

Egzamin z Kryptografii - przykładowe pytania

1. Podaj zasadę działania szyfru *Vernama*.

Przykładowa odpowiedź: Dla ustalonej liczby naturalnej n zbiór \mathcal{M} wiadomości to $\{0, 1\}^n$. Zbiory szyfrogramów \mathcal{C} i kluczy \mathcal{K} są równe \mathcal{M} .

Szyfrowanie: dla danej wiadomości $m = (m_1, \dots, m_n)$ i klucza $k = (k_1, \dots, k_n)$ szyfrogramem wiadomości m jest

$$(k_1 \oplus m_1, \dots, k_n \oplus m_n)$$

(gdzie \oplus jest funkcją xor).

Aby odszyfrować szyfrogram $c = (c_1, \dots, c_n)$ kluczem $k = (k_1, \dots, k_n)$ obliczamy

$$(k_1 \oplus c_1, \dots, k_n \oplus c_n).$$

2. Rozważmy funkcję $f : Z_{15} \rightarrow Z_5 \times Z_3$ określoną wzorem:

$$f(x) = (a \bmod 5, x \bmod 3).$$

Czy f jest bijekcją? Odpowiedź uzasadnij.

Przykładowa odpowiedź: Tak. Wynika to Chińskiego Twierdzenia o Resztach ponieważ

- $15 = 5 \cdot 3$ oraz
- 5 i 3 są względnie pierwsze.