-tego użytkownika. Bez znajomości d_i użytkownik j, $j \neq i$ nie potrafi deszyfrować kryptogramów i-tego użytkownika i to zapewni bezpieczeństwo całego systemu. Zastanów się czy powyższe założenie jest prawdziwe? Odpowiedź uzasadnij.

4. Załóżmy, że do trzech użytkowników wysłano identyczną wiadomość M. Każdy z użytkowników otrzymał M zaszyfrowane jego kluczem RSA. Ponieważ im mniejsze (krótsze) jest e, tym szyfrowanie przebiega szybciej, użytkownicy jako swój klucz jawny wybrali małe $e = 3$. Załóżmy, że użytkownicy mają różne moduły n_1, n_2, n_3. Jak Mallet może odkodować M na podstawie znajomości szyfrogramów wysłanych do owych użytkowników?

5. Niech x będzie kluczem tajnym Alice w kryptosystemie Elgamala oraz niech $\mathcal{K}_A = (p, g, y) = (101, 2, 29)$ będzie kluczem publicznym Alice. Oblicz najmniej znaczący bit klucza tajnego Alice? Obliczenia wykonaj metodą algorytmiczną.

6. Bob posiada $K_A = (n, e)$ klucz publiczny Alice do algorytmu RSA. W niewiadomy dla wszystkich sposób Mallet zdobył wartość $\phi(n)$. W jaki sposób Mallet potrafi obliczyć klucz tajny Alice?

7. Mallet zna $K_A = (n, e)$, $k_A = (n, d)$ klucz publiczny i tajny Alice do algorytmu RSA. W jaki sposób Mallet potrafi faktoryzować n?

8. Kluczem tajnym Alice do RSA jest $k_A = (n, d, p, q)$. Zapoznaj się z metodą szybkiego deszyfrowania RSA z wykorzystaniem CRT. Wykonaj testy numeryczne porównujące metodę deszyfrowania CRT z klasyczną.

9. Niech $n \in \mathbb{N}$ będzie liczbą złożoną. Oszacuj ile operacji elementarnych na bitach potrzeba do znalezienia liczby pierwszej $p \mid n$.

10. Zaproponuj efektywną metodę generowania grupy $\Phi(p)$ oraz jej generatora, gdzie p jest liczbą pierwszą.

11. Niech p będzie liczbą pierwszą, g generatorem grupy $\Phi(p)$. Niech $y \in \Phi(p)$. Oszacuj ile operacji elementarnych na bitach potrzeba do znalezienia $x = \log_g(y)$.

12. Zapoznaj się z algorytmem szyfrowania z kluczem publicznym ElGamala. Na jakich trudnych problemach obliczeniowych oparte jest bezpieczeństwo tego kryptosystemu?

13. Niech x będzie kluczem tajnym Alice w kryptosystemie Elgamala oraz niech $\mathcal{K}_A = (p, g, y) = (101, 2, 29)$ będzie kluczem publicznym Alice. Oblicz najmniej znaczący bit klucza tajnego Alice?

14. Bob pobrał klucz publiczny Alice $K_A = (p, g, y) = (13, 7, 12)$ do systemu ElGamala. Następnie zaszyfrował kluczem publicznym Alice wiadomość m i wysłał szyfrogram $C = (c_1, c_2) = (3, 11)$ do Alice. Oblicz m?