KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wybrane zagadnienia kryptograficzne [S1Inf1>WZK]

Przedmiot

Kierunek studiów
Informatyka

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
16

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać wiedzę w zakresie podstawowych algorytmów i ich analizy, systemów operacyjnych, sieci komputerowych i podstaw kryptografii. Powinien potrafić posługiwać się środowiskami programistycznymi i platformami do pisania, wykonywania i testowania programów. Powinien potrafić konstruować algorytmy i dokonywać analizy ich złożoności.

Cel przedmiotu

Przekazanie studentom wybranych zaawansowanych zagadnień kryptograficznych i wyrobienie umiejętności ich stosowania w praktyce.

Przedmiotowe efekty uczenia się

Wiedza:
Student/ka ma szczegółową wiedzę na temat:
- aktualnych problemów i rozwiązań kryptograficznych,
- projektowania i analizy szyfrów blokowych, funkcji skrótu i szyfrów asymetrycznych,
- zaawansowanych protokołów i algorytmów kryptograficznych jak obliczenia na krzywych eliptycznych, kryptowaluty, bezpieczne obliczenia wielostronne.

Umiejętności:
Student/ka potrafi:
- zaprojektować i zaimlementować system, z zastosowaniem odpowiednich metod kryptograficznych tak, aby zapewnić poufność, integralność i uwierzytelnianie przechowywanych i przetwarzanych w nim danych,
- dokonać analizy i oszacowania poziomu bezpieczeństwa zastosowanych mechanizmów kryptograficznych i oszacować, czy system jest podatny na znane ataki krytptograficzne,
- zaproponować, zaprojektować i zaimplementować alternatywne mechanizmy kryptograficzne zapewniające większy poziom bezpieczeństwa.

Kompetencje społeczne:
Student/ka rozumie, że:
- ważnym aspektem jest zastosowanie odpowiednich metod ochrony danych,
- równie ważna jast odpowiednia implementacja algorytmów kryptograficznych,
- konieczne jest aktualizowanie wiedzy na temat bezpiecznych parametrów stosowanych algorytmów, protokołów i narzędzi.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu weryfikowana jest podczas pisemnego 45-minutowego kolokwium, składającego się z 5 pytań. Próg zaliczeniowy: ponad 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, są przesyłane studentom pocztą elektroniczną na początku semestru.
Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco podczas zajęć (poprzez sprawdzenie wykonanego ćwiczenia laboratoryjnego).

Treści programowe

Wykład
1. Wprowadzenie - wyzwania współczesnej kryptografii, wprowadzenie do projektowania szyfrów blokowych i funkcji skrótu, generatorów liczb losowych.
2. Komponenty szyfrów blokowych i kryteria jakie muszą spełniać. Kryptoanaliza szyfrów.
3. Algorytmy na krzywych eliptycznych.
4. Obliczenia wielostronne, przykłady praktycznych zastosowań.
5.Uwierzytelnione szyfrowanie.
6.Kryptowaluty, smart kontrakty.
Laboratorium
1. Analiza wybranych bloków podstawień, bloków permutacji i algorytmów generowania kluczy.
2. Kryptoanaliza różnicowa.
3. Implementacja wybranego algorytmu na krzywej eliptycznej.
4. Analiza algorytmów uwierzytelnionego szyfrowania.
5. Implementacja wybranego problemu obliczeń dwustronnych.
6. Analiza bezpieczeństwa kryptowalut.

Metody dydaktyczne

Wykład prowadzony jest w sposób interaktywny (z formułowaniem pytań do studentów) przy użyciu prezentacji multimedialnych. Materiały udostępniane są studentom w wersji elektronicznej.
Ćwiczenia laboratoryjne - prezentacja problemu/ćwiczenia do zrealizowania na tablicy (z podstawowym poziomem trudności i rozszerzonym dla chętnych) oraz wykonaniem ćwiczenia w wybranym przez studenta języku programowania.

Literatura

Podstawowa
Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion 2003 (sygnatura w bibliotece PP: W 110215).
Menezes A. i inni, Kryptografia stosowana, WNT, 2005, (sygnatura w bibliotece PP: W 112188)
Uzupełniająca

Materiały udostępniane przez prowadzącego, co roku aktualizowane.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	28	1,00