**Nazwa przedmiotu:**

Protokoły kryptograficzne

**Koordynator przedmiotu:**

Zbigniew KOTULSKI

**Status przedmiotu:**

Fakultatywny dowolnego wyboru

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Telekomunikacja

**Grupa przedmiotów:**

Przedmioty techniczne

**Kod przedmiotu:**

PKRY

**Semestr nominalny:**

5 / rok ak. 2018/2019

**Liczba punktów ECTS:**

5

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

60

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 0h |
| Laboratorium: | 0h |
| Projekt: | 30h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Uzyskana wiedza i umiejętności z przedmiotów matematycznych przewidzianych dla specjalności.
Umiejętność programowania w wybranym języku programowania ogólnego przeznaczenia.
Wskazana jest znajomość języka angielskiego (umiejętność czytania tekstów naukowych i dokumentacji technicznych).

**Limit liczby studentów:**

60

**Cel przedmiotu:**

Celem wykładu jest przedstawienie możliwości, jakich dostarczają metody kryptograficzne w zakresie zapewnienia bezpieczeństwa komunikacji w sieciach otwartych oraz bezpiecznego realizowania wszelkich usług w sieci. Wykład pokazuje protokoły kryptograficzne z różnych punktów widzenia: jako algorytmy matematyczne (wykorzystujące pewne teorie matematyczne), jako model metody komunikowania się (co najmniej) dwóch stron, jako praktyczne implementacje sieciowe i jako składniki realizowanej polityki bezpieczeństwa w sieci. Po wysłuchaniu wykładu student powinien rozumieć zasady działania protokołów kryptograficznych, umieć odczytywać normy dotyczące bezpiecznej komunikacji, konfigurować (z gotowych elementów) usługi bezpieczeństwa w sieci oraz samodzielnie konstruować proste protokoły kryptograficzne.

**Treści kształcenia:**

Wykład składa się z 15 dwugodzinnych jednostek. Wykład pierwszy i ostatni mają charakter ogólny (odpowiednio, wstęp i spojrzenie na zagadnienie protokołów kryptograficznych z punktu widzenia praktyki zarządzania bezpieczeństwem sieci). Pozostałe wykłady podzielone są na trzy bloki tematyczne. Pierwszy blok jest wstępem matematycznym. Wprowadza pojęcia wstępne i elementy składowe, z których budowane są wszelkie protokoły. Drugi blok przedstawia w matematycznym ujęciu zasady budowy protokołów kryptograficznych, podstawowe rodzaje tych protokołów wraz z przykładami algorytmów realizujących. W trzecim bloku podane zostaną przykłady implementacji protokołów dostępnych w sieci, funkcja jaką pełnią i zasada działania.
W.1. Wprowadzenie i uwagi historyczne. Realizacja protokołów kryptograficznych metodami tradycyjnymi.
W.2. -W.5. Podstawy matematyczne protokołów kryptograficznych. Podstawowe funkcje matematyczne wykorzystywane w kryptografii. Prymitywy kryptograficzne. Przykłady prymitywów kryptograficznych.
W.6.-W.12. Klasyfikacja protokołów. Omówienie najważniejszych protokołów kryptograficznych: uzgadnianie klucza, wymiana informacji, podział sekretu, obliczenia rozproszone. Uwierzytelnienie i potwierdzenie autentyczności. Protokoły grupowe. Dowody z wiedzą zerową. Dodatkowe możliwości protokołów kryptograficznych.
W.13.-W.14. Wykorzystanie protokołów kryptograficznych w sieciach komputerowych. Omówienie wykorzystywanych w praktyce bezpiecznych protokołów sieciowych i metod zabezpieczeń kryptograficznych, np. ssh, ssl, https, PGP, PEM.
W.15. Polityka bezpieczeństwa w sieciach - normy, ustawy, praktyka.

**Metody oceny:**

Kolokwium 1 Materiał z wykładów 1-5. Ocena wiedzy i umiejętności praktycznych (zrozumienie działania podstawowych algorytmów kryptograficznych)
Kolokwium 2 Materiał z całego wykładu. Ocena wiedzy dotyczącej protokołów kryptograficznych. Ocena umiejętności konstruowania i zapisu specyfikacji protokołow kryptograficznych
Projekt. Ocena umiejetności odczytania dokumentacji i wdrożenia protokołu kryptograficznego. Prezentacja oprecowanego projektu i działania aplikacji.

