

# POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2015/2016

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Informatyka stosowana dla inżynierów

### 1 INFORMACJE O PRZEDMIOCIE

|   |  |
|---|--|
| NAZWA PRZEDMIOTU                        | Technologie ochrony systemów informatycznych |
| NAZWA PRZEDMIOTU<br>W JĘZYKU ANGIELSKIM | Computer system security technologies        |
| KOD PRZEDMIOTU                          | WFMiI I oIIS D7 15/16                        |
| KATEGORIA PRZEDMIOTU                    | Przedmioty specjalnościowe                   |
| LICZBA PUNKTÓW ECTS                     | 5.00   |
| SEMESTRY                                | 2  |

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 2       | 30     | 0         | 15           | 0                                | 0          | 0       |

### 3 CELE PRZEDMIOTU

**Cel 1** Zapoznanie studentów z podstawowymi pojęciami i metodami kryptograficznego zabezpieczania informacji.

**Cel 2** Zapoznanie studentów z podstawowymi algorytmami kryptograficznymi

**Cel 3** Zapoznanie studentów z podstawowymi metodami zabezpieczenia systemu operacyjnego komputera i systemu komputerowego

## 4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1 zaliczenie przedmiotów: algebra, matematyka dyskretna

## 5 EFEKTY KSZTAŁCENIA

**EK1 Wiedza** Student objaśnia podstawowe pojęcia z zakresu kryptografii

**EK2 Umiejętności** Student potrafi zrealizować podstawowe algorytmy kryptograficzne

**EK3 Wiedza** Student objaśnia podstawowe metody zabezpieczenia systemu komputerowego

**EK4 Umiejętności** Student potrafi stosować wybrane metody zabezpieczenia danych w systemie operacyjnym i w sieci komputerowej

## 6 TREŚCI PROGRAMOWE

| WYKŁAD     |  |                  |
|------------|--|------------------|
| LP         | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH   | LICZBA<br>GODZIN |
| <b>W1</b>  | Wstęp: potrzeba zabezpieczenia systemów komputerowych. Kryptografia i kryptoanaliza. Podział systemów kryptograficznych. Systemy stosowane w przeszłości.  | 2                |
| <b>W2</b>  | Symetryczne systemy kryptograficzne: ogólne zasady, współczesne realizacje: DES, AES, inne systemy. Wzrastające wymagania wobec systemów symetrycznych.  | 2                |
| <b>W3</b>  | Asymetryczne systemy kryptograficzne: ogólne zasady, system RSA.   | 2                |
| <b>W4</b>  | Systemy oparte na logarytmie dyskretnym: Massey-Omury, El Gamala, wymiany klucza Diffiego-Hellmana.  | 2                |
| <b>W5</b>  | Funkcje skrótu: ogólne zasady budowy funkcji skrótu, kolizje, odporność na kolizje. Ataki na funkcje skrótu, paradoks urodzinowy, wnioski. Realizacje funkcji skrótu.  | 2                |
| <b>W6</b>  | Podpis elektroniczny: określenie, cechy, ramy prawne. Schemat podpisu elektronicznego w systemie z kluczem publicznym: RSA, DSA.   | 2                |
| <b>W7</b>  | Schemat podpisu z algorytmem symetrycznym. Podpisy z załącznikiem i podpisy z odtwarzaniem wiadomości. Podpisy niezaprzeczalne. Podpisy ślepe.   | 2                |
| <b>W8</b>  | Identyfikacja użytkownika: system haseł. Przechowywanie haseł, weryfikacja haseł. Ataki na system haseł. Słabe hasła. Weryfikacja haseł. Hasła jednorazowe. System Kerberos.   | 2                |
| <b>W9</b>  | Zabezpieczanie połączeń internetowych: pakiet Secure Shell-korzyści ze stosowania. Schemat nawiązywania połączenia. Pakiety WinSCP i PuTTY dla Windows. Nawiązywanie połączenia za pomocą klucza publicznego w systemie SSH. | 2                |
| <b>W10</b> | Zabezpieczanie połączeń internetowych: pakiet Secure Socket Layer. Korzystanie z pakietu. certyfikaty, elementy certyfikatu, instytucje certyfikujące.   | 2                |

