Opis przedmiotu		
Kod przedmiotu	ABDZ	
Nazwa przedmiotu	Algorytmy i bezpieczeństwo danych	
Wersja przedmiotu	2	
A. Usytuowanie przedmiotu w systemie studiów		
Poziom kształcenia	Studia I stopnia	
Forma i tryb prowadzenia studiów	Niestacjonarne zaoczne	
Kierunek studiów	Elektronika i Telekomunikacja	
Profil studiów	Profil ogólnoakademicki	
Specjalność	-	
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych	
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych	
Koordynator przedmiotu	prof. nzw. dr hab. Tomasz Adamski	
B. Ogólna charakterystyka przedmiotu		
Blok przedmiotów	Inżynieria Komputerowa	
Grupa przedmiotów	Przedmioty specjalności	
Status przedmiotu	Obowiązkowy	
Język prowadzenia zajęć	Polski	
Semestr nominalny	7	
Usytuowanie realizacji w roku akademickim	Semestr letni	
Wymagania wstępne	Matematyka (z elementarnym wstępem do algebry)	
Limit liczby studentów	-	
C. Efekty kształcenia i sposób prowadzenia zajęć		
Cel przedmiotu	1. Poznanie podstawowych algorytmów komputerowych (chodzi głównie o wybrane algorytmy nienumeryczne takie jak wyszukiwanie wzorca oraz algorytmy teorioliczbowe takie jak algorytm Montgomery'ego czy Baretta stosowane w kryptografii). 2. Poznanie zasad projektowania, analizy i oceny algorytmów a w szczególności ocenę złożoności obliczeniowej algorytmów 3. Poznanie podstaw teoretycznych kryptografii i ochrony danych 4. Poznanie najważniejszych algorytmów, protokołów i metod stosowanych w systemach komputerowych i sieciach komputerowych do ochrony danych	
Efekty kształcenia	Patrz tabela 42.	
Formy zajęć i ich wymiar	Wykład	2

	Ćwiczenia	1
	Laboratorium	0
	Projekt	1
Treści kształcenia	Część 1 – Algorytmy komputerowe 1. Wprowadzenie a. Algorytm, analiza i projektowanie algorytmów b. Złożoność obliczeniowa algorytmu – podstawowe pojęcia c. Sposoby opisu algorytmów – język publikacyjny d. Zapisy asymptotyczne e. Elementarne struktury danych f. Rekurencja i metody projektowania algorytmów g. Równania rekurencyjne h. Algorytmy probabilistyczne 2. Złożoność obliczeniowa i NP zupełność a. Teoria złożoności obliczeniowej b. Problemy (problemy obliczeniowe) i problemy decyzyjne c. Algorytmy z czasem wielomianowym d. Redukowalność i problemy NP –zupełne oraz przykłady problemów NP-zupełnych e. Klasy złożoności algorytmów probabilistycznych 3. Algorytmy sortowania a. Problem sortowania b. Sortowanie bąbelkowe (bubblesort) c. Zmodyfikowane sortowanie bąbelkowe (modified bubblesort) d. Insertionsort – sortowanie przez wstawianie e. Sortowanie przez selekcję (selectionsort) f. Algorytm sortowania „mergesort" (algorytm sortowania przez scalanie) g. Algorytmy sortowania w czasie liniowym h. Sortowanie przez zliczanie – countsort i. Sortowanie pozycyjne – algorytm radixsort j. Sortowanie kubełkowe - algorytm bucketsort k. Sortowanie przez kopcowanie (ang. heapsort) l. Sortowanie szybkie – quicksort m. Szybkie algorytmy wyznaczania k-tego elementu co do wartości w ciągu. n. Sortowanie zewnętrzne o. Sieci sortujące 4. Algorytmy tekstowe a. Problem