**Egzamin:**

nie

**Literatura:**

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press 1997.
(dostępna jest darmowa wersja na stronie internetowej autorów)
(dostępny jest przekład w języku polskim)
Bruce Schneier, "Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C". J. Willey WNT, Warszawa, 2002.
Douglas R. Stinson, "Cryptography. Theory and Practice", CRC Press 1995.
Dorothy Elizabeth Robling Denning, "Kryptografia i ochrona danych", WNT 1993.
Cryptography e-print archive (strona internetowa IACR).
Literatura podawana po każdym wykładzie.
Wykłady w formie plików pdf dostępne na stronie prywatnej przedmiotu.

**Witryna www przedmiotu:**

http://studia.elka.pw.edu.pl/pub/11Z/PKRY.A/

**Uwagi:**

Projekt będzie realizowany (w zależności od wyboru dokonanego przez studentów) jedną z dwóch metod. Pierwsza metoda polega na wykonaniu opracowania teoretycznego (projektowego) dotyczącego protokołu kryptograficznego, składającego się z krytycznego opisu stanu badań (wg. literatury) oraz propozycji własnego rozwiązania. Druga metoda to przygotowanie własnej implementacji protokołu (znanego lub własnego). Projekty są wykonywane przez grupy studentów. Każda grupa będzie miała okazję przedstawić wynik swojej pracy wszystkim studentów w czasie dwóch lub trzech krótkich prezentacji.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka PKRY\_W01:**

Zna podstawowe metody matematyczne stosowane w kryptografii

Weryfikacja:

Kolokwium 1, sprawozdanie z projektu, konsultacje

**Powiązane charakterystyki kierunkowe:** K\_W01

**Powiązane charakterystyki obszarowe:** I.P6S\_WG

**Charakterystyka PKRY\_W02:**

Zna zasady działania i podstawowe przykłady algorytmów kryptograficznych

Weryfikacja:

Kolokwium 1, sprawozdanie z projektu, konsultacje

**Powiązane charakterystyki kierunkowe:** K\_W04, K\_W14

**Powiązane charakterystyki obszarowe:** I.P6S\_WG, III.P6S\_WG.o

**Charakterystyka PKRY\_W03:**

Zna podstawowe protokoły kryptograficzne i metody zabezpieczeń stosowane w sieciach komputerowych

Weryfikacja:

Kolokwium 2, implementacja projektu

**Powiązane charakterystyki kierunkowe:** K\_W10, K\_W12, K\_W05

**Powiązane charakterystyki obszarowe:** I.P6S\_WG

### Profil ogólnoakademicki - umiejętności

**Charakterystyka Kolokwium 2, sprawozdanie z projektu, implementacja projektu:**

Potrafi samodzielnie zaprojektować protokół kryptograficzny chroniący wskazaną usługę internetową

Weryfikacja:

PKRY\_U01

**Powiązane charakterystyki kierunkowe:** K\_U02, K\_U10, K\_U12

**Powiązane charakterystyki obszarowe:** I.P6S\_UK, I.P6S\_UW, III.P6S\_UW.1.o, III.P6S\_UW.4.o

**Charakterystyka PKRY\_U02:**

Potrafi zaimplementować algorytm lub protokół kryptograficzny wyspecyfikowany w standardzie lub artykule naukowym do aplikacji sieciowej

Weryfikacja:

Implementacja projektu

**Powiązane charakterystyki kierunkowe:** K\_U09, K\_U14

**Powiązane charakterystyki obszarowe:** I.P6S\_UW, III.P6S\_UW.4.o, III.P6S\_UW.1.o, III.P6S\_UW.2.o

**Charakterystyka PKRY\_U03:**

Potrafi zaprezentować zaprojektowane rozwiązanie techniczne i uzasadnoś celowość przyjętych rozwiązań technologicznych

Weryfikacja:

Demonstracja działania i prezentacja na temat projektu

**Powiązane charakterystyki kierunkowe:** K\_U02, K\_U03, K\_U08, K\_U13

**Powiązane charakterystyki obszarowe:** I.P6S\_UK, I.P6S\_UU, I.P6S\_UW, III.P6S\_UW.2.o, III.P6S\_UW.3.o

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka PKRY\_K01:**

Potrafi pracować indywidualnie i w zespole

Weryfikacja:

Realizacja zadania projektowego w grupie

**Powiązane charakterystyki kierunkowe:** K\_K03, K\_K06

**Powiązane charakterystyki obszarowe:** I.P6S\_KO

**Charakterystyka PKRY\_K02:**

Potrafi zamodzielnie uzyskiwać informacje niezbędne do rozwiązania zadania

Weryfikacja:

realizacja zadania projektowego

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K05

**Powiązane charakterystyki obszarowe:**