Zadania na zajęcia z kryptografii na WWW 2026

Kwiecień 2026

Zadanie 1. Krzywa eliptyczna

Proszę się nie przerazić pojęciem *krzywa eliptyczna*. Poniższe zadanie sprawdza, czy umiecie liczyć w arytmetyce modulo. Wszystkie wzory są podane. Zadanie nie jest trudne, jego celem jest przygotowanie do tego co będzie na zajęciach, tzn. chodzi o uświadomienie, że pracujemy z namacalnymi obiektami. Przeliczenie prostego przykładu na pewno będzie przydatne w lepszym zrozumieniu rzeczy zaprezentowanych na zajęciach, kiedy to pokażemy skąd wzięły się poniższe wzory.

Sztuczne inteligencje oczywiście potrafią rozwiązać te zadania, ale to nie o to chodzi, żeby po prostu skopiować rozwiązania z czata, tylko to samemu przeliczyć, a przynajmniej zrozumieć dlaczego czat wypluł taki wynik, a nie inny.

Wszelakoż zachęcam do skorzystania z dostępnych pomocy, zwłaszcza w przypadku, jeśli nie będziecie czegoś rozumieli. Cuda techniki potrafią fajnie tłumaczyć wszelakie kwestie, acz oczywiście nie należy podchodzić do nich bezkrytycznie.

Dla krzywej eliptycznej określonej równaniem:

$$y^2 = x^3 + ax + b$$

sumę dwóch różnych punktów $P = (x_P, y_P)$ oraz $Q = (x_Q, y_Q)$ wyznacza się według następujących kroków:

1. Obliczamy współczynnik s (nachylenie prostej):

$$s = (y_Q - y_P)(x_Q - x_P)^{-1}$$

2. Wyznaczamy współrzędne punktu $R = (x_R, y_R) = P + Q$:

$$x_R = s^2 - x_P - x_Q$$

$$y_R = s(x_P - x_R) - y_P$$

Polecenie: Dane są dwa punkty na tej krzywej P oraz Q. Oblicz współrzędne punktu $R = (x_R, y_R) = P + Q$. Pamiętaj, że wszystkie operacje (odejmowanie, mnożenie, potęgowanie oraz odwracanie) wykonujemy w arytmetyce modularnej.

a)

Dla krzywej o parametrach $a = 7, b = 3$ nad ciałem $\mathbb{F}_{13}$ (czyli modulo 13):

$$P = (3, 5), \quad Q = (6, 12)$$

Wskazówka: Aby obliczyć $3^{-1} \pmod{13}$*, znajdź taką liczbę* $k \in \{1, \ldots, 12\}$*, dla której* $3 \cdot k \equiv 1 \pmod{13}$.

b)

Dla krzywej o parametrach $a = 1, b = 1$ nad ciałem $\mathbb{F}_{19}$ (czyli modulo 19):

$$P = (0, 1), \quad Q = (2, 7)$$

c)

Krótkie wprowadzenie do ciała $\mathbb{F}_4$:
Ciało $\mathbb{F}_4$ to rozszerzenie ciała $\mathbb{F}_2$ (arytmetyki modulo 2, gdzie $1 + 1 = 0$). W ciele $\mathbb{F}_2$ wielomian $x^2 + x + 1 = 0$ nie ma pierwiastków. Aby stworzyć ciało $\mathbb{F}_4$, dodajemy do niego nowy element – α – który jest pierwiastkiem tego wielomianu. Zachodzi więc $\alpha^2 + \alpha + 1 = 0$, co w charakterystyce 2 (gdzie dodawanie to to samo co odejmowanie) zapisujemy jako $\alpha^2 = \alpha + 1$.

Ciało $\mathbb{F}_4$ składa się z 4 elementów: $\{0, 1, \alpha, \alpha + 1\}$.

Tabela dodawania (XOR):

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Tabela mnożenia:

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Krzywa eliptyczna w charakterystyce 2:
Z uwagi na właściwości ciała $\mathbb{F}_4$, nie możemy użyć równania z początku zadania. Używamy krzywej o równaniu:

$$y^2 + xy = x^3 + ax^2 + b$$

Wzory na sumę dwóch różnych punktów $R = P+Q$ na tej krzywej wyglądają następująco:

1. Współczynnik nachylenia s:

$$s = (y_P + y_Q)(x_P + x_Q)^{-1}$$

2. Współrzędne punktu R:

$$x_R = s^2 + s + x_P + x_Q + a$$

$$y_R = s(x_P + x_R) + x_R + y_P$$

Polecenie: Dla krzywej o parametrach $a = 1, b = 1$ zdefiniowanej nad ciałem $\mathbb{F}_4$, dane są punkty:

$$P = (0, 1), \quad Q = (1, \alpha)$$

Oblicz współrzędne punktu $R = (x_R, y_R) = P+Q$. Pamiętaj, że w $\mathbb{F}_4$ dodawanie i odejmowanie to ta sama operacja.

Zadanie 2

Alicja i Bartek chcą ustalić wspólny tajny klucz za pośrednictwem publicznego, niezabezpieczonego kanału komunikacji (np. internetu). Decydują się użyć klasycznego protokołu Diffiego-Hellmana.

Wspólnie i jawnie ustalają parametry (grupę multiplikatywną):

- Liczba pierwsza: $p = 23$
- Generator grupy: $g = 5$

Alicja wybiera swój tajny klucz prywatny $a = 4$.
Bartek wybiera swój tajny klucz prywatny $b = 3$.

Polecenia:

1. Oblicz klucz publiczny Alicji (A), który wyśle ona do Bartka. Zgodnie ze wzorem:

$$A \equiv g^a \pmod{p}$$

2. Oblicz klucz publiczny Bartka (B), który wyśle on do Alicji. Zgodnie ze wzorem:

$$B \equiv g^b \pmod{p}$$

3. Ewa, podsłuchująca kanał, przechwytuje wartości p, g, A oraz B. Wyjaśnij krótko, jakiego działania matematycznego musiałaby dokonać Ewa, aby poznać tajne klucze a lub b.

4. Oblicz ostateczny, wspólny klucz tajny (K) z perspektywy Alicji (korzystając z otrzymanego od Bartka klucza B i własnego klucza a):

$$K \equiv B^a \pmod{p}$$

5. Oblicz ostateczny, wspólny klucz tajny (K) z perspektywy Bartka (korzystając z otrzymanego od Alicji klucza A i własnego klucza b):

$$K \equiv A^b \pmod{p}$$

Zadanie 3

Alicja chce przesłać Bartkowi tajną wiadomość zamkniętą w pancernej skrzynce. Zarówno Alicja, jak i Bartek posiadają własne, unikalne kłódki oraz pasujące do nich klucze (Alicja ma tylko swój klucz, Bartek tylko swój).

Wiadomość musi zostać dostarczona przez niezaufanego listonosza. Listonosz z pewnością ukradnie lub przeczyta zawartość skrzynki, jeśli w jakimkolwiek momencie podróży nie będzie ona zabezpieczona kłódką. Nie ma możliwości bezpiecznego przekazania samych kluczy z pominięciem listonosza.

Polecenie: Opisz protokół (sekwencję przesyłania skrzynki i manipulacji kłódkami), który pozwoli Alicji bezpiecznie dostarczyć wiadomość Bartkowi, tak aby listonosz nigdy nie miał dostępu do niezabezpieczonej zawartości.