wyszukiwania wzorca b. Algorytm naiwny wyszukiwania wzorca c. Algorytm automatowy d. Algorytm Rabina-Karpa e. Algorytm KMP 5. Algorytmy teorioliczbowe a. Rozszerzony binarny algorytm Euklidesa b. Szybkie algorytmy podnoszenia do potęgi modulo n c. Algorytmy obliczania pierwiastka kwadratowego mod n d.Algorytm Montgomery'ego e.Algorytm Barretta f. Algorytmy testowania pierwszości Część 2 – Algorytmy i bezpieczeństwo danych 1. Kryptografia - pojęcia podstawowe a. Cele i środki kryptografii b. System kryptograficzny c. Rodzaje szyfrów (szyfry z kluczem publicznym i z kluczem prywatnym, szyfry blokowe) d. Szyfry klasyczne (szyfry podstawieniowe monoalfabetowe i polialfabetowe, szyfry przedstawieniowe, szyfry idealne) 2. Podstawy matematyczne kryptografii a. Grupy i logarytmy dyskretne b. Pierścienie i ciała c. Podzielność, kongruencje i chińskie twierdzenie o resztach, twierdzenie Eulera d. Liczby pierwsze i testowanie pierwszości 3. Systemy kryptograficzne z kluczem publicznym a. Wprowadzenie b. System kryptograficzny RSA c. System kryptograficzny Rabina d. System kryptograficzny ElGamala e. Szyfry plecakowe f. System kryptograficzny Massey'a–Omury 4. Systemy kryptograficzne z kluczem prywatnym a.Szyfry Feistala b. DES (Data Encryption Standard) i rozszerzenia, modyfikacje DES'a (DESX, 3DES) c. Szyfr AES (Advanced Encryption Standard) d. Szyfry IDEA, Serpent, Camelia 5. Funkcje skrótu a. Podstawowe definicje (funkcja jednokierunkowa, funcje słabo i silnie bezkonfliktowe) b. Funkcja hashująca Chaum'a –van Heijst'a –Pfitzmanna c. Funkcja haszująca MD 5, Whirlpool, SHA-256, SHA -3 d. Schematy ogólne tworzenia funkcji skrótu e. Paradoks dnia urodzin i ataki na funkcje skrótu 6. Tryby wykorzystania szyfrów blokowych i szyfry strumieniowe a. Tryb szyfrowania ECB i CBC b. Tryb szyfrowania OFB c. Szyfry strumieniowe 7. Uwierzytelnianie dokumentu - podpisy cyfrowe a. Podpisy cyfrowe – uwagi wstępne, typy podpisów cyfrowych b. Algorytm podpisów cyfrowych RSA c. Algorytm podpisów cyfrowych ElGamala d. Algorytm podpisów cyfrowych DSS e. Algorytm podpisów Rueppela-Nyberga e. Algorytm podpisów ślepych 8. Uwierzytelnianie strony a. Metoda haseł, metoda haseł z soleniem b. Metoda pytanie odpowiedź (metoda challenge-response) c. Protokoły z wiedzą zerową (protokoły FiataShamira i Feige-Fiata Shamira) 9. Dystrybucja kluczy, protokoły wymiany klucza a. Protokół Diffiego-Hellmana b. Protokół szerokogębnej żaby c. ProtokólNeedhama-Schroedera	
Metody oceny	Przedmiot zaliczany jest w formie egzamin pisemnego (60p). Za rozwiązanie zadań i małych projektów do samodzielnego rozwiązania nazywanych TESTami można dodatkowo zdobyć 40p (to dużo). Rozwiązywanie TESTów nie jest obowiązkowe ale bardzo zalecane. W sumie są 4 serie TESTów po 10p. Ostatecznie można zdobyć 100p. Próg zaliczenia to 50p. Przeliczenie punkty ocena jest liniowe: 50p - próg	

	zaliczenia 50-59 ocena 3 60-69 ocena 31/2 70-79 ocena 4 80-89 ocena 41/2 90-100 ocena 5
Metody sprawdzania efektów kształcenia	Patrz tabela 42.
