[PTKB] Kolokwium 2 - opracowanie

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 $(\frac{1}{2})^x = 10^{-1000}$.

$$\begin{array}{lll} (\frac{1}{2})^x & = & 10^{-1000} \\ 2^x & = & 10^{1000} \\ x & = & \log_2 10^{1000} \\ x & = & 1000 \log_2 10 \\ x & \simeq & 3321.928 \end{array} \tag{1}$$

Wybieramy $\lceil x \rceil = 3322$.

2 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:

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

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 $(ad+bc) \equiv 0 \mod 3 \Rightarrow a = 0 \wedge c = 0$, 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 $(b + d) \equiv 0 \mod 2 \Rightarrow (b = 0 \wedge d = 0) \vee (b = 1 \wedge d = 1)$. Dla drugiego przypadku otrzymujemy w $GF(2)[x]$:

$$x^2+1 \equiv (x+1)*(x+1) \tag{3}$$

Zatem wielomian jest rozkładalny.