5 marca 2024

Zadania z kryptografii, lista nr 3

1. (a) Pokaż, że algorytm Euklidesa można uogólnić na pierścień wszystkich wielomianów nad dowolnym ciałem $\mathbb{F}$, tak by obliczał dla dowolnych wielomianów $p(x)$ i $q(x)$ takie wielomiany $a(x)$ i $b(x)$, że
$$a(x)p(x) + b(x)q(x) = \mathrm{NWD}(p(x), q(x)).$$
gdzie $\mathrm{NWD}(p(x), q(x))$ jest wielomianem unitarnym (o wsp. 1 przy najwyższej potędze) największego stopnia dzielącym $p(x)$ i $q(x)$.

   (b) Udowodnij za pomocą tego algorytmu jednoznaczność rozkładu wielomianów na czynniki pierwsze czyli wielomiany nierozkładalne.

   (c) Pokaż jak z jednoznaczności rozkładu wielomianów wynika, że wielomian stopnia k w ciele ma co najwyżej k pierwiastków.

2. Niech $q(x)$ będzie wielomianem nierozkładalnym w $\mathbb{Z}_p$. Niech $\mathbb{Z}_p[x]/(q(x))$ będzie zbiorem reszt z dzielenia wielomianów nad $\mathbb{Z}_p$ przez $q(x)$ z dodawaniem i mnożeniem modulo $q(x)$. Pokaż, że $\mathbb{Z}_p[x]/(q(x))$ tworzy ciało. Elementy $\mathbb{Z}_p[x]/(q(x))$ mają postać
$$a_{k-1}x^{k-1} + \cdots + a_1 x + a_0,$$
gdzie k jest stopniem wielomianu $p(x)$. Jak można zaimplementować działania w ciele $\mathbb{Z}_p[x]/(q(x))$?

3. (a) Pokaż, że w dowolnym ciele skończonym $\mathbb{F}$ istnieje liczba naturalna p, że 1 dodana do siebie p razy daje w sumie 0.

   (b) Pokaż, że minimalne takie p jest liczbą pierwszą.

   (c) Pokaż, że ciało $\mathbb{F}$ jest przestrzenią liniową nad $\mathbb{Z}_p$. Jak z tego wynika, że liczba elementów $\mathbb{F}$ wynosi p^k, gdzie k jest wymiarem tej przestrzeni.

4. (a) Pokaż, że jeśli ciało skończone $\mathbb{F}$ ma m elementów, to
$$\prod_{y\in\mathbb{F}\setminus\{0\}} y = \prod_{y\in\mathbb{F}\setminus\{0\}} xy = x^{m-1} \prod_{y\in\mathbb{F}\setminus\{0\}} y$$
i powyższe implikuje, że $x^{m-1} = 1$ dla wszystkich $x \in \mathbb{F}$.

   (b) Pokaż, że jeśli k jest najmniejszą potęgą naturalną, że $x^k = 1$, a l jest najmniejszą potęgą naturalną, że $y^l = 1$ dla $x, y \in \mathbb{F}$, to istnieje $z \in \mathbb{F}$, że $n = \mathrm{NWW}(k, l)$ jest najmniejszą potęgą naturalną, że $z^n = 1$.

   (c) Pokaż, że jeśli k jest najmniejszą wspólną wielokrotnością wszystkich najmniejszych potęg z poprzedniego podpunktu, to istnieje y dla którego k jest najmniejszą potęgą naturalną, że $y^k = 1$. Ponadto dla wszystkich $x \in \mathbb{F}$ mamy $x^k = 1$. Pokaż też, że $k|m-1$.

   (d) Pokaż, że ponieważ wielomian $x^k - 1$ ma w ciele co najwyżej k pierwiastków mamy $k = m - 1$ i istnieje y takie, że wszystkie elementy $x \in \mathbb{F} \setminus \{0\}$ mają postać $x = y^i$. To znaczy, że grupa multiplikatywna ciała jest zawsze cykliczna.

5. Jaki rząd ma grupa $\mathbb{Z}^*_{p^k}$ złożona z elementów odwracalnych modulo p^k ($p > 2$ jest liczbą pierwszą). Jaki rząd w tej grupie ma element $p + 1$? Pokaż, że jest to grupa cykliczna.

6. Pokaż, że jeśli $\alpha > 2$, to grupa $\mathbb{Z}^*_{2^\alpha}$ nie jest cykliczna, ale 5 generuje grupę złożoną z połowy jej elementów (dokładnie tych, które przystają do 1 mod 4).

7. W AES S-boks oblicza wartość bajtu b w ten sposób, że

   - Jeśli $b \neq 0$, to $c = b^{-1}$ w ciele F_{2^8}, które jest ciałem wielomianów nad $\mathbb{Z}_2$ z działaniami modulo nierozkładalny wielomian ósmego stopnia. Jeśli $b = 0$, to $c = 0$.
   - Niech $c = c_0c_1c_2c_3c_4c_5c_6c_7$. Wtedy $d_i = c_i \oplus c_{i+4} \oplus c_{i+5} \oplus c_{i+6} \oplus c_{i+7}$ gdzie indeksy dodawane są modulo 8.
   - Wynikiem działania S-boksa jest $e = d \oplus 01100011$.

   Jak wygląda przekształcenie odwrotne do tego S-boksa?