

## [PTKB] Kolokwium 2 - opracowanie

### 1 Kolokwium 2 z PTKB (11.01.2012)

#### 1.1 Zadanie 1.

**Treść:** Ile razy trzeba wykonać protokół uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od  $10^{-1000}$ ?

**Rozwiązanie:** Prawdopodobieństwo udanego oszustwa po wykonaniu  $n$  eksperymentów wynosi  $(\frac{1}{2})^n$ . Rozwiązujemy równanie  $(\frac{1}{2})^x = 10^{-1000}$ .

$$\begin{aligned}\left(\frac{1}{2}\right)^x &= 10^{-1000} \\ 2^x &= 10^{1000} \\ x &= \log_2 10^{1000} \\ x &= 1000 \log_2 10 \\ x &\simeq 3321.928\end{aligned}$$

Wybieramy  $\lceil x \rceil = 3322$ .

#### 1.2 Zadanie 2.

**Treść:** Skonstruować system podpisów cyfrowych ElGamala „dla małych liczb”. Przyjąć odpowiedni klucz publiczny i prywatny. Podpisać dowolną wybraną wiadomość  $m$  i zweryfikować podpis.

**Rozwiązanie :**

1. Ustanawianie systemu. Wybieramy liczbę pierwszą np.  $p = 13$ . Jako generator grupy mnożymy  $Z_{13}^*$  można wybrać  $g = 2$ , ponieważ  $2^1(\text{mod}13) = 2$ ,  $2^2(\text{mod}13) = 4$ ,  $2^3(\text{mod}13) = 8$ ,  $2^4(\text{mod}13) = 3$ ,  $2^5(\text{mod}13) = 6$ ,  $2^6(\text{mod}13) = 12$ ,  $2^7(\text{mod}13) = 11$ ,  $2^8(\text{mod}13) = 9$ ,  $2^9(\text{mod}13) = 5$ ,  $2^{10}(\text{mod}13) = 10$ ,  $2^{11}(\text{mod}13) = 7$ ,  $2^{12}(\text{mod}13) = 1$  Jako klucz prywatny wybieramy losowo dowolną liczbę  $x \in \langle 2, p-2 \rangle$ . Wybierzmy np.  $x = 3$ . Będzie to tajemnica strony podpisującej wiadomość. Ujawniamy klucz publiczny  $y = g^x(\text{mod}p) = 2^3(\text{mod}13) = 8$ .

2. Podpisywanie wiadomości (dokumentu) przez stronę dysponującą tajnym kluczem prywatnym  $x$ . Wybieramy jako wiadomość podpisywaną dowolną liczbę  $m \in Z_{p-1}$  czyli w naszym przypadku  $m \in Z_{12}$ . Wiadomość jawna  $m$  jest więc jednym z elementów zbioru  $0, 1, 2, \dots, 11$ . Wybierzmy jako wiadomość podpisywaną  $m = 4$ . Mając  $m = 4$  i  $x = 3$  tworzymy teraz podpis wiadomości  $m = 4$  czyli odpowiednią parę uporządkowaną  $(a, b) \in Z_p^* \times Z_{p-1}$ . Losujemy  $k \in Z_{p-1}$  takie, że  $\text{NWD}(k, p-1) = 1$ . Niech to będzie  $k = 5$ . Obliczamy  $k^{-1}$  w pierścieniu  $Z_{p-1}$  czyli w pierścieniu  $Z_{12}$ . Łatwo sprawdzić, że  $k^{-1} = 5$ . Obliczamy  $a \in Z_p^*$  jako  $g^k(\text{mod}p)$ , mamy więc  $2^5(\text{mod}13) = 6$ . Obliczamy teraz  $b \in Z_{p-1}$  jako  $b = k^{-1} \otimes_{p-1} (m - 12 \cdot x \otimes [a]_{p-1})$ . Przy przyjętych i obliczonych wartościach mamy więc  $b = 5 \otimes_{12} (4 - 12 \cdot 3 \otimes_{12} 6) = 2$ . Zatem podpis  $(a, b)$  wiadomości  $m = 4$  ma postać pary uporządkowanej  $(6, 2)$  a podpisywana wiadomość 4 z podpisem to para uporządkowana  $(4, (6, 2))$ .

