<table>
<tr><td>Nazwa modułu kształcenia</td><td colspan="3">Kryptologia</td></tr>
<tr><td>Nazwa jednostki prowadzącej moduł</td><td colspan="3">Instytut Informatyki,
Wydział Matematyki i Informatyki</td></tr>
<tr><td>Kod modułu</td><td colspan="3">WMI.II-K-OL</td></tr>
<tr><td>Język kształcenia</td><td colspan="3">Polski</td></tr>
<tr><td>Efekty kształcenia dla modułu kształcenia</td><td colspan="3"><table>
<tr><td>Symbol</td><td>Efekty kształcenia</td><td>Odniesienie do efektów kierunkowych</td></tr>
<tr><td>E1</td><td>zna podstawowe pojęcia, zasady i metody kryptografii i kryptoanalizy</td><td>K_W01++, K_W02++</td></tr>
<tr><td>E2</td><td>Potrafi projektować i implementować podstawowe kryptosystemy</td><td>K_U01++, K_U02++,</td></tr>
<tr><td>E3</td><td>zna podstawowe pojęcia, własnosci, i algorytmy teorii liczb</td><td>K_W07++, K_W01++</td></tr>
<tr><td>E4</td><td>zna podstawowe pojęcia, własności i algorytmy kryptografii klucza publicznego</td><td>K_W07++, K_U03++, K_W15++,</td></tr>
<tr><td>E5</td><td>Potrafi projektować i implementować podstawowe kryptosystemy klucza publicznego</td><td>K_U01++, K_U03++</td></tr>
<tr><td>E6</td><td>zna podstawowe pojęcia, własności i protokoły wykorzystujące kryptografię klucza publicznego</td><td>K_U01++, K_U02++, K_U03++,</td></tr>
</table></td></tr>
<tr><td>Typ modułu kształcenia (obowiązkowy/fakultatywny)</td><td colspan="3">obowiązkowy dla kierunku informatyka, specj. stosowana, studia I stopnia/ fakultatywny dla innych specjalności</td></tr>
<tr><td>Rok studiów</td><td colspan="3">2</td></tr>
<tr><td>Semestr</td><td colspan="3">1</td></tr>
<tr><td>Imię i nazwisko osoby/osób prowadzących moduł</td><td colspan="3">dr hab. Wit Foryś</td></tr>
<tr><td>Imię i nazwisko osoby/osób egzaminującej/egzaminujących bądź udzielającej zaliczenia, w przypadku gdy nie jest to osoba prowadząca dany moduł</td><td colspan="3">dr hab. Wit Foryś</td></tr>
<tr><td>Sposób realizacji</td><td colspan="3">wykład, ćwiczenia</td></tr>
<tr><td>Wymagania wstępne i</td><td colspan="3">Wstęp do teorii mnogości, Algebra liniowa</td></tr>
</table>

dodatkowe	
Liczba godzin zajęć dydaktycznych wymagających bezpośredniego udziału nauczyciela akademickiego i studentów, gdy w danym module przewidziane są takie zajęcia	**60**
Liczba punktów ECTS przypisana modułowi	**6**
Bilans punktów ECTS	Udział w wykładach – 30 godz. Udział w cwiczeniach – 30 godz. Samodzielne rozwiązywanie zadań tablicowych (deklarowanych) – 20 godz. Samodzielne rozwiązywanie zadań z prog. MATHEMATICA – 20 godz Przygotowanie do kolokwiów oraz obecność na kolokwiach – 30 godz. Przygotowanie do egzaminu oraz obecność na egzaminie – 30 godz. Łączny nakład pracy studenta: 160 godzin , co odpowiada 6 punktom ECTS
Stosowane metody dydaktyczne	1. Wykład ilustrowany prezentacją komputerową. 2. materiały umieszczone w sieci 3. Ćwiczenia laboratoryjne i tablicowe. 4. Deklaracja rozwiązanych zadań umieszczonych w sieci.
Metody sprawdzania i oceny efektów kształcenia uzyskanych przez studentów	Kolokwia (E1, E2, E3, E4, E5, E6) Egzamin (E1, E2, E3, E4, E5, E6) Samodzielne rozwiązywanie zadań z progr MATHEMATICA i tablicowych (E1, E2, E3, E4, E5, E6) Samodzielne rozwiązywanie zadań deklarowanych
Forma i warunki zaliczenia modułu, w tym zasady dopuszczenia do egzaminu, zaliczenia, a także forma i warunki zaliczenia poszczególnych zajęć	Student otrzymuje ocenę końcowa z ćwiczeń na podstawie punktów przyznawanych za systematycznie deklarowane zadania, rozwiązywanie zadań przy pomocy prog. MATHEMATICA, tablicowych i aktywność oraz punktów uzyskanych na kolokwiach Warunkiem otrzymania zaliczenia ćwiczeń jest uzyskanie określonej liczby punktów Student otrzymuje ocenę końcową z modułu na podstawie punktów przyznawanych na ćwiczeniach oraz

