**Nazwa przedmiotu:**

Podstawy teoretyczne kryptografii i ochrony informacji - B

**Koordynator przedmiotu:**

prof. nzw. dr hab. Tomasz Adamski

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Elektronika

**Grupa przedmiotów:**

Przedmioty techniczne - zaawansowane

**Kod przedmiotu:**

PTKB

**Semestr nominalny:**

4 / rok ak. 2015/2016

**Liczba punktów ECTS:**

4

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

Liczba godzin pracy studenta i obliczanie punktów ECTS dla przedmiotu

1. godziny kontaktowe - 65h; w tym

a. obecność na wykładach –30 h
b. obecność na ćwiczeniach-15 h
c. obecność na zajęciach projektowych – 15 h
d. konsultacje – 5 h

2. przygotowanie do zajęć – 60h, w tym

a. przygotowanie do wykładów – 30 h
b. przygotowanie do ćwiczeń- 15 h
c. przygotowanie do zajęć projektowych – 15 h

Razem nakład pracy studenta 125h = 4 pkt. ECTS

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

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich

1. obecność na wykładach – 30 h
2. obecność na ćwiczeniach -15 h
3. obecność na zajęciach projektowych – 15 h
4. konsultacje z prowadzącymi zajęcia – 5h

Razem 65 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

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

Liczba punktów ECTS, które student uzyskuje w ramach zajęć
o charakterze praktycznym

1. obecność na ćwiczeniach – 15 h
2. przygotowanie do ćwiczeń – 15 h
3. przygotowanie do projektu -15 h
4. obecność na zajęciach projektowych -15 h

Razem 60h, co odpowiada 2 pkt. ECTS

Nakład pracy związany z zajęciami o charakterze praktycznym wynosi 15+15+15+15= 60h, co odpowiada 2 pkt. ECTS.

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

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 15h |
| Laboratorium:  | 0h |
| Projekt:  | 15h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Matematyka

Technika cyfrowa

Technika mikroprocesorowa

**Limit liczby studentów:**

100

**Cel przedmiotu:**

1.Zasadniczym celem przedmiotu jest wprowadzenie do metod kryptograficznych stosowanych w systemach komputerowych, sieciach komputerowych, sieciach sensorowych, rozproszonych systemach pomiarowych i telekomunikacji. Na wykładzie omawiane są m.in. matematyczne podstawy kryptografii, szyfry, uwierzytelnianie strony, protokoły kryptograficzne, podpisy cyfrowe i funkcje skrótu.
Specjalną uwagę zwrócono na zastosowania metod kryptograficznych we współczesnych rozproszonych systemach pomiarowych.

2.Ważnym celem przedmiotu jest również przekazanie słuchaczowii pewnego niezbęnego współczesnemu ińżynierowi IT spójnego quantum wiedzy i umiejętności w zakresie wpółczesnej algebry, teorii liczb, algorytmiki i teorri prawdopodobieństwa.

**Treści kształcenia:**

Treść wykładu:

1.Kryptografia - pojęcia podstawowe i szyfry klasyczne (2 h)
Cele i środki kryptografii – kryptograficzne „objectivies and primitivies”, alfabet, język, kody, odległość Hamminga, szyfr, system kryptograficzny, funkcja jednokierunkowa, rodzaje szyfrów, szyfry blokowe, szyfry strumieniowe, szyfry klasyczne, szyfr Cezara, szyfr, Playfair’a, szyfr Vigenaire’a, Enigma, szyfry podstawieniowe, szyfry polialfabetowe, szyfry przestawieniowe, szyfry produktowe, szyfry idealne, szyfr Vernama, metody kryptoanalizy szyfrów klasycznych, steganografia