3. Weryfikacja podpisu. Równanie weryfikacyjne dla podpisów ElGamala ma postać:

$$y^a \otimes_p a^b = g^m$$

gdzie podnoszenie do potęgi jest jak pierścieniu  $Z_p$ . Musimy sprawdzić dla  $y = 8$ ,  $a = 6$ ,  $b = 2$ ,  $m = 4$  i  $g = 2$  czy równanie (\*) jest spełnione.

$$\begin{aligned}L &= y^a \otimes_p a^b = 8^6 \cdot 2(\text{mod}13) = 3 \\ P &= g^m = 2^4(\text{mod}13) = 3\end{aligned}$$

Mamy więc  $L = P$  i równanie weryfikacyjne (\*) jest spełnione, zatem przedstawiony do weryfikacji podpis akceptujemy.

#### 1.3 Zadanie 3.

**Treść:** Wykazać, że charakterystyka ciała skończonego (czyli najmniejsza taka liczba  $n$ , że spełniona

jest równość  $\underbrace{1 + 1 + 1 + \dots + 1}_n = 0$  jest zawsze liczbą pierwszą.

**Rozwiązanie:** Załóżmy, że  $\text{char} K = n$  i liczba  $n = m_1 m_2$ , gdzie  $m_1, m_2 \in \mathbb{N}$ , a więc  $n \cdot 1 = (m_1 m_2) \cdot 1 = 0$ . Z łączności dodawania i rozdzielności mnożenia względem dodawania w ciele  $K$  mamy  $(m_1 m_2) \cdot 1 = (m_1 \cdot 1)(m_2 \cdot 1)$ , zatem:

$$(m_1 \cdot 1)(m_2 \cdot 1) = 0$$

Jeśli  $m_1 < n$  to z definicji charakterystyki dostajemy, że  $m_1 \cdot 1 \neq 0$ , zatem istnieje element odwrotny  $(m_1 \cdot 1)^{-1}$  do  $m_1 \cdot 1$ . Mnożąc lewostronnie równość  $(m_1 \cdot 1)(m_2 \cdot 1) = 0$  przez  $(m_1 \cdot 1)^{-1}$  dostajemy  $m_2 \cdot 1 = 0$ , ponieważ jednak  $1 \leq m_2 \leq n$  to biorąc pod uwagę definicję charakterystyki ciała musimy mieć  $m_2 = n$ . Wynika stąd, że liczba  $n$  nie jest podzielna przez żadną liczbę różną od  $n$  i  $1$ , a zatem jest liczbą pierwszą.

Można też rozumować nieco inaczej. Załóżmy, że  $\text{char} K = n$  i liczba  $n$  daje się przedstawić w postaci  $n = m_1 m_2$ , gdzie  $m_1, m_2 \in \mathbb{N}$  i  $m_1, m_2 \geq 2$ , czyli  $n$  nie jest liczbą pierwszą. Wówczas  $n \cdot 1 = (m_1 m_2) \cdot 1 = (m_1 \cdot 1)(m_2 \cdot 1) = 0$ . Ponieważ  $m_1 \cdot 1 \neq 0$  i  $m_2 \cdot 1 \neq 0$  oraz  $(m_1 \cdot 1)(m_2 \cdot 1) = 0$  co nie jest możliwe, bo ciało nie ma niezerowych dzielników zera. Zatem założenie, że  $n$  nie jest liczbą pierwszą prowadzi do sprzeczności.

#### 1.4 Zadanie 4.

**Treść:** Podać przykład liczby pseudopierwszej przy podstawie 2 i 3 jednocześnie. Czy takie liczby w ogóle istnieją?

**Rozwiązanie:** Liczba naturalna jest liczbą Carmichaela wtedy i tylko wtedy, gdy:

1. Jest liczbą złożoną.
2. Dla każdego  $a \in \mathbb{N}$  z przedziału  $1 < a < n$ , względnie pierwszej z  $n$ , liczba  $(a^{n-1} - 1)$  jest podzielna przez  $n$ .

