

Syllabus do przedmiotów:
Kryptografia z elementami algebry 06-DKALLI0
Cryptography with elements of algebra 06-DKALLI0-E

1. Podstawy teoretyczne
 - a. Kryptologia:
 - i. Podstawy protokołów: symetryczny, asymetryczny i hybrydowy protokół szyfrowania.
 - ii. Operacje elementarne na bitach.
 - iii. Złożoność obliczeniowa i związek z bezpieczeństwem.
 - iv. Algorytmy czasu wielomianowego i wykładniczego.
 - v. Funkcje jednokierunkowe. Algorytm Shora.
 - b. Algebra:
 - i. Arytmetyka modularna.
 - ii. Ciała skończone, pierścienie skończone.
 - iii. Wstęp do teorii grup.
2. Szyfrowanie symetryczne:
 - a. Szyfry blokowe: AES, DES.
3. Szyfrowanie asymetryczne:
 - a. RSA.
 - b. ElGamal/Diffie-Hellman.
 - c. Eliptyczny ElGamal/Diffie-Hellman.
4. Algorytmy post-kwantowe (jeden z kilku do wyboru)
 - a. Systemy kryptograficzne oparte na izogeniach.
 - b. Kryptosystem NTRU.
 - c. Kryptosystem McEllice.
 - d. Kryptografia na grupach nieprzemiennej (grupy macierzowe, grupy warkoczy).

Implementacje na zajęciach:

1. Algorytm potęgowania i szybkiego potęgowania.
2. Rozszerzony algorytm Euklidesa i znajdowanie odwrotności w pierścieniu reszt liczb całkowitych i pierścienia wielomianów.

Rekomendowana literatura do przedmiotu:

1. Koblitz: Wykład z teorii liczb i kryptologii.
2. Hoffstein, Pipher, Silverman: An introduction to mathematical cryptography
3. Rubinstein-Salzedo: Cryptography

Zaliczenie przedmiotu:

1. **Wykład:** egzamin (warunkiem przystąpienia jest zaliczenie ćwiczeń)
2. **Ćwiczenia: (100 pkt)**
 - a. **Projekt:** (każdy moduł ma ustalony termin doręczenia, po terminie nie są przyznawane punkty)
 - i. (10 pkt) Moduł 1: implementacja arytmetyki
 - ii. (10 pkt) Moduł 2: implementacja struktury algebraicznej
 - iii. (20 pkt) Moduł 3: implementacja kryptosystemu opartego na strukturze alg.
 - iv. (30 pkt) Moduł 4: stworzenie systemu hybrydowego
 - b. **Test wiedzy:** trzy testy, każdy po 10 pkt. (możliwość ich zaliczenia tylko we wskazanym terminie)
 - c. **Zaliczenie (progi):** 60% dst (3), 75% dst+ (3.5), 80% db (4), 85% db+ (4.5), 90% bdb (5).