2. Podstawy matematyczne kryptografii (4h)
Liczby całkowite, liczby pierwsze, podzielność, kongruencje, funkcja Eulera, algebry abstrakcyjne, działania, grupy, pojęcie logarytmu dyskretnego w grupie, pierścienie przemienne, pierścienie ilorazowe, ideały w pierścieniach, ciała, ciała skończone, pierścienie wielomianów, pierścienie z jednoznacznością rozkładu, pierścienie euklidesowe, reszty i niereszty kwadratowe, pierwiastki z jedności, symbol Legendre'a, symbol Jacobiego, małe tw. Fermata, tw. Eulera, chińskie twierdzenie o resztach, NWD, rozszerzony algorytm Euklidesa, binarny algorytm Euklidesa (algorytm Steina), złożoność obliczeniowa algorytmów, redukowalność, klasy złożoności P, NP, coNP, NP zupełność, problemy NP trudne, przykłady problemów trudnych obliczeniowo (problem rozkładu liczby całkowitej na czynniki-problem faktoryzacji, problem logarytmów dyskretnych, problem Diffi -Hellmann'a, problem plecakowy itd.), krzywe eliptyczne, kraty punktowe, problemy CVP i SVP, kody korekcyjne, LFSR i maszyny liniowe nad ciałami skończonymi, probabilistyczne i teorioinformacyjne podstawy kryptologii, paradoks dnia urodzin,

3. Szyfry z kluczem publicznym (2 h)
Szyfr RSA, modyfikacje szyfru RSA, szyfr Rabina, szyfr ElGamala, szyfry plecakowe (szyfr Merklego-Hellmana), szyfr McEliece, szyfr Massey’a-Omury, szyfry probabilistyczne, systemy kryptograficzne oparte na krzywych eliptycznych i hipereliptycznych, generacja parametrów systemów kryptograficznych z kluczem publicznym, szyfry wykorzystujące problemy obliczeniowo trudne krat teorioloiczbowych, szyfr NTRU, kryptoanaliza szyfrów z kluczem publiczym,

4. Szyfry z kluczem prywatnym (2h)
Sieci permutacyjno-podstawieniowe, szyfry Feistela, runda, S-box, efekt lawinowy, DES, 3DES, DESX, Lucipher, AES, IDEA, TES, FEAL, Serpent, Twofish, Blowfish, RC-5, Camelia, MARS, CAST - 128, CAST - 256, SAFER, RC5, RC6, SAFER, zasady projektowania szyfrów z kluczem prywatnym, kryptoanaliza szyfrów z kluczem prywatnym, ataki na szyfry z kluczem prywatnym, kryptoanaliza liniowa, kryptoanaliza różnicowa

5. Generacja bitów, liczb losowych i pseudolosowych dla celów kryptograficznych (1h)
Generatory TRNS i PRNG, postulaty losowości Golomba, liniowe generatory kongruencyjne, ziarno generatora, generatory wykorzystujące rejestry LFSR, generator Plessa, generator Geffego, generator stop-and-go, generatory kryptograficznie bezpieczne, generator RSA bitów pseudolosowych, generator BBS, generator ANSI X9.17, generator FIPS 186, generator Bluma-Micalego, generator Micalego-Schnore’a, testowanie generatorów liczb losowych, testy i pakiety statystyczne do testowania generatorów liczb losowych (system R)

6. Algorytmy testowania pierwszości i generacja liczb pierwszych (2h)
Algorytmy deterministyczne i probabilistyczne testowania piertwszości, sito Eratostenesa, liczby pseudopierwsze, liczby Carmichaela, algorytm Fermata, algorytm Solovaya-Strassena, algorytm Millera-Rabina, algorytm AKS, liczby Mersenne’a, testowanie pierwszości liczb Mersenne’a

7. Szyfry strumieniowe (2h)
Konstrukcja szyfrów strumieniowych, szyfry idealne (m.in. szyfr Vernama), szyfry strumieniowe synchroniczne i samosynchronizujące się, zastosowanie rejestrów LFSR do konstrukcji szyfrów strumieniowych, szyfry A5/1,A5/2 (telefonia komórkowa GSM), RC4, SEAL, SNOW, FISH, SOBER-128, PANAMA, ataki na szyfry strumieniowe.