wchodzących w zakres danego modułu	punktów uzyskanych podczas egzaminu pisemnego.
Treści modułu kształcenia	Klasyczne (symetryczne) kryptosystemy monoalfabetyczne i polialfabetyczne (kryptosystem Cezara, Hilla, afiniczny, Vigenere'a, Beauforta, Playfaira); twierdzenia i algorytmy z arytmetyki modularnej i podstaw teorii liczb Maszyny rotorowe – ENIGMA; podstawy teoretyczne; historia; tw. które rozstrzygnęło II wojnę światową DES, schemat Feistela; kryptoanaliza różnicowa; metody probabilistyczne (3 godz.) AES; elementy ciał Galois Idea klucza publicznego, funkcje jednokierunkowe ; problem plecakowy i kryptosystem plecakowy Algorytm Shamira przełamania kryptosystemu plecakowego, elementy teorii krat i algorytm LLL; tw. uzasadniajace poprawność RSA Liczby pseudopierwsze - testy pierwszości: Fermata, Solovaya-Strassena, Millera-Rabina; Problemy faktoryzacji; algorytm oparty na krzywych eliptycznych; podstawy teorii krzywych eliptycznych Logarytm dyskretny i przydzielanie kluczy; ciała Galois cd. ; kryptosystem Rabina, ElGamala, McEliece; podpis elektroniczny - wykorzystanie RSA Krzywe eliptyczne; kryptografia na krzywych eliptycznych część I Krzywe eliptyczne; kryptografia na krzywych eliptycznych część II Protokół kryptograficzny – wprowadzenie; Rzut monetą przez telefon; poker telefoniczny Częściowe odkrywanie sekretu; Dowody o wiedzy zerowej
Wykaz literatury podstawowej i uzupełniającej, obowiązującej do zaliczenia danego modułu	Moduł ma charakter autorski, obowiązuje przede wszystkim materiał wyłożony, literatura ma charakter pomocniczy. Literatura podana jest na początku wykładu i wskazywana na bieżąco w trakcie wykładu. [1] N.Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa, 1995 [2] R.A.Mollin, RSA and Public-Key Cryptography, Chapman_Hall CRC, 2003 [3] B. Schneier, Applied cryptography, John Wiley&Sons, 1994 [3] W.Trappe, L.C.Washington, Introduction to cryptography with Coding Theory, Prentice Hall, 2002 [4] L.C.Washington, Elliptic Curves, Number Theory and Cryptography, Chapman_Hall CRC, 2003 [5] Internet - strony www wskazane na wykładzie
Metody i kryteria oceniania	Student jest oceniany na podstawie punktów uzyskanych na ćwiczeniach – zadania przy wykorzystaniu prog. MATHEMATICA oraz tablicowe - zadania deklarowane - kolokwiów i egzaminu.

	Skalę ocen ustala wykładowca.
Wymiar, zasady i forma odbywania praktyk, w przypadku, gdy program kształcenia przewiduje praktyki	Nie dotyczy