# Bezpieczeństwo danych i elementy kryptografii - opis przedmiotu

## Informacje ogólne

| | |
|---|---|
| Nazwa przedmiotu | Bezpieczeństwo danych i elementy kryptografii |
| Kod przedmiotu | 11.3-WI-INFP-BDEK |
| Wydział | Wydział Informatyki, Elektrotechniki i Automatyki |
| Kierunek | Informatyka |
| Profil | ogólnoakademicki |
| Rodzaj studiów | pierwszego stopnia z tyt. inżyniera |
| Semestr rozpoczęcia | semestr zimowy 2022/2023 |

## Informacje o przedmiocie

| | |
|---|---|
| Semestr | 5 |
| Liczba punktów ECTS do zdobycia | 5 |
| Typ przedmiotu | obowiązkowy |
| Język nauczania | polski |
| Sylabus opracował | • dr hab. inż. Remigiusz Wiśniewski, prof. UZ |

## Formy zajęć

| Forma zajęć | Liczba godzin w semestrze (stacjonarne) | Liczba godzin w tygodniu (stacjonarne) | Liczba godzin w semestrze (niestacjonarne) | Liczba godzin w tygodniu (niestacjonarne) | Forma zaliczenia |
|---|---|---|---|---|---|
| Projekt | 15 | 1 | 9 | 0,6 | Zaliczenie na ocenę |
| Laboratorium | 30 | 2 | 18 | 1,2 | Zaliczenie na ocenę |
| Wykład | 15 | 1 | 9 | 0,6 | Zaliczenie na ocenę |

## Cel przedmiotu

- Zapoznanie studentów z podstawowymi metodami zabezpieczeń w systemach informatycznych.
- Ukształtowanie wśród studentów zrozumienia konieczności stosowania zabezpieczeń w systemach informatycznych.

## Wymagania wstępne

## Zakres tematyczny

Wprowadzenie: Podstawowe mechanizmy szyfrowania danych, bezpieczeństwo systemów danych w informatyce, zastosowanie kryptografii w życiu codziennym (podpis elektroniczny, szyfrowanie haseł w informatyce, zabezpieczenia kart elektronicznych, itd.).

Historia kryptografii: Wpływ kryptologii na bieg wydarzeń historycznych. Podstawowe algorytmy historyczne (m.in. szyfry: Cezara, Vigenere, Vernama, Playfair, ADFGVX) w kontekście współczesnych mechanizmów ochrony danych. Sposoby implementacji algorytmów historycznych
z wykorzystaniem języków programowania oraz mikrosystemów cyfrowych. Kryptoanaliza algorytmów historycznych (analiza statystyczna, entropia, cykliczność, metody wykorzystujące podstawienie n-gramów, itd.).

Algorytmy szyfrowania symetrycznego: Ogólna charakterystyka, zastosowanie, sposób realizacji
z wykorzystaniem języków programowania, implementacja z wykorzystaniem mikrosystemów cyfrowych. Porównanie realizacji programowej oraz sprzętowej (implementacja, funkcjonalność, szybkość działania, bezpieczeństwo). Algorytmy szyfrowania blokowego (AES, DES) oraz strumieniowego (RC4). Zalety, wady algorytmów symetrycznych.

Algorytmy szyfrowania asymetrycznego: Główne założenia kryptografii asymetrycznej, koncepcja klucza publicznego, podstawowe algorytmy (RSA, algorytm El-Gamala). Zalety i wady algorytmów asymetrycznych.

Funkcje skrótu (MD5, SHA-1, SHA-3). Ogólna charakterystyka, zastosowanie (hasła, podpis cyfrowy/elektroniczny, waluty Internetowe). Zalety i słabości funkcji skrótu. Implementacja programowa i sprzętowa wybranych algorytmów funkcji skrótu.

Podpis elektroniczny: Ogólna charakterystyka, zastosowanie, podstawowe własności oraz mechanizmy. Podpis tradycyjny a podpis elektroniczny - podobieństwa, różnice, porównanie pod kątem bezpieczeństwa i wiarygodności.

Opcjonalnie: Wprowadzenie i omówienie podstawowych założeń kryptoanalizy programów i aplikacji. Zastosowanie mechanizmu debugowania (ang. debugging) programów komputerowych w kryptoanalizie.

Bezpieczeństwo serwisów Internetowych, analiza najpopularniejszych ataków (m.in. *SQL-Injection*, *Cross-site Scripting*). Zabezpieczenia serwisów Internetowych na poziomie bazy, aplikacji, serwera.