8. Tryby wykorzystania szyfrów blokowych (1h)
Zasady stosowania szyfrów blokowych, tryb elektronicznej książki kodowej (ECB), tryb wiązania bloków zaszyfrowanych (CBC), tryby PCBC, CFB, OFB, tryb licznikowy CTR, tryb BC

9. Funkcje skrótu (2h)
Własności i klasyfikacja kryptograficznych funkcji skrótu, funkcje skrótu słabo i silnie bezkolizyjne, kluczowane funkcje skrótu (MAC), funkcje skrótu bez klucza, funkcje skrótu Chauma-van Heijsta- Pfitzmann'a, ogólne schematy tworzenia funkcji skrótu, schemat Daviesa itd, funkcje skrótu wykorzystujące szyfry blokowe, ataki na funkcje skrótu, paradoks dnia urodzin, atak urodzinowy, przykłady algorytmów funkcji skrótu (MD5, SHA-1, SHA-256, SHA-512, RIPEMD-160, HAVAL, Whirlpool, Tiger itd.)

10. Identyfikacja-uwierzytelnianie strony (2h)
Hasła, słabe uwierzytelnianie, solenie, identyfikacja metodą "pytanie-odpowiedź, dowody z wiedzą zerową, jaskinia wiedzy zerowej, protokoły identyfikacji oparte na dowodach z wiedzą zerową, algorytm Fiat'a-Shamir'a, algorytm Feige-Fiat'a-Shamir'a, algorytm Guillou-Quisquatera, algorytm Schnorr'a, uwierzytelnianie na grafach, ataki na protokoły identyfikacji

11. Uwierzytelnianie dokumentu - podpisy cyfrowe (2h)
Podstawowe cechy podpisu cyfrowego i rodzaje podpisów cyfrowych, podpisy wykorzystujące RSA, podpisy ElGamala, podpisy ElGamala na grupach, podpisy Rabina, standard DSS, podpisy Nyberga-Ruepla, podpisy Rabina –Wiliamsa, podpisy wykorzystujące protokół uwierzytelniania strony (podpisy Fiat'a-Shamir'a, podpisy Feige’go-Fiata-Shamira, podpisy Guillou-Quisquatera), podpisy Schnorr'a, podpisy niezaprzeczalne, podpisy niepodrabialne, podpisy ślepe, podpisy jednokrotne (podpis jednokrotny Lamporta, podpis jednokrotny Rabina, podpis jednokrotny Matyasa-Meyera), znaczniki czasu (stemplowanie czasem)

12.Efektywna implementacja algorytmów kryptograficznych (2h)
Algorytmy szybkiego dodawania, odejmowania, mnożenia i dzielenia wielokrotnej precyzji dla liczb całkowitych, algorytm Shonhagego-Strassena, algorytmy szybkiej arytmetyki resztowej wielokrotnej precyzji (algorytmy szybkiego podnoszenia do potęgi modulo, szybkie algorytmy redukcji modulo, algorytm Montgomery’ego, algorytm Barretta), algorytmy obliczania NWD, binarny algorytm Euklidesa (algorytm Steina), i binarny rozszerzony algorytm Euklidesa), generacja wielomianów nierozkładalnych nad , generacja generatorów grupy multiplikatywnej ciała skończonego, algorytmy pierwiastkowania modulo, algorytm obliczania wartości symbolu Legendre’a, układy do obliczeń resztowych i realizacja algorytmów kryptograficznych w strukturach FPGA i ASIC, kryptograficzne karty chipowe, rozwiązania małej mocy dla sieci sensorowych o ograniczonych zasobach, biblioteki kryptograficzne Open SSL, NTL, Botan, Crypto++

13. Uzgadnianie kluczy, dystrybucja kluczy, protokoły wymiany klucza (1h)
Zaufana trzecia strona, TTP, protokoły Diffi-Hellmann’a, atak „man i the middle” protokół szerokogębnej żaby, protokół Needhama-Schroedera