Patrząc na najmniejsze liczby Carmichaela:

$$\begin{aligned} 561 &= 3 \cdot 11 \cdot 17 \\ 1105 &= 5 \cdot 13 \cdot 17 \end{aligned}$$

widzimy, że liczba Carmichaela 1105 jest względnie pierwsza zarówno z 2, jak również 3, a więc pozwala ona stworzyć liczby pseudopierwsze  $2^{1105-1} - 1$  oraz  $3^{1105-1} - 1$ .

#### 1.5 Zadanie 5.

**Treść:** Podać przykład ciała  $GF(3^2)$ , czyli ciała o 9 elementach.

**Rozwiązanie:** Ciało  $GF(p^n)$ , gdzie  $p$  jest liczbą pierwszą oraz  $n \in \mathbb{N}$ , można wygenerować:

- Znajdując wielomian  $f(x)$  stopnia  $n$  nierozkładalny w pierścieniu  $GF(p)[x]$ .
- Znajdując wszystkie możliwe reszty z dzielenia wielomianu  $f(x)$  w pierścieniu  $GF(p)[x]$ .
- Wykorzystując działania dodawania i mnożenia wielomianów modulo  $f(x)$ .

Wielomianem drugiego stopnia nierozkładalnym w ciele  $G(3)[x]$  jest  $x^2 + 1$  (patrz: Zadanie 7.). Wszystkie możliwe reszty z dzielenia tego wielomianu w pierścieniu  $G(3)[x]$  to:  $2x+2$ ,  $2x+1$ ,  $2x$ ,  $x+2$ ,  $x+1$ ,  $x$ ,  $2$ ,  $1$ .

#### 1.6 Zadanie 7.

**Treść:** Wykazać, że wielomian  $x^2+1$  jest nierozkładalny w pierścieniu wielomianów  $GF(3)[x]$ , a jest rozkładalny w pierścieniu wielomianów  $GF(2)[x]$ .

**Rozwiązanie:** Wielomian drugiego stopnia można rozłożyć za pomocą dwóch wielomianów pierwszego stopnia, więc:

$$\begin{aligned} x^2 + 1 &= (ax + b) * (cx + d) \\ x^2 + 1 &= (ac)x^2 + (ad + bc)x + bd \end{aligned}$$

Dla ciała  $GF(3)[x]$ ,  $b, d \in \{0, 1, 2\}$  oraz  $a, c \in \{1, 2\}$  (bo wielomian musi być rozkładalny). Rozważmy wszystkie możliwe wartości  $(ad+bc) \bmod 3$ . Jeżeli  $(ad+bc) \equiv 0 \bmod 3 \Rightarrow a = 0 \wedge c = 0$ , co jest sprzeczne z dziedziną, a więc wielomian nie może być rozkładalny.

Dla ciała  $GF(2)[x]$ ,  $b, d \in \{0, 1\}$  oraz  $a, c \in \{1\}$ . Jeżeli  $(b+d) \equiv 0 \bmod 2 \Rightarrow (b=0 \wedge d=0) \vee (b=1 \wedge d=1)$ . Dla drugiego przypadku otrzymujemy w  $GF(2)[x]$ :

$$x^2 + 1 \equiv (x + 1) * (x + 1)$$

Zatem wielomian jest rozkładalny.

## 1.7 Zadanie 8.

**Treść:** Wykazać, że w grupie skończonej dla każdego  $a \in G$  mamy:  $a^{rzG} = 1$ , gdzie  $rzG$  oznacza rząd grupy  $G$ . Wykazać, wykorzystując ten fakt, twierdzenie Eulera. (Wskazówka: wykorzystać twierdzenie Lagrange'a: dla grup skończonych rząd podgrupy jest dzielnikiem rzędu grupy).

