KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Kryptografia i podstawy kryptoanalizy [S2Inf1E-CYB>KRYP]

Przedmiot

Kierunek studiów
Informatyka/Computing

Rok/Semestr
1/1

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
30

Laboratorium
30

Inne (np. online)
0

Ćwiczenia
15

Projekty/seminaria
0

Liczba punktów ECTS

6,00

Koordynatorzy

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

dr Joanna Weissenberg
joanna.weissenberg@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 algorytmów kryptograficznych. Powinien potrafić posługiwać się środowiskami programistycznymi i platformami do pisania, wykonywania i testowania programów. Powinien potrafić konstruować algorytmy i dokonywać analizy ich złożoności. Powinien posiadać umiejętności pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Przekazanie studentom wiedzy na temat zaawansowanych zasad działania algorytmów kryptograficznych i nauczenie ich projektowania. Zapoznanie studentów z metodami projektowania wybranych algorytmów i protokołów kryptograficznych, nauczenie metod analizy i oceny wybranych systemów kryptograficznych.

Przedmiotowe efekty uczenia się

Wiedza:
student/ka ma szczegółową wiedzę na temat:
- jakie kryteria powinien spełniać bezpieczny system informatyczny i jakie środki ochrony należy zastosować aby to osiągnąć,
- ma uporządkowaną i podbudowaną teoretycznie wiedzę ogólną związaną z kluczowymi zagadnieniami z zakresu kryptograficznych mechanizmów ochrony danych (szyfry symetryczne i asymetryczne, funkcje skrótu, podpisy cyfrowe), krzywych eliptycznych, protokołów uwierzytelniania, algorytmów zarządzania kluczami i dzielenia sekretu, protokołów zapewniających bezpieczeństwo w sieci i bezpieczeństwo poczty,
- ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień z zakresu projektowania i oceny szyfrów,
- ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach kryptografii

Umiejętności:
student/ka potrafi:
- przeanalizować i zaprojektować wybrane komponenty szyfrów, spełniające określone kryteria, odporne na kryptoanalizę
- zaprojektować i zaimplementować wybrane algorytmy kryptograficzne
- zaprojektować i zaimlementować system, z zastosowaniem odpowiednich metod kryptograficznych tak, aby zapewnić poufność, integralność i uwierzytelnianie przechowywanych i przetwarzanych w nim danych, przeanalizować wydajność zaimplementowanego systemu
- 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, aktualnych metod kryptograficznych,
- 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 godzinnego egzaminu, składającego się z 5 pytań. Próg zaliczeniowy: ponad 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, są dostępne w ramach systemu eKursy.
Umiejętności nabyte w ramach ćwiczeń i zajęć laboratoryjnych weryfikowane są na bieżąco podczas zajęć (poprzez sprawdzenie wykonanego zadania czy ćwiczenia laboratoryjnego) oraz przez jedno 30-minutowe kolokwium po 8 laboratorium z wiedzy, która była niezbędna do wykonania i zrozumienia ćwiczeń.

Treści programowe

Treści programowe:
Szyfry blokowe, AE, generatory ciągów pseudolosowych. Funkcje skrótu.
Kryptografia asymetryczna. Podpisy cyfrowe, zarządzanie materiałem kryptograficznym. Metody uwierzytelniania. Metody podziału sekretu. ECRSA, ECDH, ECDSA.

Tematyka zajęć

Tematyka wykładów
1. Szyfry blokowe - analiza podstawowych komponentów szyfrów blokowych i kryteriów projektowych, jakie muszą spełniać. Aktualne wykorzystywane tryby pracy szyfrów blokowych - szyfrowanie z uwierzytelnianiem.
2. Teoria chaosu i generatory ciągów pseudolosowych, rozszerzone testy losowości ciągów.
3. Funkcje skrótu - projektowanie funkcji skrótu, klasyfikacja funkcji ze względu na budowę, kryteria jakie muszą spełniać dobre funkcje skrótu, MAC, ataki na funkcje skrótu, zastosowania, struktura Sponge

- na przykładzie funkcji Keccak.
4. Kryptografia asymetryczna - analiza wybranych algorytmów i protokołów opartych o szyfry asymetryczne. Protokół OTR.
5. Podpisy cyfrowe, zarządzanie materiałem kryptograficznym.
6. Metody uwierzytelniania - protokoły wykorzystujące poznane mechanizmy kryptograficzne - symetryczne, asymetryczne i funkcje skrótu, przegląd aktualnych metod uwierzytelniania (proceduralne, bezhasłowe, przez portale społecznościowe,..), metody biometryczne.
7. Metody podziału sekretu - algorytm Shamira i jego modyfikacja z identyfikacją oszusta, wybrane metody steganograficzne.
8. Wykorzystanie krzywych eliptyczne w kryptografii - ECRSA, ECDH, ECDSA.

Cwiczenia:
W ramach ćwiczeń studenci poznają te zagadnienia matematyczne z algebry, matematyki dyskretnej, artytmetyki modularnej, które potrzebne są do projektowania i analizy algorytmów kryptograficznych.
Laboratorium
1. Analiza najważniejszego komponentu szyfrów blokowych i kryteriów jakie musi spełniać. Implementacja metod do analizy S-bloków: zbalansowania, lawinowości i nieliniowości .
2. Implementacja generatora ciągów losowych opartego na wybranym algorytmie z teorii chaosu, oraz testów sprawdzających losowość wygenerowanego ciągu.
3. Implementacja algorytmu Berlecampa-Massey"a.
4. Implementacja algorytmu podziału sekretu lub zarządzania materiałem kryptograficznym
5. Implementacja protokołu OTR.
6. Implementacja wybranego systemu kryptograficznego w zespołach.

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 tablicowe i 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 w ramach laboratorium.

Literatura

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

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	150	6,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	75	3,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	75	3,00