| WYKŁAD |   |                  |
|--------|---|------------------|
| LP     | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH  | LICZBA<br>GODZIN |
| W11    | Wykrywanie włamań do systemów komputerowych. Analiza zachowań użytkowników. Analiza statystyczna i analiza na podstawie reguł.                | 2                |
| W12    | Szkodliwe programy: wirusy komputerowe, robaki, zombie, konie trojańskie i inne. Klasyfikacja, struktura, sposób działania wirusów i robaków. | 2                |
| W13    | Ochrona przed wirusami i innymi złośliwymi programami: programy antywirusowe, klasyfikacja, metody działania. Systemy immunologiczne.         | 2                |
| W14    | Ataki typu Denial of Service. Struktura ataku, sieci ataku, metody przeciwdziałania.  | 2                |
| W15    | Ściany ogniowe: zasady konstrukcji, funkcje, cele, rodzaje, konfiguracje. Kontrola dostępu do danych. Systemy zaufane.                        | 2                |

| LABORATORIUM |  |                  |
|--------------|--|------------------|
| LP           | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH   | LICZBA<br>GODZIN |
| L1           | Przypomnienie podstawowych pojęć z dziedziny algebry, wykorzystywanych w dalszym procesie kształcenia. | 1                |
| L2           | Bezpieczeństwo systemu operacyjnego Linux.   | 2                |
| L3           | Bezpieczeństwo systemu operacyjnego Windows  | 2                |
| L4           | Realizacja, w dowolnym (obiektywnym) języku programowania algorytmu podpisu cyfrowego RSA.             | 1                |
| L5           | Realizacja, w dowolnym (obiektywnym) języku programowania protokołu Diffiego-Hellmana.                 | 1                |
| L6           | Realizacja, w dowolnym (obiektywnym) języku programowania szyfru blokowego DES                         | 2                |
| L7           | Wprowadzenie do pakietu OpenSSL.   | 1                |
| L8           | Budowa centrum certyfikującego z wykorzystaniem pakietu OpenSSL w trybie z linii komend.               | 2                |
| L9           | Wykorzystanie pakietu OpenSSL do budowy bezpiecznych aplikacji.  | 3                |

## 7 NARZĘDZIA DYDAKTYCZNE

N1 Ćwiczenia laboratoryjne

N2 Dyskusja

N3 Wykłady

N4 Konsultacje

## 8 OBCIĄŻENIE PRACĄ STUDENTA

| FORMA AKTYWNOŚCI   | ŚREDNIA LICZBA GODZIN<br>NA ZREALIZOWANIE<br>AKTYWNOŚCI |
|--|---|
| <b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>                                     |   |
| Godziny wynikające z planu studiów   | 45  |
| Konsultacje przedmiotowe   | 10  |
| Egzaminy i zaliczenia w sesji  | 10  |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |   |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 30  |
| Opracowanie wyników  | 20  |
| Przygotowanie raportu, projektu, prezentacji, dyskusji   | 20  |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>135</b>  |
| SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU  | 5.00  |

## 9 SPOSOBY OCENY

### OCENA FORMUJĄCA

F1 Ćwiczenie praktyczne

F2 Odpowiedź ustna

F3 Sprawozdanie z ćwiczenia laboratoryjnego

### OCENA PODSUMOWUJĄCA

P1 Średnia ważona ocen formujących

P2 Test

### WARUNKI ZALICZENIA PRZEDMIOTU

W1 1. Zaliczenie ćwiczeń mogą uzyskać studenci, którzy regularnie uczęszczali na ćwiczenia

W2 2. Ocena końcowa jest średnią z ocen P1-P2.

### OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

B1 Podstawą oceny aktywności bez udziału nauczyciela jest ocena przygotowanego przez studenta sprawozdania z laboratorium.