**Rozwiązanie:** W ciągu  $a^1, a^2, \dots, a^{rzG}, a^{rzG+1}$  muszą być dwa elementy równe, tzn. dla pewnych  $k', k'' \in [1, rzG + 1], k' < k''$  musimy mieć  $a^{k'} = a^{k''}$ . Zatem  $a^{k''-k'} = 1$ . Istnieje więc takie  $k \in [1, rzG](k = k'' - k')$ , że  $a^k = 1$ . Niech  $r$  będzie najmniejszym takim  $k$ , że  $a^k = 1$ , wówczas zbiór  $H = \{a^1, a^2, \dots, a^r\}$  stanowi podgrupę cykliczną rzędu  $r$  grupy  $G$ . Ponieważ, z twierdzenia Lagrange'a,  $r$  jest dzielnikiem rzędu grupy  $G$ , więc również  $a^{rzG} = 1$ .

Twierdzenie Eulera: jeśli  $n \in \mathbb{N}, n \geq 2$  i  $a \in \mathbb{N}$  oraz  $NWD(a, n) = 1$  to  $a^{\phi(n)} \equiv 1 \pmod{n}$ , gdzie  $\phi$  jest funkcją Eulera. Rozważmy grupę multiplikatywną  $Z_n^*$ . Grupa  $Z_n^*$  ma rząd równy  $\phi(n)$ . Zatem korzystając z  $a^{rzG} = 1$  dostajemy, że dla każdego  $a \in Z_n^*$  mamy  $a^{\phi(n)} \equiv 1 \pmod{n}$ . Warunek  $a \in Z_n^*$  jest równoznaczny warunkowi  $NWD(a, n) = 1$ . Zatem twierdzenie Eulera jest prostym wnioskiem z ogólnego twierdzenia teoriogrupowego  $a^{rzG} = 1$ .

## 1.8 Zadanie 10.

**Treść:** Załóżmy, że mamy dwie niezależne zmienne losowe  $X_1$  oraz  $X_2$  o wartościach w zbiorze  $Z_2 = \{0, 1\}$ . Wykazać, że jeśli  $X_1$  ma rozkład równomierny, to również  $X_1 \oplus X_2$  ma rozkład równomierny. Ten fakt jest podstawą protokołu o nazwie „rzut monetą przez telefon”.

**Rozwiązanie:** Najpierw wykażemy, że odwzorowanie  $Y = X_1 \otimes X_2$  jest zmienną losową. Ogólnie rzecz biorąc, jeśli  $(\Omega, \mathfrak{M})$  jest przestrzenią mierzalną,  $(E_t, \mathfrak{F}_t)_{t \in T}$  jest dowolną rodziną przestrzeni mierzalnych, a odwzorowania  $f_t : \Omega \rightarrow E_t$  są  $(\mathfrak{M}, \mathfrak{F}_t)$  mierzalne dla każdego  $t \in T$  to odwzorowanie  $P_{f_t} : \Omega \rightarrow \prod_{t \in T} E_t$  jest  $(\mathfrak{M}, \prod_{t \in T} \mathfrak{F}_t)$  mierzalne. Stosując ten ogólny fakt do naszej sytuacji stwierdzamy, że odwzorowanie  $(X_1, X_2)$  jest  $(\mathfrak{M}, 2^{\{0,1\}} \otimes 2^{\{0,1\}})$  mierzalne. Odwzorowanie  $S : \{0, 1\} \times \{0, 1\} \ni (x_1, x_2) \rightarrow x_1 \oplus x_2 \in \{0, 1\}$  jest oczywiście  $(2^{\{0,1\}} \otimes 2^{\{0,1\}}, 2^{\{0,1\}})$  mierzalne, zatem  $Y = X_1 \oplus X_2$  jako superpozycja odwzorowań mierzalnych  $(X_1, X_2)$  i  $S$  jest  $(\mathfrak{M}, 2^{\{0,1\}})$  mierzalne,

jest więc zmienną losową.

