Szkoła Doktorska nr 3
Politechnika Warszawska

Karta przedmiotu oferowanego w Szkole Doktorskiej nr 3

– semestr letni 2020/2021

1. TYTUŁ
[PL] **Entropia dla inżynierów** [ENG] **Entropy for engineers**
2. JĘZYK WYKŁADOWY PRZEDMIOTU ORAZ PUNKTY ECTS:
polski, 3 ECTS
3. WYMIAR GODZIN, FORMA PROWADZONYCH ZAJĘĆ:
15, Wykład (WYK), Zajęcia komputerowe (ZKO)
4. DANE WYKŁADOWCY
dr hab. inż. Teodor Buchner
5. DYSCYPLINA NAUKOWA
Nauki fizyczne
6. JEDNOSTKA PROWADZĄCA
Szkoła doktorska nr 3
7. JEDNOSTKA REALIZUJĄCA
105000 - Wydział Fizyki
8. TYP PRZEDMIOTU:
Obieralny
9. SPOSÓB WERYFIKACJI EFEKTÓW UCZENIA SIĘ:
Zaliczenie

10. OPIS SKRÓCONY PRZEDMIOTU:

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.

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

11. OPIS PRZEDMIOTU:

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.

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

12. LITERATURA

-

13. EFEKTY UCZENIA SIĘ:

Szkoła Doktorska nr 3
Politechnika Warszawska

-