KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Systemy szyfrowania i certyfikacji [S2Teleinf2>SSiC]

Przedmiot

Kierunek studiów
Teleinformatyka

Rok/Semestr
1/1

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
14

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

prof. dr hab. inż. Mieczysław Jessa
mieczyslaw.jessa@put.poznan.pl

Wykładowcy

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 i angielskim.

Cel przedmiotu

Celem nauczania przedmiotu jest zapoznanie studentów z podstawami matematycznymi kryptografii, metodami szyfrowania i certyfikacji wiadomości oraz wykształcenie umiejętności posługiwania się metodami matematycznymi na etapie tworzenia, analizy i używania metod szyfrowania i certyfikatów.

Przedmiotowe efekty uczenia się

Wiedza:
Ma poszerzoną i pogłębioną wiedzę w zakresie niektórych działów matematyki, obejmującą elementy analizy matematycznej, procesy stochastyczne, metody optymalizacji oraz metody numeryczne

[K2_W01], [K2_W11].
Ma pogłębioną wiedzę w zakresie przetwarzania i bezpieczeństwa informacji w systemach teleinformatycznych [K2_W08], [K2_W10].

Umiejętności:
Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie [K2_U01], [K2_U15], [K2_U17].
Potrafi wykorzystać poznane metody i modele matematyczne, w razie potrzeby odpowiednio je modyfikując, do realizacji projektów w obszarze teleinformatyki [K2_U06], [K2_U14].
Potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia [K2_U11], [K2_U16].

Kompetencje społeczne:
Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz do krytycznej oceny odbieranych treści [K2_K01].
Jest gotów do wypełniania zobowiązań społecznych [K2_K02].

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. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania otwarte, przesyłane są studentom drogą elektroniczną.
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 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 modularnej, logarytm dyskretny, reszty kwadratowe, pierwiastki kwadratowe, właściwości operacji XOR, zasady budowy szyfrów blokowych, szyfry blokowe używane współcześnie, m.in. 3DES, AES, BLOWFISH, SERPENT, CAST, RC5, RC6. Omawiane są właściwości szyfrów strumieniowych, metody wytwarzania 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 certyfikacji i tworzenia infrastruktury klucza publicznego (PKI), podstawy kryptografii post-kwantowej (PQC) 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, metod square-and-multiply oraz wykorzystanie poznanych twierdzeń w projektowaniu algorytmu RSA dla celów szyfrowania i uwierzytelniania danych.
Laboratorium obejmuje przykłady szyfrowania za pomocą szyfrów blokowych oraz szyfrów strumieniowych, w którym bezpieczne ciągi pseudolosowe są wytwarzane w oparciu o szyfry blokowe pracujące w trybie OFB i CTR, realizację przykładowych podpisów cyfrowych metodami tradycyjnymi oraz za pomocą PQC.

Tematyka zajęć

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 modularnej, logarytm dyskretny, reszty kwadratowe, pierwiastki kwadratowe, właściwości operacji XOR, zasady budowy szyfrów blokowych, szyfry blokowe używane współcześnie, m.in. 3DES, AES, BLOWFISH, SERPENT, CAST, RC5, RC6. Omawiane są właściwości szyfrów strumieniowych, metody wytwarzania 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 certyfikacji i tworzenia infrastruktury klucza publicznego (PKI), podstawy kryptografii post-kwantowej (PQC) 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, metod square-and-multiply oraz wykorzystanie poznanych twierdzeń w projektowaniu algorytmu RSA dla celów szyfrowania i uwierzytelniania danych.
Laboratorium obejmuje przykłady szyfrowania za pomocą szyfrów blokowych oraz szyfrów strumieniowych, w którym bezpieczne ciągi pseudolosowe są wytwarzane w oparciu o szyfry blokowe pracujące w trybie OFB i CTR, realizację przykładowych podpisów cyfrowych metodami tradycyjnymi oraz za pomocą PQC.

Metody dydaktyczne

Wykład: połączenie wykładu tradycyjnego z wykładem problemowym.
Ćwiczenia: klasyczna problemowa.
Laboratorium: połączenie metody klasycznej z działaniami grupowymi.

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	78	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	40	1,50