Propozycje tematów projektowych:

1. **Funkcje KDF (Key-derivation Functions): Algorytmy, demonstracje działania.**

2. **Szyfrowanie w pełni homomorficzne (*Fully Homomorphic Encryption*), implementacja, istniejące biblioteki, praktyczne zastosowania.**

3. Kryptografia krzywych eliptycznych – stworzenie materiałów dydaktycznych, prezentacja idei, demonstracja działań, zastosowanie w kryptografii, biblioteki programistyczne.

4. Kryptograficzne generatory liczb – przegląd, prezentacja sposobów działania, dostępne implementacje

5. Technologia blockchain – zastosowania inne niż kryptowaluty, istniejące zastosowania, pomysłu na przyszłość, propozycje

6. ,,Chaotyczna'' kryptografia. Kryptografia wykorzystując teorię chaosu (deterministyczny chaos). Zastosowania. Algorytmy. Demonstracje.

7. eVoting: wykorzystanie kryptografii do głosowania elektronicznego. Przegląd rozwiązań protokołów, realizacja dla potrzeb dydaktycznych.

8. Kryptografia postkwantowa oparta na kratach (*lattice-based cryptography*), przegląd koncepcji, istniejące implementacje, testy funkcjonalności.

9. Kryptografia postkwantowa oparta na funkcjach skrótu (*hash-based cryptography*), np. schemat podpisu Merkla. Przegląd koncepcji, implementacje przykłady użycia.

10. Kryptografia postkwantowa oparta o kody korekcyjne (*code-based cryptography*), np. system McEliece. Przegląd koncepcji, implementacje, przykłady użycia.

11. Kryptografia postkwantowa oparta o isogenie (*isogeny*). Przegląd koncepcji, implementacje, przykłady użycia.

12. Karty smartcard w kryptografii – wykorzystanie kart inteligentnych w połączeniu z kryptografią.

13. Algorytmy faktoryzacji liczb całkowitych, demonstracje dydaktyczne, implementacje.

14. Kryptografia z wykorzystaniem liczb całkowitych Gaussa (liczby zespolone o części rzeczywistej i urojonej ze zbioru liczb całkowitych). Możliwe zastosowania. Algorytmy. Demonstracje.

15. Kryptosystemy progowe (*threshold cryptosystem*): idea, demonstracja działania.

16. Kody uwierzytelniania wiadomości (*MAC, Message Authentication Code*) : przegląd, opis, demonstracje dydaktyczne.

17. *Identity-based cryptography.* Idea. Zastosowania. Algorytmy. Demonstracja.

18. Lekka kryptografia, kryptografia dla IoT, *lightweight cryptography:* przegląd algorytmów, implementacje demonstracyjne.

19. *Honey encryption.* Algorytmy, implementacje, demonstracja.