KARTA PRZEDMIOTU

Kod przedmiotu	**0613-2INF-F56-KRY**	
Nazwa przedmiotu w języku	polskim	***Kryptografia***
	angielskim	***Cryptography***

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	Informatyka
1.2. Forma studiów	stacjonarne
1.3. Poziom studiów	studia I-stopnia inżynierskie
1.4. Profil studiów	ogólnoakademicki
1.5. Osoba przygotowująca kartę przedmiotu	prof. UJK dr hab. Andrzej Chrzęszczyk
1.6. Kontakt	achrzesz@ujk.edu.pl

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Język wykładowy	polski
2.2. Wymagania wstępne	Analiza matematyczna Algebra liniowa

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć		wykłady, ćwiczenia laboratoryjne
3.2. Miejsce realizacji zajęć		zajęcia w pomieszczeniu dydaktycznym UJK
3.3. Forma zaliczenia zajęć		wykłady – zaliczenie z oceną, ćwiczenia laboratoryjne – zaliczenie z oceną projekt
3.4. Metody dydaktyczne		wykład, ćwiczenia w pracowni komputerowej
3.5. Wykaz literatury	**podstawowa**	1. Chrzęszczyk A., Algorytmy teorii liczb i kryptografii. BTC. Legionowo 2010 2. Koblitz N., Wykład z teorii liczb i kryptografii. WNT. Warszawa 1995
	uzupełniająca	1. Smart N., Cryptography: An Introduction, McGraw Hill 2002, www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf

4. CELE, TREŚCI I EFEKTY UCZENIA SIĘ

4.1. Cele przedmiotu

Wykład:

C1. Zapoznanie z podstawowymi metodami stosowanymi w kryptografii

Ćwiczenia laboratoryjne, projekt:

C1. Rozwijanie umiejętności implementacji algorytmów kryptograficznych i zastosowania zdobytej wiedzy z wykorzystaniem narzędzi komputerowych

4.2. Treści programowe

Wykład:

Funkcje skrótu i ich zastosowania. Kryptografia z kluczem symetrycznym. System AES. Kryptografia z kluczem publicznym. Wymiana kluczy Diffiego-Hellmana. Systemy RSA, Elgamal. Podpis cyfrowy DSA. Krzywe eliptyczne. Wymiana kluczy z wykorzystaniem krzywych eliptycznych - ECDH. Podpis cyfrowy z wykorzystaniem krzywych eliptycznych - ECDSA.

Ćwiczenia laboratoryjne

Funkcje skrótu i ich zastosowania. Kryptografia z kluczem symetrycznym. System AES. Kryptografia z kluczem publicznym. Wymiana kluczy Diffiego-Hellmana. Systemy RSA, Elgamal. Podpis cyfrowy DSA. Krzywe eliptyczne. Wymiana kluczy z wykorzystaniem krzywych eliptycznych - ECDH. Podpis cyfrowy z wykorzystaniem krzywych eliptycznych - ECDSA.

4.3. Przedmiotowe efekty uczenia się

Efekt	Student, który zaliczył przedmiot	Odniesienie do kierunkowych efektów uczenia się
w zakresie **WIEDZY:**		
W01	ma wiedzę na temat matematycznych podstaw kryptografii	INF1A_W01 INF1A_W07 INF1A_W12
W02	zna takie pojęcia kryptografii jak funkcje skrótu, szyfrowanie z kluczem symetrycznym, szyfrowanie z kluczem publicznym, podpis cyfrowy.	INF1A_W01 INF1A_W07 INF1A_W12
W03	rozumie znaczenie kryptograficznej ochrony wykorzystywanych danych	INF1A_W13-W14
w zakresie **UMIEJĘTNOŚCI:**		
U01	potrafi wykorzystać metody szyfrowania z kluczem symetrycznym i publicznym do ochrony danych oraz metody podpisu cyfrowego do potwierdzenia tożsamości	INF1A_U01
U02	potrafi realizować algorytmy szyfrowania i podpisu cyfrowego za pomocą wybranego języka programowania	INF1A_U10
U03	umie analizować problemy bezpieczeństwa informacji i rozwiązywać problemy z tym związane	INF1A_U16
w zakresie **KOMPETENCJI SPOŁECZNYCH:**		
K01	potrafi formułować i argumentować opinie dotyczące bezpieczeństwa informacji	INF1A_K02

4.4. Sposoby weryfikacji osiągniecia przedmiotowych efektów uczenia się

Efekty przedmiotowe *(symbol)*	Sposób weryfikacji (+/-)											
	Kolokwium			Zadania domowe			Zadania domowe					
	Forma zajęć			*Forma zajęć*			*Forma zajęć*					
	W	*L*	*P*	*W*	*L*	*P*	*W*	*L*	*P*			
W01	+											
W02	+											
W03	+											
U01		+			+			+				
U02		+			+			+				
U03		+			+			+				
K01		+			+			+				

4.5. Kryteria oceny stopnia osiągniecia efektów uczenia się

Forma zajęć	Ocena	Kryterium oceny
wykład (W)	**3**	osiągnięcie <50-60) % wymogów stosowanych w metodach oceny
	3,5	osiągnięcie <61-70) % wymogów stosowanych w metodach oceny
	4	osiągnięcie <71-80) % wymogów stosowanych w metodach oceny
	4,5	osiągnięcie <81-90) % wymogów stosowanych w metodach oceny
	5	osiągnięcie <91-100> % wymogów stosowanych w metodach oceny
laboratorium (L)	**3**	osiągnięcie <50-60) % wymogów stosowanych w metodach oceny
	3,5	osiągnięcie <61-70) % wymogów stosowanych w metodach oceny
	4	osiągnięcie <71-80) % wymogów stosowanych w metodach oceny
	4,5	osiągnięcie <81-90) % wymogów stosowanych w metodach oceny
	5	osiągnięcie <91-100> % wymogów stosowanych w metodach oceny
projekt (P)	**3**	osiągnięcie <50-60) % wymogów stosowanych w metodach oceny
	3,5	osiągnięcie <61-70) % wymogów stosowanych w metodach oceny
	4	osiągnięcie <71-80) % wymogów stosowanych w metodach oceny
	4,5	osiągnięcie <81-90) % wymogów stosowanych w metodach oceny
	5	osiągnięcie <91-100> % wymogów stosowanych w metodach oceny

BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta	
	Studia stacjonarne	**Studia niestacjonarne**
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/		
Udział w wykładach	30	
Udział w laboratoriach	30	
Udział w konsultacjach		
*Udział w egzaminie/kolokwium zaliczeniowym**		
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/		
*Przygotowanie do wykładu**	20	
Przygotowanie do laboratorium	20	
*Przygotowanie do egzaminu/kolokwium**		
Zebranie materiałów do projektu	25	
*Opracowanie prezentacji multimedialnej**		
*Inne (należy wskazać jakie? np. e-learning pod kontroli nauczyciela)**		
ŁĄCZNA LICZBA GODZIN	***125***	
PUNKTY ECTS za przedmiot	**5**	

niepotrzebne usunąć

Przyjmuję do realizacji *(data i czytelne podpisy osób prowadzących przedmiot w danym roku akademickim)*

.....