Politechnika Poznańska
Wydział Informatyki

Europejski **S**ystem **T**ransferu **P**unktów

KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu: **Programowanie kart elektronicznych**							Kod
Kierunek studiów: **Informatyka**			Profil kształcenia (ogólnoakademicki, praktyczny): ogólnoakademicki				Rok / Semestr: 1 / 2
Specjalność: Systemy informatyczne w zarządzaniu			Moduł oferowany w języku: polski				Moduł (obligatoryjny/obieralny): obligatoryjny
Forma zajęć:							Liczba punktów ECTS: 4
Wykłady: 30	Ćwiczenia: -		Laboratoria: 30		Projekty / seminaria: -		
Stopień studiów: II stopień	Forma studiów (stacjonarna/niestacjonarna): stacjonarna		Obszar(y) kształcenia i dziedzina(y) nauki i sztuki: nauki techniczne				Podział ECTS (liczba i %): 4 100%

Status modułu w programie studiów (podtawowy, kierunkowy, inny) (ogólnouczelniany, z innego kierunku)

kierunkowy	specjalnościowy

Odpowiedzialny za przedmiot – wykładowca:

dr inż. Marek Mika

Instytut Informatyki PP
ul. Piotrowo 2, 60-965 Poznań
e-mail: Marek.Mika@cs.put.poznan.pl
,

Inni prowadzący:

mgr inż. Marek Gosławski

Politechnika Poznańska, Dział Rozwoju Oprogramowania
pl. Marii Skłodowskiej-Curie 5, 60-965 Poznań
e-mail: Marek.Goslawski@put.poznan.pl

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z kryptografii. Powinien posiadać umiejętność rozwiązywania podstawowych problemów z zakresu projektowania aplikacji umiejętność programowania w językach wysokiego poziomu oraz umiejętność pozyskiwania informacji ze wskazanych źródeł. Powinien również rozumieć konieczność poszerzania swoich kompetencji). Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu:

1. Przekazanie studentom podstawowej wiedzy dotyczącej kart elektronicznych, w zakresie budowy, zasad działania, zastosowań i programowania.
2. Rozwijanie u studentów umiejętności projektowania i programowania systemów wykorzystujących karty elektroniczne.

Efekty kształcenia	Odniesienie do kierunkowych efektów kształcenia	Stopień realizacji kierunkowego efektu kształcenia
Wiedza W wyniku przeprowadzonych zajęć student:		
1. ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie budowy, zasad działania, programowania i zastosowań kart elektronicznych	**K_W4**	**+++**
2. ma podbudowaną teoretycznie szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki, takimi jak: konstrukcja kart elektronicznych, protokoły transmisji stosowane w kartach elektronicznych, systemy operacyjne kart elektronicznych, komunikacja karty z czytnikiem, programowanie kart elektronicznych	**K_W5**	**+++**
3. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce i w wybranych pokrewnych dyscyplinach naukowych	**K_W6**	**++**
4. ma podstawową wiedzę o cyklu życia systemów informatycznych sprzętowych lub programowych	**K_W7**	**++**
5. zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z wybranego obszaru informatyki	**K_W8**	**++**
Umiejętności W wyniku przeprowadzonych zajęć student powinien wykazać się umiejętnościami w zakresie (student będzie potrafił):		
1. potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł (w języku ojczystym i angielskim), integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie	**K_U1**	**++**
2. potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia	**K_U5**	**++**
3. potrafi wykorzystać do formułowania i rozwiązywania zadań metody analityczne	**K_U9**	**+**
4. potrafi — przy formułowaniu i rozwiązywaniu zadań inżynierskich — integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty	**K_U10**	**++**
5. potrafi formułować i testować hipotezy związane z problemami inżynierskimi	**K_U12**	**+**
6. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych	**K_U13**	**++**
7. potrafi zaproponować ulepszenia (usprawnienia) istniejących rozwiązań technicznych	**K_U21**	**+**
8. potrafi ocenić przydatność metod i narzędzi służących do rozwiązania zadania inżynierskiego, polegającego na budowie lub ocenie systemu informatycznego lub jego składowych, w tym dostrzec ograniczenia tych metod i narzędzi	**K_U24**	**+**
9. potrafi — zgodnie z zadaną specyfikacją, uwzględniającą aspekty pozatechniczne — zaprojektować system informatyczny oraz zrealizować ten projekt — co najmniej w części — używając właściwych metod, technik i narzędzi, w tym przystosowując do tego celu istniejące lub opracowując nowe narzędzia	**K_U27**	**++**
Kompetencje społeczne W wyniku przeprowadzonych zajęć student zdobędzie wymienione niżej kompetencje. Zaliczenie przedmiotu oznacza, że student:		
1. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe	**K_K1**	**++**

2. zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych lub też do poważnej utraty zdrowia, a nawet życie	**K_K4**	**++**
3. potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	**K_K6**	**+**

Sposoby weryfikacji efektów kształcenia

Ocena formująca:

a) w zakresie wykładów:
- na podstawie odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,

b) w zakresie laboratoriów / ćwiczeń:
- na podstawie oceny bieżącego postępu realizacji zadań,

Ocena podsumowująca:

a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez:
- ocenę wiedzy i umiejętności wykazanych na kolokwium pisemnym w formie testu wielokrotnego wyboru. Test składa się z 25 pytań. Za odpowiedzi na każde pytanie można zdobyć maksymalnie 4 punkty, a za cały test punktów 100. Do uzyskania oceny 3,0 należy zdobyć co najmniej 51 punktów. Ocena 3,5 za co najmniej 61 punktów, 4,0 za co najmniej 71 punktów itd.
- omówienie wyników egzaminu,

b) w zakresie laboratoriów / ćwiczeń weryfikowanie założonych efektów kształcenia realizowane jest przez:
- ocenianie zadań wykonywanych w ramach kolejnych zajęć, za każde poprawnie wykonane zadanie można otrzymać maksymalnie 1 punkt, na podstawie liczby zdobytych punktów wystawiana jest ocena cząstkowa
- test końcowy obejmujący zagadnienia przećwiczone w ramach zajęć laboratoryjnych, test składa się z losowo wybranych pytań dotyczących każdego z tematów ćwiczeń, za każdą poprawną odpowiedź można otrzymać 1 punkt, na podstawie liczby zdobytych punktów wystawiana jest druga ocena cząstkowa
- wykonanie i obrona projektu – trzecia ocena cząstkowa
- ocena końcowa wystawiana jest na podstawie trzech ocen cząstkowych

Uzyskiwanie punktów dodatkowych za aktywność podczas zajęć, a szczególnie za:
- omówienia dodatkowych aspektów zagadnienia,
- efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,
- uwagi związane z udoskonaleniem materiałów dydaktycznych,
- wskazywanie trudności percepcyjnych studentów umożliwiające bieżące doskonalenia procesu dydaktycznego.

Treści programowe

Program wykładu obejmuje następujące zagadnienia:

Geneza kart elektronicznych. Przegląd podstawowych zastosowań KE. Rola standaryzacji. Rodzaje kart (wypukłe, z paskiem magnetycznym, pamięciowe stykowe i bezstykowe, procesorowe stykowe i bezstykowe, wielomegabajtowe, optyczne). Cechy fizyczne KE (formaty, styki, materiały, cechy zabezpieczające, moduły z chipem). Cechy elektryczne KE (styki, napięcie i prąd zasilania, zegar, transmisja danych, sekwencje aktywujące i dezaktywujące). Mikrokontrolery KE (technologie półprzewodnikowe, typy procesorów, typy pamięci, moduły komunikacyjne, zegar i inne moduły). Struktury danych. Kodowanie danych alfanumerycznych. Notacja SDL. KE jako automat skończony. Kody wykrywające i korygujące błędy. Kompresja danych. Kryptologia (symetryczne algorytmy szyfrujące: DES, AES, IDEA, COMP128, Milanage; asymetryczne algorytmy szyfrujące: RSA, DSS, algorytm krzywych eliptycznych; wielokrotne szyfrowanie; wyrównywanie danych; uwierzytelnianie komunikatów i kryptograficzna suma kontrolna), funkcje haszujące, generowanie i testowanie liczb losowych, uwierzytelnianie kart i czytników (jednostronne symetryczne, dwustronne symetryczne, statyczne asynchroniczne, dynamiczne asynchroniczne), podpisy cyfrowe, certyfikaty, zarządzanie kluczami, uwierzytelnianie osób. Komunikacja z kartą (komunikaty: ATR, PPS, APDU). Bezpieczna transmisja danych pomiędzy kartą a czytnikiem. Kanały i protokoły logiczne. Łączenie terminali z systemami wyższego poziomu. Transmisja danych dla kart stykowych (warstwa transportowa, protokoły kart pamięci, protokoły transmisyjne T=0 i T=1, protokoły USB, MMC i SWP). Transmisja danych dla kart bezstykowych (sprzężenia indukcyjne i pojemnościowe, transfer zasilania, transfer danych, NFC, karty bezstykowe bliskiego i dalekiego zasięgu, karty zbliżeniowe). Programowanie KE (polecenia: plikowe, odczytu i zapisu, wyszukiwania, uwierzytelniania osób i urządzeń, kryptograficzne, zarządzania plikami i aplikacjami, kompletujące, testowania sprzętu, bazodanowe, transmisji danych). Polecenia związane z zastosowaniem karty (dla portmonetek elektronicznych, dla kart kredytowych i debetowych). Zarządzane plikami karty elektronicznej (struktura pliku, cykl życia pliku, typy plików, nazwy plików, wybór pliku, struktura pliku EF, warunki dostępu, atrybuty). Systemy operacyjne KE (podstawowe założenia i funkcje, przetwarzanie poleceń, zasady projektowania i implementacji, kompletowanie karty, organizacja i zarządzanie pamięcią, zarządzanie plikami, dostęp do zasobów, operacje atomowe, wielozadaniowość, wydajność, zarządzanie aplikacjami, kody narodowe). Typy systemów operacyjnych KE: JavaCard, Multos, BasicCard, Linux, Small-OS. Produkcja I zapewnienie jakości kart elektronicznych. Bezpieczeństwo kart elektronicznych (typy ataków, historia ataków, ataki i obrona w trakcie projektowania, produkcji i użytkowania). Czytniki kart elektronicznych (cechy fizyczne i elektryczne, interfejs użytkownika, interfejs aplikacji, bezpieczeństwo). Zastosowania KE w: systemach płatności, systemach telekomunikacyjnych, systemach służby zdrowia, systemach transportu, identyfikacji, paszportach, w zabezpieczeniach IT. Projektowanie aplikacji.

