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).