Politechnika Warszawska | Szkoła Doktorska nr 3

Karta przedmiotu oferowanego w Szkole Doktorskiej nr 3 – semestr letni 2021/2022

TYTUŁ
Entropia dla inżynierów
JEDNOSTKA PROWADZĄCA
Szkoła Doktorska nr 3
DYSCYPLINA NAUKOWA
Nauki fizyczne
JEDNOSTKA REALIZUJĄCA
105000 - Wydział Fizyki
OPIS SKRÓCONY PRZEDMIOTU
Treść przedmiotu to rola losowości w kryptografii, techniki tworzenia sygnałów pseudolosowych w praktyce IT oraz użytkowe wprowadzenie w kryptografię z elementami teorii bezpieczeństwa informacji oraz analizy ruchu sieciowego (analiza TCI/IP z wykorzystaniem Wireshark) 1. Generator liczb losowych Linux jako przykład generatora liczb pseudolosowych, entropia generatora, generator blokujący i nieblokujący 2. Metryki losowości, testy FIPS 140-2 generatorów liczb pseudolosowych 3. Konsekwencje braku losowości: generacja kluczy RSA 4. Faktoryzacja kluczy RSA – wg. Bernstein, Heringer, Lange 5. Kryptografia krzywych eliptycznych 6. Kryptografia post-kwantowa, 7. Pakiety sieciowe Ethernet jako źródło sygnału losowego 8. Pasywna identyfikacja systemów operacyjnych na podstawie własności pakietów sieciowych
METODY I KRYTERIA OCENIANIA ORAZ FORMA ZALICZENIA ZAJĘĆ
Zajęcia składają się z 8 jednostek dydaktycznych. Każda z nich składa się z godzinnego wprowadzenia oraz godziny na konsultacje, dyskusje projektowe w zespole, przy wsparciu prowadzącego i omówienie wyników poprzednich zajęć. Każda z jednostek może być realizowana na trzech poziomach: 3,4 i 5 – w praktyce student wybiera sobie ocenę.

JĘZYK WYKŁADOWY PRZEDMIOTU	PUNKTY ECTS
polski	3

FORMA PROWADZONYCH ZAJĘĆ	WYMIAR GODZIN	PROWADZĄCY
Zajęcia zintegrowane (ZIN)	30	Teodor Buchner, dr hab. inż.