**KRYTERIA OCENY**

| EFEKT KSZTAŁCENIA 1 |  |
|---------------------|--|
| NA OCENĘ 2.0        | Student nie zna ogólnych zasad systemów kryptograficznych symetrycznych i niesymetrycznych lub nie ma podstawowych wiadomości na temat funkcji skrótu i podpisu elektronicznego lub nie potrafi podać po 1 przykładzie dla każdego wymienionego zagadnienia.   |
| NA OCENĘ 3.0        | Student zna ogólne zasady systemów kryptograficznych symetrycznych i niesymetrycznych, ma podstawowe wiadomości na temat funkcji skrótu i podpisu elektronicznego. Potrafi podać po 1 przykładzie dla każdego wymienionego zagadnienia.  |
| NA OCENĘ 3.5        | Student zna ogólne zasady poszczególnych systemów kryptograficznych symetrycznych i niesymetrycznych, ma wystarczające wiadomości na temat funkcji skrótu i podpisu elektronicznego. Potrafi podać przykłady dla każdego wymienionego zagadnienia.   |
| NA OCENĘ 4.0        | Student zna algorytmy różnych systemów kryptograficznych symetrycznych i niesymetrycznych, zna algorytmy funkcji skrótu i podpisu elektronicznego. Potrafi podać różne przykłady dla każdego ze znanych systemów kryptograficznych.  |
| NA OCENĘ 4.5        | Student zna algorytmy różnych systemów kryptograficznych symetrycznych i niesymetrycznych, zna algorytmy funkcji skrótu i podpisu elektronicznego. Potrafi podać różne przykłady dla każdego ze znanych systemów kryptograficznych. Rozumie matematyczne podstawy tych systemów.   |
| NA OCENĘ 5.0        | Student zna szczegółowo algorytmy różnych systemów kryptograficznych symetrycznych i niesymetrycznych, zna szczegółowo algorytmy funkcji skrótu i podpisu elektronicznego. Potrafi podać przykłady dla każdego znanego systemu kryptograficznego. Rozumie matematyczne podstawy tych systemów.   |
| EFEKT KSZTAŁCENIA 2 |  |
| NA OCENĘ 2.0        | Student nie potrafi wykonać poprawnie trzech z następujących zadań: zrealizować programowo wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfry blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu. |
| NA OCENĘ 3.0        | Student potrafi wykonać poprawnie trzy z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.       |
| NA OCENĘ 3.5        | Student potrafi wykonać poprawnie cztery z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.     |

|                     |  |
|---------------------|--|
| NA OCENĘ 4.0        | Student potrafi wykonać poprawnie pięć z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.   |
| NA OCENĘ 4.5        | Student potrafi wykonać poprawnie wszystkie z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu.  |
| NA OCENĘ 5.0        | Student potrafi wykonać poprawnie wszystkie z następujących zadań: zrealizować programowo: wybrany algorytm podpisu cyfrowego, wybrany protokół uzgadniania kluczy, wybrany szyfr blokowy, wybrany algorytm szyfrowania z kluczem publicznym, wybrany współczesny algorytm szyfrowania z kluczem tajnym, wybrany algorytm funkcji skrótu. Potrafi logicznie uzasadnić wybór zastosowanych metod. |
| EFEKT KSZTAŁCENIA 3 |  |
| NA OCENĘ 2.0        | Student nie zna podstawowych zasad identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działania wirusów komputerowych i sposobów ochrony przed nimi, zasady działania ścian ogniowych.  |
| NA OCENĘ 3.0        | Student zna podstawowe zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych.  |
| NA OCENĘ 3.5        | Student zna różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych.   |
| NA OCENĘ 4.0        | Student zna i rozumie różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych.   |
| NA OCENĘ 4.5        | Student zna i rozumie różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji.  |
| NA OCENĘ 5.0        | Student zna i w pełni rozumie różne zasady identyfikacji użytkownika, zabezpieczenia połączeń internetowych, działanie wirusów komputerowych i sposoby ochrony przed nimi, zasadę działania ścian ogniowych. Potrafi wyciągać logiczne wnioski z posiadanych w tym zakresie informacji. Potrafi uzupełniać wiadomości uzyskane podczas zajęć informacjami pozyskanymi z zewnątrz.                |
| EFEKT KSZTAŁCENIA 4 |  |

