KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Podstawy kryptografii

Przedmiot

Kierunek studiów
Elektronika i Telekomunikacja

Rok/semestr
IV/VII

Studia w zakresie (specjalność)

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
30	0	
Ćwiczenia	Projekty/seminaria	
15	0	

Liczba punktów ECTS

3

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Mieczysław Jessa

mieczyslaw.jessa@put.poznan.pl

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać usystematyzowaną wiedzę z zakresu algebry, rachunku prawdopodobieństwa, działania sieci komputerowych przewodowych i bezprzewodowych oraz sieci mobilnych 2G, 3G i 4G. Powinien również posiadać umiejętność pozyskiwania informacji z literatury, baz danych oraz innych źródeł w języku polskim lub angielskim.

Cel przedmiotu

Przekazanie studentom podstawowej wiedzy na temat kryptografii. Wytworzenie u studentów umiejętności oceny jakości zabezpieczeń kryptograficznych.

Przedmiotowe efekty uczenia się

Wiedza

1. Posiada wiedzę dotyczącą podstawowych metod kryptograficznej ochrony informacji gromadzonej i przesyłanej w sieciach telekomunikacyjnych i komputerowych.

2. Zna pojęcia charakteryzujące sieci telekomunikacyjne i komputerowe oraz rozumie techniczne znaczenie tych pojęć.

Umiejętności

1. Potrafi integrować uzyskane informacje, dokonywać ich interpretacji, wyciągać wnioski i uzasadniać opinie.

Kompetencje społeczne

1. Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się.

2. Ma poczucie odpowiedzialności za zaprojektowane systemy elektroniczne i telekomunikacyjne i zdaje sobie sprawę z potencjalnych niebezpieczeństw dla innych ludzi lub społeczeństwa ich nieodpowiedniego wykorzystania.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana na podstawie pisemnego zaliczenia, składającego się z 5 pytań otwartych, identycznie punktowanych. Próg zaliczeniowy wynosi 50% punktów. Rozkład progów dla ocen od 2 do 5 jest równomierny. Zestaw pytań jest losowany indywidualnie ze zbioru zagadnień. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania otwarte, przesyłane są studentom drogą mailową z wykorzytaniem uczelnianej poczty elektronicznej.

Wiedza i umiejętności nabyte w czasie ćwiczeń rachunkowych są weryfikowane na podstawie pisemnego zaliczenia, składajcego się z 5 zadań rachunkowych. Próg zaliczeniowy wynosi 50%. Rozkład progów dla ocen od 2 do 5 jest równomierny.

Treści programowe

W ramach wykładu studenci poznają podstawowe pojęcia kryptografii takie jak: poufnośc, integralność, uwierzytelnianie, autoryzacja, niezaprzeczalność, dostępność, funkcja jednokierunkowa, funkcja jednokierunkowa z zapadką, system kryptograficzny (symetryczny, asymetryczny, z kluczem tajnym, z kluczem publicznym), bezpieczeństwo bezwarunkowe, obliczeniowe, udowadnialne, postulat Kerckhoffsa, liczby losowe, bezpieczne liczby pseudolosowe, funkcja skrótu, podpis elektroniczny, podpis cyfrowy, certyfikat. Omawiane są matematyczne podstawy kryptografii: kongruencje, algorytm Euklidesa, Tw. Fermata, Eulera, odwrotność liczby w arytmetyce modulo, rozszerzony algorytm Euklidesa, Chińskie twierdzenie o resztach, rozwiązywanie układów równań, potęgowanie modularne, reszty kwadratowe, pierwiastki kwadratowe modulo. Przedstawiane są konstrukcje szyfrów blokowych oraz tryby użycia szyfrów blokowych (ECB, CBC, CFB, OFB), szyfry strumieniowe, właściwości i ograniczenia stosowania szyfrów blokowych i strumieniowych, wybrane metody szyfrowania (szyfry jednoalfabetowe, wieloalfabetowe, transpozycyjne, wieloznakowe, szyfr Vigenere'a, Enigma, DES, IDEA, AES), wybrane metody szyfrowania z kluczem publicznym (szyfr ElGamala, RSA, szyfr Rabina). Omawiana jest kryptograficzna funkcja skrótu, funkcje silnie i słabo bezkonfliktowe, przykłady funkcji skrótu (MD5, SHA-1, SHA-2, SHA-3), metody podpisu cyfrowego, PKI oraz metody uwierzytelniania (hasła, osobiste numery identyfikacyjne PIN, protokoły challenge-response z kluczem tajnym, z kluczem publicznym, kryptograficzne sumy kontrolne, podpisy cyfrowe, dowody z wiedzą zerową). Wykład uzupełniają przykłady użycia metod kryptograficznych w telekomunikacji (GSM, UMTS, 4G, SSL/TLS, SSH). W ramach ćwiczeń rozwiązywane są zadania ilustrujące użycie algorytmu Euklidesa, Tw. Fermata, Tw. Eulera,

metod obliczania odwrotności liczby w arytmetyce modulo, rozszerzonego algorytmu Euklidesa, Chińskiego twierdzenie o resztach, reszt kwadratowych, pierwiastków kwadratowych modulo oraz metod square-and-multiply w rozwiązywaniu problemów kryptograficznych.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.

2. Ćwiczenia: klasyczna problemowa

Literatura

Podstawowa

1. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone „Kryptografia stosowana”, WNT, Warszawa 2005.

2. B. Schneier „Kryptografia dla praktyków”, WNT, Warszawa, 2002.

3. W. Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”, Wyd. V, Helion 2012.

Uzupełniająca

1. J. A. Buchmann „Wprowadzenie do kryptografii”, PWN, 2006.

2. M. Karbowski, Podstawy kryptografii, Helion, 2014.

3. M. Kutyłowski, W-B. Strothmann „Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych”, Read Me, Warszawa, 1999.

4. N. Ferguson, B. Schneier „Kryptografia w praktyce”, Helion, 2004.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	90	3,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	55	2,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)[1]	35	1,0

[1] niepotrzebne skreślić lub dopisać inne czynności