III KONFERENCJA DYDAKTYCZNA
Nauczanie Przedmiotów Ścisłych i Technicznych
19 października 2023r.

ZASTOSOWANIA WIELOMIANÓW NAD CIAŁAMI SKOŃCZONYMI W KRYPTOGRAFII

Mirosław Kurkowski

Wydział Matematyczno-Przyrodniczy. Szkoła Nauk Ścisłych
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
m.kurkowski@uksw.edu.pl

Jak wiadomo w algebrze rozważa się wielomiany nad pierścieniami, czyli strukturami mającymi dwa działania: addytywne i multiplikatywne. Różnorodność tych pierścieni daje całe spektrum pierścieni wielomianów o różnych własnościach. Jednymi z ciekawszych przykładów wielomianów nad ciałami skończonymi są wielomiany nad GF2, czyli nad ciałem dwuelementowym. Dobrym przykładem praktycznego zastosowania takich wielomianów jest konstrukcja algorytmu obecnego standardu szyfrowania symetrycznego, jakim jest szyfr AES. W referacie zostaną przedstawione metody reprezentacji bloków bitowych w postaci wielomianów 7-go stopnia nad GF2 będących resztami z dzielenia przez pewien wielomian pierwotny 8-go stopnia oraz definicja operacji "czarnej kropki" będącej jedną z kluczowych operacji szyfru AES. Zabawy z "czarną kropką" mogą być wykorzystywane w dydaktyce na poziomie szkoły średniej, jako ciekawostka nieco innej "rzeczywistości" matematycznej.