Egzamin	Tak
Literatura	Część 1 – Algorytmy • T.Adamski, J.Ogrodzki; Wprowadzenie do algorytmów komputerowych i struktur danych; Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2014 • T.Adamski; Zbiór zadań z kryptografii i ochrony informacji; Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2014 • D.E.Knuth; Sztuka programowania; WNT, Warszawa 2002 • T. H. Cormen, C.E. Leiserson, R.L. Rivest, C.Stein ; Wprowadzenie do algorytmów; WNT, Warszawa 2004 • R. Neapolitan i K.Naimpour; Podstawy algorytmów z przykładami w C++; Hellion 2004 • A.Aho, J.Hopcroft, J.Ullman; Projektowanie i analiza algorytmów komputerowych; Hellion, 2004 • L.Banachowski, K.Diks, W.Rytter; Algorytmy i struktury danych;WNT, Warszawa 1996 • E.Reingold, J.Nievergelt,N.Deo; Algorytmy kombinatoryczne; PWN, Warszawa 1985 • P.Wróblewski; Algorytmy, struktury danych i techniki programowania; Helion, Warszawa 1996 Część 2 – Algorytmy i bezpieczeństwo danych • J.Buchmann; Wprowadzenie do kryptografii; PWN, 2006 • A. Menezes, P. Oorschot, S. Vanstone; Handbook of Applied Cryptography; CRC Press Inc., 1997. (treść książki jest zamieszczona na stronie www: http://cacr.math.uwaterloo.ca/hac. Istnieje również tłumaczenie polskie wydane przez WNT • M.Kutyłowski; W.Strothmann; Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych; Wyd.2, Oficyna Wydawnicza Read Me;1999 • N.Koblitz; Wykład z teorii liczb i kryptografii; WNT, Warszawa 1995 • N.Koblitz; Algebraiczne aspekty kryptografii; WNT, Warszawa 2000 • B.Schneier; Kryptografia dla praktyków; Wiley & WNT, Warszawa 2004 • J. Stokłosa, T.Bilski, T.Pankowski; Kryptograficzna ochrona danych w systemach komputerowych; PWN. Poznań 2004 • W.Stallings; Ochrona danych w sieci i intersieci; WNT, 1998
Witryna www przedmiotu	https://red.okno.pw.edu.pl/witryna/home.php dostęp dla zalogowanych studentów
D. Nakład pracy studenta	
Liczba punktów ECTS	6
Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia	30g -wykład + 30g praca własna w domu 15g -ćwiczenia + 15g praca w domu 15g - projekt + 15g praca w domu Praca samodzielna studenta (praca w domu i w bibliotece uzupełniona kontaktami z prowadzącym przedmiot przez Internet) jest głównym sposobem opanowywania materiału przez słuchacza wykładu. Bardzo istotnym elementem wykładu jest duża ilość zadań i miniprojektów do samodzielnego rozwiązania. Miniprojekty mogą zostać rozszerzone do tzw. Projektu Zespołowego a ten z kolei do pracy dyplomowej. Sumaryczna liczba godzin pracy studenta: 120
Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:	3
Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	3
E. Informacje dodatkowe	
Uwagi	Przedmiot ma charakter podstawowy. Nacisk kładziony jest więc na zrozumienie stosowanych technik matematycznych, algorytmów i metod.
Data ostatniej aktualizacji	31.01.2015

Tabela 42. Efekty przedmiotowe	
Profil ogólnoakademicki – wiedza	
Efekt:	Student ma poszerzoną i pogłębioną wiedzę z matematyki (teoria algorytmów, teoria liczb, algebra, teoria prawdopodobieństwa) umożliwiającą zrozumienie zasady działania i projektowanie bezpiecznych systemów informatycznych i elektronicznych. Zna algorytmy, metody i techniki służące do zapewnienia bezpieczeństwa w procesie magazynowania i transmisji informacji.
Kod:	K_W01
Weryfikacja:	egzamin, ocena zadań domowych, ocena projektów, ocena poziomu wiedzy przy bezpośrednim kontakcie ze studentem na konsultacjach
Powiązane efekty kierunkowe	K_W01
Powiązane efekty obszarowe	T1A_W01, T1A_W02, T1A_W03, T1A_W07
Efekt:	Student ma podbudowaną teoretycznie wiedzę z zakresu algorytmów kryptograficznych oraz realizacji software'owej i hardware'owej systemów kryptograficznych w tym systemów kryptografii kwantowej
Kod:	K_W04
Weryfikacja:	egzamin, zadania domowe, projekty, bezpośredni kontakt ze studentem na konsultacjach
Powiązane efekty kierunkowe	K_W04
Powiązane efekty obszarowe	T1A_W04, T1A_W07
Profil ogólnoakademicki – umiejętności	
Efekt:	Student potrafi wyszukiwać informacje i dokonywać niezbędnych syntez
Kod:	K_U01, KU04
Weryfikacja:	ocena zadań i projektów
Powiązane efekty kierunkowe	K_U01, K_U04
Powiązane efekty obszarowe	T1A_U01, T1A_U04
Profil ogólnoakademicki – kompetencje społeczne	
Efekt:	Student ma świadomość roli społecznej absolwenta dobrej uczelni technicznej.
Kod:	K_K02
Weryfikacja:	Weryfikacja tego efektu kształcenia jest dosyć trudna bo dotyczy postawy życiowej studenta.
Powiązane efekty kierunkowe	K_K02
Powiązane efekty obszarowe	T1A_K02