Zajęcia laboratoryjne prowadzone są w formie piętnastu 2-godzinnych ćwiczeń, odbywających się w laboratorium. Ćwiczenia podzielone są na dwie części. W pierwszej studenci wykonują kolejne ćwiczenia praktyczne zapoznając się z różnymi technologiami. Część ta kończy się testem sprawdzającym zdobytą wiedzę. Druga część związana jest z realizacją projektu praktycznego lub teoretycznego. Program laboratorium obejmuje następujące zagadnienia:

Obsługa następujących typów kart elektronicznych: JavaCard, SIM, BasicCard, .NET oraz legitymacja studencka. Szyfrowanie. Obsługę i przechowywanie na karcie kluczy szyfrujących i podpisu cyfrowego. Języki i techniki programowania kart elektronicznych. Zastosowania kart elektronicznych.

Metody dydaktyczne:

1. wykład: prezentacja multimedialna
2. ćwiczenia laboratoryjne: rozwiązywanie zadań, ćwiczenia praktyczne, zdanie o charakterze projektowym

Literatura podstawowa:

1. Smart Card Handbook, 4th edition, Rankl W., Effing W., Wiley, 2010
2. RFID Handbook, 3rd edition, Finkenzeller K., Wiley, 2010

Literatura uzupełniająca:

1. Smart Card Applications – Design models for programming and using smart cards. Rankl W., Wiley, 2007.
2. Java Card Technology for Smart Cards. Chen Z., Addison-Wesley, 2000.
3. Power Analysis Attacks: Revealing the Secrets of Smart Cards. Mangard S., Oswald E., Popp T., Springer, 2007
4. Normy, standardy i specyfikacje: ANSI, DIN, ISO/IEC, IEEE, RFC, RSA Inc., CEN, EMV, ETSI, FIPS, Global Platform, ITU, Java Card Platform, SEIS.
5. Czasopisma specjalistyczne
6. Internet

Bilans nakładu pracy przeciętnego studenta	
Czynność	**Czas**
1. udział w zajęciach laboratoryjnych / ćwiczeniach : 15 x 2 godz.,	30 godz.,
2. przygotowanie do ćwiczeń laboratoryjnych: 10 x 1 godz.,	10 godz.
3. realizacja projektu praktycznego (napisanie programu / programów, uruchomienie i weryfikacja) lub teoretycznego (zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi) (czas poza zajęciami laboratoryjnymi)	10 godz.
4. przygotowanie do sprawdzianów	5 godz.
5. udział w wykładach	30 godz.
6. przygotowanie do zaliczenia wykładów i udział w kolokwium zaliczeniowym	15 godz.

Obciążenie pracą studenta		
forma aktywności	**godzin**	**ECTS**
Łączny nakład pracy	100	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2÷3
Zajęcia o charakterze praktycznym	50	2