Udowodnimy teraz równomierność rozkładu zmiennej losowej  $Y = X_1 \oplus X_2$ . Oznaczmy:

$$\begin{aligned} A_0 &= \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 0\}, \\ A_1 &= \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 0\}, \\ B_0 &= \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 1\}, \\ B_1 &= \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 1\}. \end{aligned}$$

Wówczas zdarzenia  $A_0, A_1, B_0, B_1$  są parami rozłączne. Stąd i z niezależności zmiennych losowych  $X_1$  i  $X_2$  oznaczając  $P(X_1 = 0) = p_0, P(X_1 = 1) = p_1$  dostajemy:

$$\begin{aligned} P(Y = 1) &= P(A_1 \cup B_1) = P(A_1) + P(B_1) = \\ &= P(X_1 = 1) \cdot P(X_2 = 0) + \\ &+ P(X_1 = 0) \cdot P(X_2 = 1) = \\ &= p_1 \cdot \frac{1}{2} + p_2 \cdot \frac{1}{2} = \frac{1}{2} \end{aligned}$$

ponieważ  $p_0 + p_1 = 1$ . Podobnie:

$$\begin{aligned} P(Y = 0) &= P(A_0 \cup B_0) = P(A_0) + P(B_0) = \\ &= P(X_1 = 0) \cdot P(X_2 = 0) + \\ &+ P(X_1 = 1) \cdot P(X_2 = 1) = \\ &= p_1 \cdot \frac{1}{2} + p_2 \cdot \frac{1}{2} = \frac{1}{2} \end{aligned}$$

a więc istotnie zmienna losowa  $Y = X_1 \oplus X_2$  ma rozkład równomierny.

## 2 Zadania przygotowujące do kolokwium #2 z PTKB

### 2.1 Zadanie 2.

**Treść:** Ile razy trzeba wykonać protokół uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od  $10^{-100}$ .

**Rozwiązanie:** Patrz 1.1

### 2.2 Zadanie 3.

**Treść:** Pokazać jak musi spreparować protokół Fiata-Shamira Prover nie znający tajemnicy (a więc oszust lub zapominalski) by zawsze na wyzwanie  $e = 1$  odpowiadać prawidłowo.

**Rozwiązanie:**

1. Prover nie znający tajemnicy  $s$  prawdziwego Provera (czyli nie znający klucza prywatnego) losuje liczbę  $r \in Z_n, r \neq 0, 1$ . Podnosi do kwadratu modulo  $n$  (przypominamy, że  $n = pq$ , gdzie  $p, q$  są różnymi liczbami pierwszymi) i przesyła w pierwszym kroku protokołu do Verifiera liczbę  $x = (r^2(\text{mod } n)(s^2(\text{mod } n))^{-1})(\text{mod } n)$ , gdzie  $s \in Z_n$  jest tajemnicą (kluczem prywatnym) prawdziwego Provera,  $s^2(\text{mod } n) \in Z$ , kluczem publicznym a odwrotność jest  $n$  brana w pierścieniu  $Z_n$ .
2. Jeśli Verifier żąda w drugim kroku protokołu odpowiedzi na pytanie  $e = 1$  to Prover wysyła do Verifiera liczbę  $y = r$
3. Verifier sprawdza teraz równanie weryfikacyjne sprawdzając czy:

$$y^2(\text{mod } n) = (x * s^2)(\text{mod } n)$$

Równanie to jest dla  $y = r$  i  $x = (r^2(\text{mod } n)(s^2(\text{mod } n))^{-1})(\text{mod } n)$  Proverowi udało się dobrze odpowiedzieć na pytanie  $e = 1$  Verifiera.

### 2.3 Zadanie 33.

**Treść:** Obliczyć wartość symbolu Legendre'a: a)  $(\frac{35}{7})$  b)  $(\frac{64}{5})$

**Rozwiązanie:**

1. 
$$(\frac{35}{7}) = (\frac{5}{7})(\frac{7}{7}) = 0$$
2. 
$$(\frac{64}{5}) = (\frac{4}{5}) = 1$$

### 2.4 Zadanie 10.

**Rozwiązanie:** Patrz 1.8