14. Dzielenie tajemnic (1h)
Algorytm interpolacyjny Shamira, algorytm wykorzystujący RNS

15. Protokoły kryptograficzne (1h)
Rzut monetą przez telefon, protokoły głosowania przez Internet, stemplowanie czasem-time stamping, protokoły SSL, TLS

16. Zarządzanie kluczami (key management), infrastruktura klucza publicznego (PKI) (1h)
Infrastruktura klucza publicznego (PKI), urząd do spraw certyfikatów (CA)-organizacja, zarządzanie kluczami (key management), Kerberos, modele bezpieczeństwa

17. Kryptografia kwantowa (2h)
Zasady kryptografii kwantowej, protokół BB 84, protokół E91, protokół S09, position-based quantum cryptography

Treść ćwiczeń:

1.Systemy kryptograficzne, szyfry klasyczne, ataki na szyfry klasyczne (2h)

2.Obliczanie wartości funkcji Eulera, tw. Eulera i jego zastosowania, pierścień
i jego własności (1h)

3.Liczby pierwsze i testowanie pierwszości, sito Eratostenesa, algorytm Millera-Rabina (1h)

4. Grupy, podgrupy, dzielniki normalne, grupy ilorazowe, grupy cykliczne i ich własności, tw. Lagrange’a, logarytm dyskretny w grupie, krzywe eliptyczne, bazy Gaussa, bazy normalne (2h)

5.Pierścienie, ciała i ich własności, chińskie twierdzenie o resztach, zapis RNS, algorytmy konwersji z zapisu RNS na naturalny zapis binarny (2h)

6.Szyfry z kluczem publicznym (szyfr RSA, ElGamala, Rabina, NTRU) , algorytm Diffiego-Hellmana uzgadniania kluczy (2h)

7. Szyfry z kluczem prywatnym (DES,AES,IDEA,TES, szyfry Feistala) (2h)

8.Algorytmy uwierzytalniania strony, jaskinia z wiedzą zerową, dowody z wiedzą zerową (1h)

9. Algorytmy uwierzytelnianie dokumentu, podpisy cyfrowe (podpisy ElGamala, podpis DSS) (1h)

10.Efektywne implementacje algorytmów kryptograficznych (algorytm Mongomery’ego, algorytm Barretta, szybkie podnoszenie do potęgi modulo) (1h)

Projekt-uwagi realizacyjne
Projekty są indywidualne w tym sensie, że każdy student rozwiązuje inny, odrębny problem samodzielnie. Przyjęto zasadę jeden student-jeden projekt. Projekt zaliczany jest dwuetapowo. Etap 1 to zaliczanie wstępne polegające na zatwierdzeniu zasadniczych koncepcji projektu i analizie teoretycznej proponowanego rozwiązania wraz z oceną poziomu bezpieczeństwa i efektywności stosowanych algorytmów . Etap 2 to zaliczenie końcowe polegające na przedstawieniu całości projektu wraz z częścią implementacyjną (programową lub układową). Projekty zmieniane są na nowe w każdej edycji przedmiotu.

**Metody oceny:**

Sposoby weryfikacji zakładanych efektów kształcenia:

Do uzyskania jest 200pkt:
 Egzamin 100 pkt
 Ćwiczenia 70 pkt
 Projekt 30 pkt

Do zaliczenia potrzeba min. 100 pkt

Weryfikacja odbywa się na podstawie wyników 3 kolokwiów (po 20 pkt), ocen za zadania domowe (w sumie za 20pkt)) oraz oceny za projekt (30 pkt).

