KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Podstawy Kryptografii

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	Laboratoria	Inne (np. online)
30	30	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Anna Grocholewska-Czuryło

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać wiedzę w zakresie podstawowych algorytmów i ich analizy, systemów operacyjnych i sieci komputerowych. 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 kryptograficznych metod ochrony danych w systemach informatycznych i wyrobienie umiejętności ich stosowania w praktyce.

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,

- kryptograficznych mechanizmów ochrony danych (szyfry, funkcje skrótu, podpisy cyfrowe, krzywe eliptyczne, blockchainy),

- protokołów uwierzytelniania, zarządzania kluczami i dzielenia sekretu, protokołów zapewniających bezpieczeństwo w sieci i bezpieczeństwo poczty.

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 godzinnego egzaminu, składającego się z 8 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) oraz przez jedno 30-minutowe kolokwium po 8 laboratorium z wiedzy, która była niezbędna do wykonania i zrozumienia ćwiczeń.

Treści programowe

Wykład

1. Wprowadzenie - definicja bezpieczeństwa systemu informatycznego, kryteriów jakie taki system musi spełniać, środków utrzymania bezpieczeństwa (fizyczne, techniczne, organizacyjne i prawne), polityka bezpieczeństwa, wstęp do rodzajów systemów kryptograficznych, zasada Kerckhoffsa, typy ataków kryptoanalitycznych

2. Szyfry blokowe - podstawienia, przestawienia, sieci podstawieniowo-przestawieniowe Shannona, algorytmy DES, AES - ich podstawowe komponenty, tryby pracy szyfrów blokowych, szyfry strumieniowe, generatory ciągów pseudolosowych (kongruencyjne, RSA, BBS, LFSR, NLFSR) i testy losowości ciągów.

3. Funkcje 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 - podstawy matematyczne, algorytmy RSA, DH, El-Gamala, Rabina, Plecakowy, protokoły wykorzystujące algorytm RSA - o wiedzy zerowej, ślepe podpisy cyfrowe, obliczenia wielostronne - problem milionerów.

5. Podpis cyfrowy i PKI (Infrastruktura klucza publicznego), protokoły LDAP i OCSP.

6. Metody uwierzytelniania - protokoły PAP, CHAP, EAP, protokoły wykorzystujące poznane mechanizmy kryptograficzne - symetryczne, asymetryczne i funkcje skrótu, przegląd aktualnych metod uwierzytelniania (proceduralne, bezhasłowe, przez portale społecznościowe,..).

7. Metody podziału sekretu - algorytm Shamira i jego modyfikacja z identyfikacją oszusta, kryptografia wizualna i steganografia.

8. Krzywe eliptyczne w kryptografii - ECRSA, ECDH, ECDSA.

9. Kryptoanaliza - metody kryptoanalizy szyfrów blokowych, strumieniowych, asymetrycznych i funkcji skrótu.

10. Technologia blockchain - budowa, bezpieczeństwo, przykładowe wykorzystania.

Laboratorium

1. Implementacja prostego szyfru wykorzystującego podstawienie lub przestawienie i przeprowadzenie kryptoanalizy szyfrów zaimplementowanych przez innych studentów.

2. Implementacja generatora ciągów losowych BBS, oraz 4 podstawowych testów sprawdzających losowość wygenerowanego ciągu.

3. Implementacja wybranego trybu pracy szyfrów blokowych, przy wykorzystaniu podstawowego trybu pracy ECB, ocena propagacji błędów w różnych trybach pracy.

4. Implementacja algorytmu RSA.

5. Implementacja algorytmu DH.

6. Przeprowadzenie analizy szybkości działania różnych dostępnych funkcji skrótu, analiza kryteriów jakie powinna spełniać dobra funkcja skrótu.

7. Implementacja metody steganograficznej osadzania wiadomości na najmniej znaczącym bicie obrazu.

8. Implementacja metody podziału sekretu Shamira.

9. Implementacja metody podziału sekretu kryptografii wizualnej.

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

Stokłosa J. (red.), Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej, Poznań, 2005 (sygnatura w bibliotece PP: W 104521).

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	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium na laboratorium, przygotowanie do egzaminu)[1]	40	2,0

[1] niepotrzebne skreślić lub dopisać inne czynności