Kryptografia praktyczna: Podstawowe metody ochrony kont Internetowych (np. kont pocztowych, bankowych, czy profili w serwisach społecznościowych). Praktyczne sposoby doboru haseł. Metody ochrony przed wirusami komputerowymi. Podstawy zabezpieczeń urządzeń mobilnych. Przydatne narzędzia wspomagające ochronę danych w życiu codziennym (m.in. kopie bezpieczeństwa, zapory sieciowe, archiwizacja danych, uwierzytelnianie dwuetapowe z zastosowaniem kluczy U2F, itp.).

## Metody kształcenia

**Wykład:** wykład konwencjonalny, dyskusja

**Laboratorium:** gry dydaktyczne, burza mózgów, zajęcia praktyczne, ćwiczenia laboratoryjne

**Projekt:** metoda projektu

## Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

| Opis efektu | Symbole efektów | Metody weryfikacji | Forma zajęć |
|---|---|---|---|
| Potrafi dostrzec i zminimalizować zagrożenia związane z bezpieczeństwem danych w programach komputerowych, aplikacjach internetowych oraz systemach cyfrowych | • K_W19 | • sprawdzian<br>• bieżąca kontrola na zajęciach | • Laboratorium |
| Potrafi zabezpieczyć przesyłane dane zarówno w zakresie programów komputerowych, jak i aplikacji internetowych | • K_W18<br>• K_U29 | • bieżąca kontrola na zajęciach<br>• projekt | • Laboratorium<br>• Projekt |
| Ma podstawową wiedzę związaną z aspektami prawnymi ochrony danych (aplikacje komputerowe, serwisy internetowe, systemy cyfrowe, karty elektroniczne, podpis cyfrowy) | • K_W18<br>• K_W19 | • kolokwium | • Wykład |
| Potrafi wykorzystać istniejące algorytmy kryptograficzne do zabezpieczenia aplikacji komputerowych oraz systemów cyfrowych | • K_W18<br>• K_U29 | • bieżąca kontrola na zajęciach<br>• projekt | • Laboratorium<br>• Projekt |
| Rozumie potrzebę ochrony systemów informatycznych, ma świadomość konieczności stosowania zabezpieczeń informatycznych w życiu codziennym (dostęp do danych elektronicznych/komputera, zastosowanie kart elektronicznych oraz podpisu elektronicznego) | • K_W18<br>• K_W19<br>• K_K03 | • bieżąca kontrola na zajęciach<br>• dyskusja<br>• kolokwium<br>• obserwacja i ocena aktywności na zajęciach | • Wykład<br>• Laboratorium |
| Ma podstawową wiedzę związaną z ochroną i bezpieczeństwem danych w aplikacjach komputerowych (programy komputerowe), aplikacjach Internetowych (serwisy internetowe) oraz urządzeniach mobilnych | • K_W18<br>• K_W19 | • bieżąca kontrola na zajęciach<br>• dyskusja<br>• kolokwium<br>• sprawdzian | • Wykład<br>• Laboratorium |

## Warunki zaliczenia

**Wykład** - warunkiem zaliczenia jest uzyskanie pozytywnych ocen z kolokwiów pisemnych lub ustnych przeprowadzonych co najmniej raz w semestrze

**Laboratorium** - warunkiem zaliczenia jest uzyskanie pozytywnych ocen ze wszystkich ćwiczeń laboratoryjnych, przewidzianych do realizacji w ramach programu laboratorium

**Projekt** - warunkiem zaliczenia jest uzyskanie pozytywnych ocen ze wszystkich zadań projektowych, przewidzianych do realizacji w ramach zajęć projektowych.

**Składowe oceny końcowej** = wykład: 30% + laboratorium: 40% + projekt: 30%

## Literatura podstawowa


1. Karbowski M., Podstawy Kryptografii, Helion, Warszawa, 2021.
2. Stinson D.R., Kryptografia, WNT, Warszawa, 2005.
3. Aho A. V., Hopcroft J. E., Ullman J. D., Algorytmy i struktury danych. Helion, Warszawa, 2003.


## Literatura uzupełniająca


1. Schneier B., Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT, Warszawa, 2002.
2. Strona internetowa *https://niebezpiecznik.pl*.
3. Strona internetowa *https://zaufanatrzeciastrona.pl*
4. Mitnick K., Wozniak S., Simon W. L., Duch w sieci. Moje przygody jako najbardziej poszukiwanego hakera wszech czasów, Helion, Gliwice, 2019.
5. Mitnick K., Simon W. L., Wozniak S., Sztuka podstępu. Łamałem ludzi, nie hasła, Helion, Gliwice, 2016.


## Uwagi

Zmodyfikowane przez dr hab. inż. Remigiusz Wiśniewski, prof. UZ (ostatnia modyfikacja: 19-04-2022 22:40)