19 kwietnia 2024

Zadania z kryptografii, lista nr 6

1. Pokaż jak znając $n = pq$ i $\varphi(n)$ można prosto wyliczyć p i q.

2. Pokaż, że jeśli m nie jest względnie pierwsze z $n = pq$ to w RSA również $m^{ed} \bmod n = m$.

3. Alicja chce przesłać tę samą wiadomość m do Boba i Charliego za pomocą kryptosystemu RSA. Bob i Charlie używają tego samego n, ale różnych wykładników klucza jawnego e_B i e_C. Załóżmy ponadto, że $\gcd(e_B, e_C) = 1$. Pokaż, jak Oskar może odszyfrować wiadomość m po przechwyceniu jej szyfrogramów przeznaczonych dla Boba i Charliego. Czy daje to mu możliwość odtworzenia kluczy deszyfrujących.

4. Alicja chce przesłac tę samą wiadomość m do Boba, Charliego i Davida za pomocą kryptosystemu RSA. Załóżmy, że $e_B = e_C = e_D = 3$ dla różnych n_B, n_C, n_D. Pokaż, jak Oskar może odszyfrować wiadomość m po przechwyceniu jej szyfrogramów.

5. Wiadomość m jest punktem stałym kryptosystemu RSA, gdy $m^e \bmod n = m$. Pokaż, że liczba punktów stałych kryptosysytemu RSA wynosi $(\gcd(e-1, p-1)+1) \cdot (\gcd(e-1, q-1)+1)$ gdzie $n = pq$.

6. Pokaż, że dla $n = pq$ jeśli dla wszystkich m mamy $m^{ed} \equiv m \bmod n$, to $ed \equiv 1 \bmod \mathrm{NWW}(p-1, q-1)$.

7. Alicja otrzymała od Boba wiadomość m zaszyfrowaną swoim kluczem publicznym RSA. Oskar zna szyfrogram c tej wiadomości. Alicja zaoferowała udostępnić Oskarowi maszynerię deszyfrującą pod warunkiem, że nie będzie odszyfrowywał nią c. Pokaż, jak używając raz tej maszynerii Oskar może jednak odszyfrować c podając do odszyfrowania losowy szyfrogram.

8. Pokaż w jaki sposób można przeszyfrować szyfrogram ElGamala uzyskując z szyfrogramu $(g^x, h^x m)$ nowy szyfrogram $(g^y, h^y m)$ będący szyfrogramem ElGamala wiadomości m dla losowego y nie mając dostępu do klucza prywatnego.

9. (trójprzebiegowy protokół Shamira) W protokole obie strony mają uzgadnioną liczbę pierwszą $p = 2q + 1$. Alicja chce przesłać wiadomość $m \in \mathbb{Z}_p^*$ rzędu q. Alicja losuje $a \in \mathbb{Z}_q^*$, Bob losuje $b \in \mathbb{Z}_q^*$.

   - $A \to B : m^a$,
   - $B \to A : (m^a)^b$,
   - $A \to B : (m^{ab})^{a^{-1}} = m^b$,
   - B wylicza $m = (m^b)^{b^{-1}}$.

   Pokaż, że Oskar nie umie wyliczyć m z przechwyconej komunikacji przy założeniu CDH.

10. Pokaż, jak osoba znająca n, e, d gdzie $n = pq$ a e i d są odpowiednio jawnym i tajnym wykładnikiem RSA może sfaktoryzować n. Możliwym rozwiązaniem jest wielokrotne powtórzenie następującej procedury

    - Zachodzi $ed - 1 = 2^k m$, gdzie $k > 0$ i m nieparzyste.
    - Wylosuj $x \in \mathbb{Z}_n$.
    - Oblicz $x^m, x^{2m}, x^{4m}, \ldots, x^{2^k m}$.
    - W powyższym ciągu znajdź ostatni element z różny od 1.
    - Jeśli $z = x^{2^k m}$, to $p = \mathrm{NWD}(x, n)$.
    - Jeśli $z \neq -1$, to $p = \mathrm{NWD}(z-1, n)$.

    Uzasadnij, że powyższa metoda prowadzi do wyliczenia p dla co najmniej połowy wszystkich możliwych wartości x.