Praca MacWilliamsa i Sloane'a [125] stanowi standardowe odniesienie dla teorii kodowania. Najnowszy podręcznik na ten temat to Huffman i Pless [98].

Bitcoin został po raz pierwszy opisany w białej księdze [144]. Jako czytelne podręcznikowe wprowadzenie polecamy [155].

Ćwiczenia

13.1. W kryptosystemie Cocksa opartym na tożsamości sprawdź, czy

$$\left(\frac{1+K_{\mathcal{U}}^{pryw}(t_1)^{-1}}{n}\right)=\pm 1.$$

13.2 Przyjmijmy, że kryptosystem Cocksa oparty na tożsamości został zaimplementowany z głównym kluczem publicznym $n = 16402692653$ i przyjmijmy, że użytkownik $\mathcal{U}$ ma klucz publiczny $K_{\mathcal{U}}^{pub} = 9305496225$.

(a) Niech $t_1 = 3975333024$ oraz $t_2 = 4892498575$. Sprawdź, czy $\left(\frac{t_1}{n}\right)=\left(\frac{t_2}{n}\right)=-1$.

(b) Zaszyfruj tekst jawny $x = -1$, korzystając z „losowych" wartości t_1 i t_2, otrzymując szyfrogram (y_1, y_2).

(c) Biorąc pod uwagę, że $K_{\mathcal{U}}^{pryw} = 96465$, sprawdź, czy odszyfrowanie (y_1, y_2) jest równe x.

13.3. Przyjmijmy, że masz przykład problemu **BDH**, a konkretnie składającego się z:

- grup addytywnych $(G_1,+)$ i $(G_2,+)$ rzędu q (q jest liczbą pierwszą) oraz multiplikatywnej grupy $(G_3, \cdot)$ rzędu q,
- parowania e_q: $G_1 \times G_2 \to G_3$,
- elementu $P \in G_1$,
- elementu $Q \in G_2$ rzędu q oraz
- elementów aQ, $bQ \in G_2$ dla pewnych a, $b \in \mathbb{Z}_q^*$.

Pokaż, że jeśli możesz rozwiązać problem **CDH** w G_3, to możesz rozwiązać dany przykład problemu **BDH**.

13.4. Celem tego pytania jest wykonanie pewnych obliczeń z użyciem kryptosystemu Pailliera. Przyjmijmy, że $p = 1041817$ oraz $q = 716809$.

(a) Niech $x_1 = 726095811532$, $r_1 = 270134931749$, $x_2 = 450864083576$ oraz $r_2 = 378141346340$. Oblicz $y_1 = e_K(x_1, r_1)$ i $y_2 = e_K(x_2, r_2)$.

(b) Niech $y_3 = y_1y_2 \bmod n^2$. Oblicz $x_3 = d_K(y_3)$, korzystając z algorytmu odszyfrowania dla kryptosystemu Pailliera .

(c) Sprawdź, czy $x_3 \equiv x_1 + x_2 \pmod{n}$.