KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Zaawansowane systemy szyfrowania

Przedmiot

Kierunek studiów
Teleinformatyka

Rok/semestr
1/1

Studia w zakresie (specjalność)

Profil studiów
ogólnoakademicki

Poziom studiów
drugi

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obowiązkowy

Liczba godzin

Wykład
15

Laboratoria
15

Inne (np. online)

Ćwiczenia
15

Projekty/seminaria
0/0

Liczba punktów ECTS

3

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr hab. inż. Mieczysław Jessa, prof. PP
Instytut Telekomunikacji Multimedialnej
Tel.: +48 61 665 3854, email:
mieczyslaw.jessa@put.poznan.pl

Odpowiedzialny za przedmiot/wykładowca:

mgr. Paweł Kubczak, ITM, 61 665 3859
pawel.kubczak@put.poznan.pl

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową usystematyzowaną wiedzę na temat działania sieci teleinformatycznych. Powinien znać podstawowe zagrożenia bezpieczeństwa dla

danych przesyłanych, przetwarzanych i gromadzonych w sieciach teleinformatycznych. Powinien znać podstawowe pojęcia kryptografii oraz rozumieć znaczenie standardów międzynarodowych dla zapewnienia bezpieczeństwa w teleinformatyce. Powinien również posiadać umiejętność pozyskiwania informacji z literatury, baz danych oraz innych źródeł w języku polskim lub angielskim.

Cel przedmiotu

Celem nauczania przedmiotu jest zapoznanie studentów z podstawami matematycznymi kryptografii oraz wykształcenie umiejętności posługiwania się metodami matematycznymi na etapie tworzenia, analizy, używania zaawansowanych metod szyfrowania oraz pogłębienie wiedzy na temat systemów szyfrowania wykorzystywanych w teleinformatyce.

Przedmiotowe efekty uczenia się

Wiedza

1. Ma poszerzoną wiedzę z zakresu teorii liczb, teorii prawdopodobieństwa i statystyki matematycznej niezbędną do opisu i oceny jakości działania szyfrów blokowych oraz szyfrów strumieniowych wykorzystywanych w teleinformatyce.
2. Zna zaawansowane metody szyfrowania oraz sposoby ich wykorzystania dla ochrony informacji przesyłanej i przechowywanej w systemach teleinformatycznych.
3. Rozumie znaczenie kryptografii dla zapewnienia bezpieczeństwa danych przesyłanych w sieciach teleinformatycznych i gromadzonych w bazach danych.

Umiejętności

1. Potrafi przewidzieć skutki braku zabezpieczeń kryptograficznych urządzeń i sieci dla bezpieczeństwa danych przesyłanych i gromadzonych w systemie teleinformatycznym.
2. Umie pracować w grupie nad rozwiązaniem problemu ochrony danych i sieci teleinformatycznej przed nieuprawnionym dostępem lub modyfikacją.

Kompetencje społeczne

1. Jest gotów do pozyskania nowej wiedzy niezbędnej dla zapewnienia bezpieczeństwa systemom teleinformatycznym metodami kryptograficznymi.
2. Ma poczucie odpowiedzialności za bezpieczeństwo zaprojektowanych systemów teleinformatycznych i zdaje sobie sprawę z potencjalnych niebezpieczeństw dla innych ludzi lub społeczeństwa ich nieodpowiedniego zabezpieczenia.

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 wykorzystaniem uczelnianej poczty elektronicznej.

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

Treści programowe

W ramach zajęć studenci poznają podstawy matematyczne kryptografii, zasady budowy szyfrów blokowych, przykłady szyfrów blokowych używanych współcześnie, zasady budowy szyfrów strumieniowych, metody wytwarzania ciągów rzeczywiście losowych, bezpiecznych ciągów pseudolosowych, metody oceny jakości ciągów bitów używanych w kryptografii za pomocą testów statystycznych i restartów, przykłady bezpiecznych generatorów liczb pseudolosowych oraz szyfrów strumieniowych. Studenci poznają metody podpisu cyfrowego, zasady tworzenia infrastruktury klucza publicznego (PKI), podstawy kryptografii post-kwantowej oraz podstawowe scenariusze ataku na system kryptograficzny w podziale na metody ogólne i specjalizowane.

W ramach wykładu studenci poznają podstawy matematyczne kryptografii tj. grupy, grupy multiplikatywne, generator grupy, pierścienie, ciała, kongruencje, testowanie pierwszości liczb, faktoryzacja, wielomiany o współczynnikach w ciele skończonym, algorytm Euklidesa, funkcja Eulera, Małe Twierdzenie Fermata, Twierdzenie Eulera, Chińskie twierdzenie o resztach, Tożsamość Bezout, odwrotność liczby w arytmetyce modularnej, rozszerzony algorytm Euklidesa, potęgowanie liczb całkowitych w arytmetyce modulo n, logarytm dyskretny, reszty kwadratowe, pierwiastki kwadratowe, właściwości operacji XOR, zasady budowy szyfrów blokowych, szyfry blokowe używane współcześnie, m.in. 2DES, 3DES, AES, BLOWFISH, SERPENT, CAST, RC5, RC6. Omawiane są właściwości szyfrów strumieniowych, metody wytwarzania ciągów rzeczywiście losowych, bezpiecznych ciągów pseudolosowych, metody oceny jakości ciągów bitów używanych w kryptografii za pomocą testów statystycznych i restartów, przykłady bezpiecznych generatorów liczb pseudolosowych oraz szyfrów strumieniowych: BBS, RC4, ANSI X9.17, FIPS 186 itp. Studenci poznają metody podpisu cyfrowego, zasady tworzenia infrastruktury klucza publicznego (PKI), podstawy kryptografii post-kwantowej oraz podstawowe scenariusze ataku na system kryptograficzny w podziale na metody ogólne i specjalizowane.
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 twierdzenia o resztach, reszt kwadratowych, metod square-and-multiply oraz wykorzystanie poznanych twierdzeń w projektowaniu algorytmu RSA.
Laboratorium obejmuje przykłady szyfrowanie za pomocą szyfru symetrycznego blokowego, wytwarzanie ciągu rzeczywiście losowego, wytwarzanie bezpiecznego ciągu pseudolosowego, przykłady szyfrowania za pomocą szyfru symetrycznego strumieniowego oraz przykłady szyfrowania za pomocą szyfru asymetrycznego.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.
2. Ćwiczenia: klasyczna problemowa.
3. Laboratorium: 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. Hoffstein, J. Pipher, J. H. Silverman „An Introduction to Mathematical Cryptography, Springer, 2008."
2. J. A. Buchmann „Wprowadzenie do kryptografii”, PWN, 2006.
3. M. Karbowski, Podstawy kryptografii, Helion, 2014.
4. M. Kutyłowski, W-B. Strothmann „Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych”, Read Me, Warszawa, 1999.
5. N. Ferguson, B. Schneier „Kryptografia w praktyce”, Helion, 2004.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	86	3.0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2.0
Praca własna studenta (przygotowanie do zaliczenia, przygotowanie do ćwiczeń, przygotowanie do laboratorium, studia literaturowe)	41	1.0