**Egzamin:**

tak

**Literatura:**

Materiały dydaktyczne:
[1] A.Menezes, P.van Oorsschot, S.Vanstone; Handbook of Applied Cryptography; CRC Press 1996.
[2] N.Koblitz; Wykład z teorii liczb i kryptografii; WNT, Warszawa 1995.
[3] N.Koblitz; Algebraiczne aspekty kryptografii; WNT, Warszawa 2000.
[4] B.Schneier; Kryptografia dla praktyków; Wiley & WNT, Warszawa 1995.
[5] J. Stokłosa, T.Bilski, T.Pankowski; Kryptograficzna ochrona danych w systemach komputerowych; PWN. Poznań 2001.
[6] W.Stallings; Ochrona danych w sieci i intersieci; WNT, 1998.
[7] T.Cormen, C.Leiserson, R.Rivest; Wprowadzenie do algorytmów; WNT, Warszawa 1997.
[8] J.Pieprzyk, T.Hardjono,J.Seberry; Teoria bezpieczeństwa systemów komputerowych; Helion-Springer, Gliwice 2005.
[9] T.Adamski; Podstawy teoretyczne kryptografii i ochrony informacji; materiały wykładowe w formacie PDF na stronie przedmiotu
[10] T.Adamski; Zbiór zadań z podstawy teoretycznych kryptografii i ochrony informacji; materiały do ćwiczeń w formacie PDF na stronie przedmiotu

**Witryna www przedmiotu:**

studia.elka.pw.edu.pl/ind

**Uwagi:**

Projekt-uwagi realizacyjne

Projekty są indywidualne w tym sensie, że każdy student rozwiązuje inny, odrębny problem samodzielnie. Przyjęto zasadę jeden student-jeden projekt. Projekt zaliczany jest dwuetapowo. Etap 1 to zaliczanie wstępne polegające na zatwierdzeniu zasadniczych koncepcji projektu i analizie teoretycznej proponowanego rozwiązania wraz z oceną poziomu bezpieczeństwa i efektywności stosowanych algorytmów . Etap 2 to zaliczenie końcowe polegające na przedstawieniu całości projektu wraz z częścią implementacyjną (programową lub układową). Projekty zmieniane są na nowe w każdej edycji przedmiotu.

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt K\_W01:**

Ma poszerzoną i pogłębioną wiedzę z matematyki (teorial liczb, algebra, teoria prawdopodobieństwa) umożiwiającą projektowanie bezpiecznych systemów elektronicznych

Weryfikacja:

egzamin, ocena zadań domowych, ocena projektów

**Powiązane efekty kierunkowe:** K\_W01

**Powiązane efekty obszarowe:** T2A\_W01

**Efekt K\_W04:**

Ma podbudowaną teoretycznie wiedzę z zakresu algorytmów kryptograficznych i konstrukcji systemów kryptograficznych w tym systemów kryptografii kwantowej

Weryfikacja:

egzamin, zadania domowe, projekty

**Powiązane efekty kierunkowe:** K\_W04

**Powiązane efekty obszarowe:** T2A\_W04

### Profil ogólnoakademicki - umiejętności

**Efekt K\_U01:**

potrafi wyszukiwać informacje i dokonywać niezbędnych syntez

Weryfikacja:

ocena projektu

**Powiązane efekty kierunkowe:** K\_U01

**Powiązane efekty obszarowe:** T2A\_U01

**Efekt K\_U04:**

potrafi przygotować i przedstawić w języku polskim prezentację ustną, dotyczącą zagadnień z zakresu elektroniki

Weryfikacja:

Obrona projektu

**Powiązane efekty kierunkowe:** K\_U04

**Powiązane efekty obszarowe:** T2A\_U04

**Efekt K\_U08:**

potrafi wykorzystać metody analityczne i symulacyjne do konstrukcji bezpiecznych systemów kryptograficznych

Weryfikacja:

Ocena projektu

**Powiązane efekty kierunkowe:** K\_U08

**Powiązane efekty obszarowe:** T2A\_U09

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt K\_K02:**

Ma świadomość roli społecznej absolwenta dobrej uczelni technicznej

Weryfikacja:

Nie da się niestety tego sprawdzić

**Powiązane efekty kierunkowe:** K\_K02

**Powiązane efekty obszarowe:** T2A\_K07