|              |  |
|--------------|--|
| NA OCENĘ 2.0 | Student nie potrafi wykonać poprawnie trzech z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w wybranym systemie operacyjnym, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego  |
| NA OCENĘ 3.0 | Student potrafi wykonać poprawnie trzy z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w wybranym systemie operacyjnym, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego  |
| NA OCENĘ 3.5 | Student potrafi wykonać poprawnie cztery z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w systemie operacyjnym, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego   |
| NA OCENĘ 4.0 | Student potrafi wykonać poprawnie wszystkie z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w systemie operacyjnym, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać podstawowe komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego  |
| NA OCENĘ 4.5 | Student potrafi wykonać poprawnie wszystkie z następujących zadań: zastosować wybraną metodę zapewnienia bezpieczeństwa danych w systemie operacyjnym, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać zaawansowane komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego, potrafi zaimplementować aplikację, wykorzystującą narzędzia OpenSSL                 |
| NA OCENĘ 5.0 | Student potrafi wykonać poprawnie wszystkie z następujących zadań: zastosować wybrane metody zapewnienia bezpieczeństwa danych w systemie operacyjnym Linux i Windows, zaimplementować algorytm podpisu cyfrowego RSA, przeprowadzić procedurę uzgadniania kluczy Diffiego-Hellmana, zaszyfrować plik danych szyfrem blokowym DES, wykorzystać zaawansowane komendy pakietu OpenSSL trybie z linii komend w celu budowy centrum certyfikującego, potrafi zaimplementować aplikację, wykorzystującą narzędzia OpenSSL |

## 10 MACIERZ REALIZACJI PRZEDMIOTU

| EFEKT KSZTAŁCENIA | ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU | CELE PRZEDMIOTU | TREŚCI PROGRAMOWE                                     | NARZĘDZIA DYDAKTYCZNE | SPOSOBY OCENY  |
|-------------------|--|-----------------|---|-----------------------|----------------|
| EK1               |  | Cel 1           | W1 W2 W3 W4<br>W5 W6 W7 L1<br>L4 L5 L6                | N2 N3 N4              | F1 F2 F3 P1 P2 |
| EK2               |  | Cel 2           | W1 W2 W3 W4<br>W5 W6 W7 L1<br>L4 L5 L6                | N1 N2 N4              | F1 F2 F3 P1 P2 |
| EK3               |  | Cel 3           | W8 W9 W10<br>W11 W12 W13<br>W14 W15 L2 L7<br>L8 L9    | N2 N3 N4              | F1 F2 F3 P1 P2 |
| EK4               |  | Cel 3           | W8 W9 W10<br>W11 W12 W13<br>W14 W15 L2 L3<br>L7 L8 L9 | N1 N3 N4              | F1 F2 F3 P1 P2 |

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA

- [1] | **Ogiela M.** — *Bezpieczeństwo systemów komputerowych*, Kraków, 2002, AGH
- [2] | **Stallings W.** — *Kryptografia i bezpieczeństwo sieci komputerowych : koncepcje i metody bezpiecznej komunikacji*, Gliwice, 2012, Helion

### LITERATURA UZUPEŁNIAJĄCA

- [1] | **Stallings, W.** — *Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii*, Gliwice, 2012, Helion
- [2] | **B. Schneier** — *Kryptografia dla praktyków*, Warszawa, 2002, WNT

### LITERATURA DODATKOWA

- [1] | **Karbowski M.** — *Podstawy kryptografii*, Gliwice, 2014, Helion
- [2] | **Szeliga M.** — *Bezpieczeństwo w sieciach Windows : kompendium administratora sieci*, Gliwice, 2003, Helion

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr hab. Andrzej Karafiat (kontakt: akaraf@pk.edu.pl)





## OSOBY PROWADZĄCE PRZEDMIOT

1 Dr hab Andrzej Karafiat (kontakt: akaraf@pk.edu.pl)

2 Dr Agnieszka Krok (kontakt: agakrok@poczta.fm)

## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

---

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....

.....