Kryptografia – przykładowe zadania na Test nr 3

Zagadnienia:

- wielomiany: działania, stopień, rozkładalność, dzielenie z resztą, rozszerzony Euklides (*przyda się w drugim punkcie*),
- arytmetyka w pierścieniach ilorazowych, w szczególności w ciele F_{256}. Ile elementów ma podany pierścień ilorazowy?

Przykładowe pytania:

1. Podzielić z resztą wielomian f przez g w $\mathbb{Z}_{10}[X]$, gdzie $f(x) = 2X^5 + 8X^4 + 7X^3 + 3X + 5$, $g(X) = 3X^3 + 7X^2 + 5X + 1$. Obliczyć $f + g$, $f \cdot g$.
2. Czy podany wielomian jest rozkładalny?
   (a) $x^2 + 1$ w $\mathbb{Z}[x]$,
   (b) $x^2 + 1$ w $\mathbb{Z}/2[x]$,
   (c) $x^2 + x$ w $\mathbb{Z}[x]$.
3. Ile elementów ma podany pierścień?
   - $\mathbb{Z}_2[x]$,
   - $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$,
   - $\mathbb{Z}_{10}[x]/(x^8 + x^4 + x^3 + x + 1)$,
4. W ciele $F_{256} = \mathbb{F}_2[a]$, gdzie $a^8 + a^4 + a^3 + a + 1 = 0$ znajdź wyniki następujących działań i przedstaw w najprostszej możliwej postaci:
   (a) $\frac{1}{a^2+1}$,
   (b) $(a^6 + a^5) \cdot (a^4 + a^3)$,
   (c) $(a^6 + a^5) + (a^4 + a^3)$.