Autor*: prof. dr hab. inż. Zbigniew Kotulski*

Bezpieczeństwo danych (BDAN)
Data Security

Poziom kształcenia: I stopień
Forma i tryb prowadzenia przedmiotu: stacjonarna
Kierunek studiów: Cyberbezpieczeństwo
Specjalność:
Grupa przedmiotów:
Poziom przedmiotu: podstawowy
Status przedmiotu: obowiązkowy
Język przedmiotu: polski
Semestr nominalny (tylko dla przedmiotów obowiązkowych): 2
Minimalny numer semestru: 2
Wymagania wstępne, zalecane przedmioty poprzedzające: WCYBER
Limit liczby studentów: 60

Powód zgłoszenia przedmiotu: program studiów na nowym kierunku Cyberbezpieczeństwo

Cel przedmiotu:

Celem przedmiotu jest zapoznanie studentów z problematyką bezpieczeństwa danych w czasie ich przechowywania i przesyłania, a także z pewnymi aspektami bezpieczeństwa danych przetwarzanych. Podstawą stosowanych metod bezpieczeństwa jest kryptografia, zatem zagadnienia z nią związane są linia przewodnią wykładu. Omawiane są podstawowe algorytmy kryptograficzne i ich zastosowania do budowy protokołów kryptograficznych i realizacji usług bezpieczeństwa. Przedstawiane treści są uzupełnione o inne metody stosowane w bezpieczeństwie danych (steganografia, bezpieczeństwo fizyczne i organizacyjne), jak również o aspekt społecznościowy cyberbezpieczeństwa.

Treść kształcenia:

WYKŁADY:

1. **Wstęp do ochrony danych (2 godz.)**
   Potrzeba i cel ochrony danych, zasady postępowania z danymi i nośnikami danych, przegląd metod ochrony w czasie przechowywania, przesyłania i przetwarzania danych; wprowadzenie do kryptografii z uwagami historycznymi, hasła i klucze;

2. **Kryptografia bezkluczowa i symetryczna, elementy kryptoanalizy (6 godz.)**
   Integralność danych i kryptograficznie bezpieczne funkcje skrótu, przykłady funkcji skrótu (SHA-1,2,3); szyfry symetryczne, szyfry blokowe i tryby pracy szyfrów blokowych, przykłady szyfrów blokowych (DES, AES); konstrukcje kryptograficzne z wykorzystaniem funkcji skrótu (MAC, hash trees) i szyfrów blokowych (Davies-Mayer).

Elementy kryptoanalizy szyfrów blokowych (klasyfikacja ataków, analiza liniowa i różnicowa).

3. **Steganografia i maskowanie danych (2 godz)**
   Steganografia i maskowanie w zbiorach danych, steganogrfia obrazu i dźwięku, steganografia w językach znaczników, przykłady wykorzystania steganografii i maskowania danych, wykrywanie steganografii i ochrona przed steganografią w danych;

4. **Uzgodnienie klucza i kryptografia asymetryczna (6 godz.)**
   Protokół Diffie-Hellmana, wersje protokołu uzgodnienia klucza, kryptografia asymetryczne: RSA, ElGamal, krzywe eliptyczne, podpisy cyfrowe z dodatkowymi możliwościami, proste zastosowania kryptografii asymetrycznej;

5. **Podpis elektroniczny (2 godz.)**
   Podpis elektroniczny według standardów i według ustawodawstwa, usługi realizowane z wykorzystaniem podpisu elektronicznego: znakowanie czasem, certyfikaty, niezaprzeczalność i zaprzeczalność;

6. **Prywatność danych (2 godz)**
   Uwarunkowania prawne i kontekst bezpieczeństwa. Rozwiązania kryptograficzne: anonimowość, odwoływalna anonimowość, pseudonimowość i wirtualna tożsamość. Zbieranie danych, gromadzenie danych przetworzonych, rozpowszechnianie danych, inwazje w zakresie prywatności i ich skutki, inżynieria społeczna i media społecznościowe;

7. **Dostęp do danych i protokoły kryptograficzne (4 godz.)**
   Uwierzytelnienie: kryptograficzne protokoły uwierzytelnienia, biometria, dowody z wiedza zerową; protokoły podziału sekretu, bezpieczne obliczenia rozproszone. Bezpieczny dostęp do danych, modele dostępu: DAC, MAC, RBAC, ABAC, itd.

