

Kryptografia z elementami algebry
Laboratorium 5, AES - arytmetyka ciała \mathbb{F}_{2^8}
(Moduł 4)

Niech

$$(\mathbb{F}_{2^8}, +, \cdot)$$

1. Zaimplementuj funkcję `suma()`
Dane: $(xy)_H, (uw)_H \in \mathbb{F}_{2^8}$
Wynik: $(x'y')_H \in \mathbb{F}_{2^8}$, gdzie $(x'y')_H = (xy)_H + (uw)_H$.
2. Zaimplementuj funkcję `xtime()`
Dane: $(xy)_H \in \mathbb{F}_{2^8}$
Wynik: $(x'y')_H \in \mathbb{F}_{2^8}$, gdzie $(x'y')_H = (xy)_H \cdot (02)_H$.
3. Zaimplementuj funkcję `iloczyn()`
Dane: $(xy)_H, (uw)_H \in \mathbb{F}_{2^8}$
Wynik: $(x'y')_H \in \mathbb{F}_{2^8}$, gdzie $(x'y')_H = (xy)_H \cdot (uw)_H$.
4. Zaimplementuj funkcję `odwrotnosc()`
Dane: $(xy)_H \in \mathbb{F}_{2^8}$
Wynik: $(uw)_H \in \mathbb{F}_{2^8}$, gdzie $(xy)_H \cdot (uw)_H = (01)_H$.

UWAGA: Implementację powyższych funkcji wykonaj na bitach!