KARTA PRZEDMIOTU / COURSE DESCRIPTION

Nazwa przedmiotu w języku polskim / Course name in Polish
Entropia dla inżynierów
Nazwa przedmiotu w języku angielskim / Course name in English
Entropy for engineers
Dyscyplina / Scientific discipline
Nauki fizyczne
Opis skrócony / Short description
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
Opis / Description
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
Język / Language
Polski/ Polish

ECTS	3	**Prowadzący/ Lecturer**	dr hab. inż Teodor Buchner

Forma zaliczenia / Examination	Zaliczenie/ Credit
Wykład / Lecture	15
Zajęcia komputerowe/ Computer classes	15