8. **Kryptoanaliza i wykorzystanie obliczeń kwantowych (2 godz.)**
   Kryptoanaliza algorytmów asymetrycznych: metody faktoryzacji i obliczania logarytmu dyskretnego; algorytm Shora i jego kwantowa wersja, wykorzystanie obliczeń kwantowych w kryptografii;

9. **Kryptografia postkwantowa i nowe kierunki w kryptografii (2 godz.)**
   Wykorzystanie algorytmów symetrycznych do podpisu elektronicznego, kryptografia na kratach, kryptografia wielomianowa, metody szyfrowania obraz (układy chaotyczne, kryptografia DNA);

10. **Ochrona zasobów danych przechowywanych (2 godz.)**
    Bazy i repozytoria danych, chmury obliczeniowe; ochrona danych w systemach baz danych, statystyczne bazy danych, ochrona danych na stronach www i w urządzeniach mobilnych;

ĆWICZENIA:
–

LABORATORIA:
–

PROJEKT:

Projekt polega na zaprojektowaniu i oprogramowaniau bezpiecznej aplikacji przetwarzającej dane.
Projekt będzie obejmował: ustalenie tematu, zebranie i analizę literatury dotyczącej tematyki projektu, zaplanowanie własnego rozwiązania, implementację i testy rozwiązania, prezentację wyników w grupie projektowej;

W ramach projektu przewidziane są dwa zadania laboratoryjne:
1. Zapoznanie się z profesjonalnymi bibliotekami kryptograficznymi w podstawowych językach programowania (java, C++, python), ich uruchomienie i wykonanie podstawowych obliczeń matematycznych; prezentacja wyników na seminarium w grupie projektowej.

2. Zapoznanie się z narzędziami do testowania protokołów kryptograficznych, przeprowadzenie testów bezpieczeństwa wybranych protokołów; prezentacja wyników na seminarium w grupie projektowej.

ZAJĘCIA ZINTEGROWANE:
–

Treść kształcenia - streszczenie w jęz. angielskim:

The aim of the course is to present students the problems of data security during data storage and transmission, as well as with some aspects of the security of data processed. The basis for the security methods used is cryptography, therefore the issues related to it are the lecture's guiding line. The fundamental cryptographic algorithms and their applications to the construction of cryptographic protocols and the implementation of security services are discussed. Presented content is supplemented with other methods used in data security (steganography, physical and organizational security), as well as on the social aspect of cybersecurity.

Egzamin: tak

Literatura i oprogramowanie:

Literatura:
1. Książki z kryptografii z serii WN-T TAO.
2. Prezentacje do wykładów.
3. Aktualna literatura podawana na wykładzie.

Oprogramowanie:

1. Biblioteki kryptograficzne zrealizowane w ramach międzynarodowych projektów naukowych lub z publicznie dostępnych repozytoriów uczelnianych.
2. System do analizy bezpieczeństwa lub poprawności protokołów kryptograficznych, np. Avispa

Wymiar godzinowy zajęć:	W	C	L	P
	30	–	-	30

Przewidywane formy kształcenia i organizacja przedmiotu

Realizacja przedmiotu obejmuje następujące formy zajęć:

- wykład prowadzony w wymiarze 2 godz. tygodniowo,
- zajęcia projektowe; w ramach tych zajęć student (w zespole dwuosobowym) będzie wykonywał zadanie programistyczne z zakresu bezpieczeństwa danych;
- zajęcia w laboratorium realizowane w ramach projektu

Sprawdzanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych – ocenę sprawozdań i prezentacji z realizacji zadań;
- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocena prezentacji i raportu z realizacji zadania;
- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym oraz – w przypadkach wątpliwości co do oceny – na egzaminie ustnym,

Wymiar w jednostkach ECTS: 4 pkt.

Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):

1. *liczba godzin kontaktowych – **50 godz.**, w tym*
   - *obecność na wykładach: **30 godz.**,*
   - *obecność na zajęciach projektowych: **4 godz.**,*
   - *obecność na zajęciach laboratoryjnych (w ramach projektu): **8 godz.**,*
   - *udział w konsultacjach związanych z realizacją przedmiotu: **5 godz.***
   - *obecność na egzaminie: **3 godz.** (pomijamy ew. egzamin ustny)*

2. *praca własna studenta – **55 godz.**, w tym*
   - *analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów, realizacji projektu i przygotowań do zajęć w laboratorium (w ramach projektu): **20 godz.***
   - *realizacja projektu: **25 godz.**.*
   - *przygotowanie do egzaminu: **10 godz.***

Łączny nakład pracy studenta wynosi 105 godz., **co odpowiada 4 p**kt. **ECTS.**

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich: 2 pkt. ECTS, co odpowiada **50** godz. kontaktowym.

Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym: 2 pkt. ECTS (co odpowiada **52** godz. realizacji projektu i laboratorium)

Efekty kształcenia/uczenia się

efekty kształcenia/uczenia się student, który zaliczył przedmiot:	forma zajęć/ technika kształcenia	sposób weryfikacji (oceny)*
WIEDZA		
W1: ma wiedzę dotyczącą podstawowych pojęć z zakresu kryptografii	wykład + projekt + zajęcia w laboratorium	projekt, zajęcia w laboratorium, egzamin
W2: ma podstawową wiedzę o protokołach kryptograficznych	wykład + projekt + zajęcia w laboratorium	zajęcia w laboratorium, egzamin
W3: ma wiedzę z zakresu metod ochrony danych	wykład + projekt + zajęcia w laboratorium	projekt egzamin
W4: ma podstawową wiedzę z zakresu kryptoanalizy	wykład + zajęcia w laboratorium	zajęcia w laboratorium egzamin
W5: ma podstawową wiedzę z zakresu steganografii danych i steganalizy	wykład + zajęcia w laboratorium	zajęcia w laboratorium, egzamin
UMIEJĘTNOŚCI		
U1: potrafi prześledzić działanie algorytmu i protokołu kryptograficznego	wykład + zajęcia w laboratorium	projekt
U2: potrafi zaprogramować algorytm i protokół na podstawie dokumentacji	wykład + zajęcia w laboratorium	projekt
U3: potrafi zaprojektować bezpieczną usługę sieciową z przechowywaniem i przesyłaniem danych	wykład + zajęcia w laboratorium	projekt
U4: potrafi dobrać właściwe metody ochrony dla przechowywanych danych	wykład + zajęcia w laboratorium	projekt
U5: potrafi ocenić poprawność i stopień bezpieczeństwa protokołu kryptograficznego	projekt + zajęcia w laboratorium	zajęcia w laboratorium
U6: potrafi zaprojektować i zrealizować proste zadanie inżynierskie z zakresu bezpieczeństwa danych i sporządzić dokumentacje prac	projekt + zajęcia w laboratorium	projekt + zajęcia w laboratorium
KOMPETENCJE SPOŁECZNE		
KS1: widzi konieczność korzystania z aktualnej literatury w zakresie bezpieczeństwa danych (publikacje naukowe, standardy)	wykład + projekt + zajęcia w laboratorium	projekt + zajęcia w laboratorium
KS2: rozumie konieczność wykorzystywania sprawdzonych metod ochrony i technologii bezpieczeństwa	wykład + projekt	n/d

Uwagi:

Data i podpis autora (kierownika zespołu autorskiego): później