KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu **Kryptoanaliza**		Kod **1010332431010337158**
Kierunek studiów **Informatyka**	Profil kształcenia (ogólnoakademicki, praktyczny) **ogólnoakademicki**	Rok / Semestr **2 / 3**
Ścieżka obieralności/specjalność **Bezpieczeństwo systemów informatycznych**	Przedmiot oferowany w języku: **polski**	Kurs (obligatoryjny/obieralny) **obligatoryjny**
Stopień studiów: **II stopień**	**Forma studiów** (stacjonarna/niestacjonarna) **stacjonarna**	
Godziny Wykłady: **1** Ćwiczenia: **-** Laboratoria: **1** Projekty/seminaria: **-**		Liczba punktów **3**
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) **inny**	(ogólnouczelniany, z innego kierunku) **ogólnouczelniany**	
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki **nauki techniczne**		**Podział ECTS (liczba i %)** **3 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Krzysztof Chmiel
email: krzysztof.chmiel@put.poznan.pl
tel. 61 665 35 31
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	K_W01: ma podstawową wiedzę w zakresie matematyki, obejmującą algebrę, analizę, logikę, probabilistykę oraz elementy matematyki dyskretnej i stosowanej. K_W04: ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie podstawowych algorytmów i ich analizy, technik projektowania algorytmów, abstrakcyjnych struktur danych i ich implementacji, problemów obliczeniowo trudnych.
2	**Umiejętności:**	K_U01: potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie. K_U06: posługuje się językiem angielskim w stopniu wystarczającym do porozumiewania się, a także czytania ze zrozumieniem opisów i instrukcji dotyczących urządzeń elektronicznych, narzędzi informatycznych, aplikacji i podobnych dokumentów.
3	**Kompetencje społeczne**	K_K02: ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje. K_K04: ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania.

Cel przedmiotu:

Poznanie metod różnicowej i liniowej analizy kryptograficznej oraz ich rozszerzeń, w zakresie generowania najlepszych charakterystyk i identyfikacji klucza algorytmu szyfrowania blokowego.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie ochrony danych i bezpieczeństwa systemów informatycznych. - [K_W13]

Umiejętności:

1. Potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania. - [K_U03]

2. Potrafi zastosować odpowiednie metody ochrony danych i zapewnić bezpieczeństwo systemu informatycznego. - [K_U17]

Kompetencje społeczne:

1. Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania. - [K_K04]

2. Ma świadomość ważności dokładnego wykonania projektu, zachowania standardów notacyjnych, przestrzegania poprawności językowej i terminowego oddania prac. - [K_K07]

Sposoby sprawdzenia efektów kształcenia

Wykład: egzamin pisemny.

Laboratorium: ocena realizowanych ćwiczeń i sporządzanych sprawozdań.

Treści programowe

Wykład: Różnicowa i liniowa aproksymacja szyfrów blokowych. Algorytmy obliczania tablic aproksymacji. Aproksymacja losowych S-bloków. Aproksymacja arytmetycznej sumy i różnicy. Ocena jakości szyfru blokowego. Pośrednia ocena algorytmu typu DES. Kryptoanaliza różnicowa algorytmu DES. Kryptoanaliza liniowa algorytmu DES. Kryptoanaliza różnicowo-liniowa. Rozszerzenia kryptoanalizy różnicowej. Rozszerzenia kryptoanalizy liniowej.

Laboratorium: Różnicowa kryptoanaliza bloków podstawień Si. Liniowa kryptoanaliza bloków podstawień Si. Różnicowa kryptoanaliza funkcji bazowej f. Liniowa kryptoanaliza funkcji bazowej f. Różnicowa kryptoanaliza algorytmów DES1 i DES2. Liniowa kryptoanaliza algorytmów DES1 i DES2. Różnicowa kryptoanaliza algorytmów DES3 i DES4. Liniowa kryptoanaliza algorytmów DES3 i DES4. Różnicowa kryptoanaliza algorytmów DES5 i DES6. Liniowa kryptoanaliza algorytmów DES5 i DES6.

Literatura podstawowa:

1. Ochrona danych i zabezpieczenia w systemach teleinformatycznych, J. Stokłosa (red.), Wydawnictwo Politechniki Poznańskiej, 1?214, Poznań, 2003, 2005.

2. Metody różnicowej i liniowej kryptoanalizy szyfrów blokowych, K. Chmiel, Rozprawa habilitacyjna Nr 443, Wydawnictwo Politechniki Poznańskiej, 1?212, Poznań, 2010.

Literatura uzupełniająca:

1. Ćwiczenie z kryptoanalizy różnicowej algorytmu DES. Program CWAR, K. Chmiel, Raport 498, IAII PP, 1?89, Poznań 2004.

2. Ćwiczenie z kryptoanalizy liniowej algorytmu DES. Program CWAL, K. Chmiel, Raport 499, IAII PP, 1?87, Poznań 2004.

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Wykłady	15
2. Laboratoria	15
3. Konsultacje i egzamin	20
4. Przygotowanie do ćwiczeń laboratoryjnych i wykonanie sprawozdań	15
5. Przygotowanie do sprawdzianów i egzaminu	10

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	75	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	50	2
Zajęcia o charakterze praktycznym	25	1