Kryptografia

Laboratorium - lista nr 4, 15 IV

Problem 1 Udowodnij, że jeżeli G, H są grupami to grupą jest też $G \times H$.

Problem 2 Niech $N = pq$ oraza niech $[N, e_1], [N, e_2]$ będą kluczami publicznymi Alicji i Boba. Pokaż, że jeżeli Ewa wyśle zaszyfrowaną wiadomość do Alicji $c_1 = m^{e_1} \bmod N$ i do Boba $c_2 = m^{e_2} \bmod N$ to na tej podstawie (z c_1 i c_2) można obliczyć m bez znajomości kluczy prywatnych. Jakie jest prawdopodobieństwo sukcesu Twojego ataku?

Problem 3 Załóżmy, że trzej użytkownicy RSA, Lech, Czech i Rus, mają klucze publiczne $[N_i, 3]$ dla $i = 1, 2, 3$, gdzie N_i są parami względnie pierwsze. Załóżmy, że Alicja chce przesłać ten samą wiadomość m do każdego z nich obliczając $c_i = m^3 \bmod N_i$, $1 \leq i \leq 3$. W jaki sposób można wyliczyć m posiadając c_1, c_2, c_3 (bez faktoryzowania N_1, N_2, N_3)?

Problem 4 Niech $N = pq$ będzie iloczynem dwóch różnych liczb pierwszych. Pokaż, że jeżeli $\phi(N)$ oraz N są znane to jest możliwe obliczenie p i q w wielomianowym czasie.

Problem 5 Niech $N = pq$ będzie iloczynem dwóch różnych liczb pierwszych. Pokaż, że jeżeli N i liczba całkowita d taka, że $3d = 1 \bmod \phi(N)$ są znane to można znaleźć p i q w czasie wielomianowym.

Problem 6 Znajdź ciąg $(a_i)_{i \geq 1}$ liczb naturalnych, dla których algorytm Euklidesa potrzebuje dokładnie i iteracji do obliczenia $\gcd(a_{i+1}, a_i)$.

Problem 7 Udowodnij, że jeżeli $\gcd(a, m) = 1$ oraz $\gcd(b, m) = 1$ to $\gcd(ab, m) = 1$.

Problem 8 Wykorzystaj test Fermata do udowodnienia, że piąta liczba Fermata $F_5 = 2^{2^5} + 1$ jest liczbą złożoną. Udowodnij, że każda liczba Feramta jest pseudopierwsza względem 2.

Problem 9 Wykorzystaj test Millera-Rabina do udowodnienia, że piąta liczba Fermata jest złożona.

Problem 10 Pokaż, że w RSA wykładnik deszyfrujący d może być wybrany tak, aby $de = 1 \bmod lcm(p-1, q-1)$ (zamiast $de = 1\phi(N)$).

Problem 11 Działanie $\oplus$ dla liczb Fibonacciego jest zdefiniowane następująco: $F_i \oplus F_j = F_{i+j}$. Każdą liczbę naturalną N możemy w jednoznaczny sposób przedstawić za pomocą sumy liczb Fibonacciego (wykorzystując w tym celu algorytm zachłanny) $N = F_{i_1} + F_{i_2} + \ldots + F_{i_k}$ tak, że w reprezentacji nie występują dwie kolejne liczby Fibonacciego (tzw. reprezentacja Zeckendorffa).

Dla $N = F_{i_1} + \ldots + F_{i_n}, M = F_{j_1} + \ldots + F_{j_m}$ niech

$$\begin{aligned} N \oplus M \;=\; & F_{i_1+j_1} + \; F_{i_1+j_2} + \; \ldots + \; F_{i_1+j_m} \\ & \qquad \ldots \\ & F_{i_n+j_1} + \; F_{i_n+j_2} + \; \ldots + \; F_{i_n+j_m} \end{aligned}$$

Pokaż, że działanie $\oplus$ jest przemienne i łączne. Pokaż jak mając $N \oplus M$ obliczyć NM. Pokaż jak mając NM obliczyć $N \oplus M$.