



<p>1. potrafi posługiwać się technikami informacyjno-komunikacyjnymi wykorzystywanymi przy realizacji kilkuosobowego projektu - [K2st_U2]</p> <p>2. 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 pozatechniczne - [K2st_U5]</p> <p>3. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych stosowanych w obszarze kart elektronicznych - [K2st_U6]</p> <p>4. potrafi poprawnie użyć wybraną metodę szacowania pracochłonności wytwarzania oprogramowania dla kart elektronicznych - [K2st_U7]</p> <p>5. potrafi ocenić przydatność metod i narzędzi służących do rozwiązania zadania inżynierskiego, polegającego na zaprojektowaniu z zaimplementowaniu pewnego oprogramowania dla karty elektronicznej, uwzględniając możliwości i ograniczenia systemów korzystających z kart elektronicznych - [K2st_U9]</p> <p>6. potrafi (zgodnie z zadaną specyfikacją, uwzględniającą aspekty pozatechniczne) zaprojektować oprogramowanie dla karty elektronicznej i zrealizować ten projekt (co najmniej w części) używając właściwych metod, technik i narzędzi - [K2st_U11]</p>
<p><b>Kompetencje społeczne:</b></p>
<p>1. .rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe - [K2st_K1]</p> <p>2. rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu informatyki w rozwiązywaniu problemów badawczych i praktycznych z zakresu kart elektronicznych2 - [K2st_K2]</p>

<p style="text-align: center;"><b>Sposoby sprawdzenia efektów kształcenia</b></p>
<p>Efekty kształcenia przedstawione wyżej weryfikowane są w następujący sposób:</p> <p>Ocena formująca:</p> <p>a)w zakresie wykładów:</p> <ul style="list-style-type: none"><li>- na podstawie odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach;</li></ul> <p>b) w zakresie laboratorium:</p> <ul style="list-style-type: none"><li>- na podstawie oceny bieżącego postępu realizacji zadań,</li></ul> <p>Ocena podsumowująca:</p> <p>a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez:</p> <p>ocenę wiedzy i umiejętności wykazanych na kolokwium pisemnym w formie testu. Test może składać się z 20 do 50 pytań otwartych jak i zamkniętych. W przypadku pytań zamkniętych jest to test wielokrotnego wyboru. Punktacja poszczególnych pytań podana jest będzie w treści pytania. Na ocenę 3,0 należy zdobyć co najmniej 50% punktów. Ocenę 3,5 można otrzymać za co najmniej 60% punktów, 4,0 za co najmniej 70% punktów itd.)</p> <p>b) w zakresie laboratoriów weryfikowanie założonych efektów kształcenia realizowane jest przez:</p> <ul style="list-style-type: none"><li>- 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 częściowa</li><li>- 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 częściowa</li><li>- wykonanie i obrona projektu ? trzecia ocena częściowa</li><li>- ocena końcowa wystawiana jest na podstawie trzech ocen częściowych</li></ul> <p>Uzyskiwanie punktów dodatkowych za aktywność podczas zajęć, a szczególnie za:</p> <ul style="list-style-type: none"><li>- omówienia dodatkowych aspektów zagadnienia,</li><li>- efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,</li><li>- umiejętność współpracy w ramach zespołu praktycznie realizującego zadanie szczegółowe w laboratorium,</li><li>- uwagi związane z udoskonaleniem materiałów dydaktycznych,</li><li>- wskazywanie trudności percepcyjnych studentów umożliwiające bieżące doskonalenia procesu dydaktycznego</li></ul>
<p style="text-align: center;"><b>Treści programowe</b></p>
<p>Program wykładu obejmuje następujące zagadnienia:</p> <p>RGeneza 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</p>

(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 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. Zszyfrowanie. 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, zadania o charakterze projektowym

#### Literatura podstawowa:

1. K. Mayes, K. Markantonakis (red.), Smart cards, tokens, security and applications (wyd. 2), Springer, 2017 (<https://link.springer.com/content/pdf/10.1007%2F978-3-319-50500-8.pdf>)
2. M. Kubas, M. Molski: Karta elektroniczna : bezpieczny nos?nik informacji, Mikom, 2002
3. W. Rankl, W. Effing: Smart card handbook (wyd. 4), Wiley, 2010
4. U. Hansmann, M. S. Nicklous, T. Schäck, A. Schneider, F. Seliger: Smart Card Application Development Using Java (wyd. 2), Springer 2012. (<https://link.springer.com/book/10.1007%2F978-3-642-55969-3>)

#### Literatura uzupełniająca:

1. www.smartcardbasics.com
2. S. Mangard, E. Oswald, T. Popp: Power analysis attacks: Revealing the secrets of smart cards, Springer, 2007 (<https://link.springer.com/content/pdf/10.1007%2F978-0-387-38162-6.pdf>)
3. S. A. Ahson, M Ilyas: Near Field Communications Handbook, Taylor & Francis, 2016 (<http://library.put.poznan.pl/do/access?TandFbooks9781420088151>)
4. K. Finkenzeller: RFID Handbook, (wyd. 3), Wiley, 20

#### Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w zajęciach laboratoryjnych:	30
2. przygotowanie do ćwiczeń laboratoryjnych	7
3. udział w wykładach	30
4. przygotowanie do zaliczenia wykładów i udział w kolokwium zaliczeniowym	5
5. udział w konsultacjach	2
6. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), ok. 50 stron	5

#### Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	79	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	62	2
Zajęcia o charakterze praktycznym	40	1