

KARTA OPISU MODUŁU KSZTAŁCENIA		
Nazwa modułu/przedmiotu Kryptografia		Kod 1010332411010331905
Kierunek studiów Informatyka	Profil kształcenia (ogólnoakademicki, praktyczny) (brak)	Rok / Semestr 1 / 1
Ścieżka obieralności/specjalność -	Przedmiot oferowany w języku: polski	Kurs (obligatoryjny/obieralny) obligatoryjny
Stopień studiów: II stopień	Forma studiów (stacjonarna/niestacjonarna) stacjonarna	
Godziny Wykłady: 2 Ćwiczenia: - Laboratoria: 1 Projekty/seminaria: -		Liczba punktów 5
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) (brak)		(ogólnouczelniany, z innego kierunku) (brak)
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki nauki techniczne		Podział ECTS (liczba i %) 5 100%

Odpowiedzialny za przedmiot / wykładowca:

dr hab. inż. Janusz Stokłosa, prof. nadzw.
email: janusz.stoklosa@put.poznan.pl
tel. +48 61 665 37 57
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	Wiedza:	Ma poszerzoną i pogłębioną wiedzę w zakresie wybranych zagadnień matematyki. Ma pogłębioną wiedzę w zakresie bezpieczeństwa danych.
2	Umiejętności:	Potrąfi zaproponować i uzasadnić ulepszenia istniejących rozwiązań informatycznych.
3	Kompetencje społeczne	Potrąfi myśleć i działać w sposób kreatywny i przedsiębiorczy.

Cel przedmiotu:

Celem jest nauczenie studentów zasad działania i projektowania algorytmów kryptograficznych.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Ma pogłębioną wiedzę w zakresie kryptografii i wstępna z kryptoanalizy. - [K_W11]

Umiejętności:

1. Potrafi - przy formułowaniu i rozwiązywaniu problemów informatycznych - integrować wiedzę z różnych dziedzin i dyscyplin naukowych. - [K_U07]

Kompetencje społeczne:

1. Potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy. - [K_K01]

Sposoby sprawdzenia efektów kształcenia

Wykład zaliczany jest na podstawie egzaminu pisemnego; kontynuacją egzaminu pisemnego może być egzamin ustny. Kryterium formalnym zdania egzaminu pisemnego jest uzyskanie więcej niż połowę maksymalnej liczby punktów zsumowanych za wszystkie uzyskane odpowiedzi.

Ćwiczenia laboratoryjne zalicza się na podstawie obecności, wykonanych ćwiczeń, jakości sprawozdań i sprawdzianu końcowego.

Treści programowe

<p>Wykłady obejmują: Szyfry blokowe (przykłady budowy szyfrów blokowych; permutacje, podstawienia, funkcje boolowskie; kryteria projektowania bloków podstawień). Generatory ciągów pseudolosowych (generatory ciągów; komponenty generatorów: LFSR, NFSR, FCSR; losowość ciągów; złożoność liniowa ciągów). Szyfry strumieniowe (szyfry synchroniczne i samosynchronizujące; przykłady). Szyfry wykładnicze (Rabina, El-Gamala, Pohlinga-Hellmana, plecakowy). Funkcje skrótu (dedykowane (SHA); zbudowane z wykorzystaniem arytmetyki modularnej; atak urodzinowy). Podpisy cyfrowe (DSA; El-Gamala; kryptografia na krzywych eliptycznych). Uwierzytelnianie (dowody z wiedzą zerową). Niezaprzeczalność. Zarządzanie materiałem kryptograficznym (protokół El-Gamala, współdzielenie sekretu model Lenstry-Verheula).</p> <p>Laboratoria obejmują: Kryptograficzne kryteria projektowania bloków podstawień ? testowanie S-bloków. Testy i generatory ciągów pseudolosowych. Protokoły podpisów cyfrowych. Zarządzanie materiałem kryptograficznym. Algorytmy steganograficzne.</p>		
<p>Literatura podstawowa:</p> <ol style="list-style-type: none"> 1. Wprowadzenie do kryptografii, Buchmann J. A., Wydawnictwo Naukowe PWN, Warszawa, 2006 2. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001 		
<p>Literatura uzupełniająca:</p> <ol style="list-style-type: none"> 1. Fundamentals of Computer Security, Pieprzyk J., Hardjono T., Seberry J., Springer, Berlin, 2003 2. Kryptografia dla praktyków, Schneier B., WNT, Warszawa, 2002 3. Kryptologia. Budowa i łamanie zabezpieczeń, Wobst R., Wydawnictwo RM, Warszawa, 2002 4. Kryptografia w praktyce, Ferguson N., Schneier B., Helion, Gliwice, 2004 5. Wybrane artykuły z Lecture Notes in Computer Science, Advances in Cryptology, Springer. 		
<p>Bilans nakładu pracy przeciętnego studenta</p>		
<p>Czynność</p>		<p>Czas (godz.)</p>
1. Wykłady		30
2. Bieżąca praca nad zagadnieniami przekazywanymi na wykładzie		15
3. Ćwiczenia laboratoryjne		15
4. Przygotowanie do laboratoriów		15
5. Przygotowanie do sprawdzianu		10
6. Przygotowanie sprawozdań z laboratorium		10
7. Przygotowanie do egzaminu		20
8. Udział w konsultacjach i egzaminie		10
<p>Obciążenie pracą studenta</p>		
<p>forma aktywności</p>	<p>godzin</p>	<p>ECTS</p>
Łączny nakład pracy	125	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	50	2
Zajęcia o charakterze praktycznym	50	2