Politechnika Warszawska

Wydział Fizyki

Kryptografia i bezpieczeństwo informacji dla fizyków

Sprawozdanie z zadania nr. 5 na temat:

**Kryptografia krzywych eliptycznych**

Data wykonania zadania w laboratorium: 19.11.2019r.

**Wykonali:**

Maciej Czarnecki

Denys Morokov

Fizyka techniczna II stopień, 2 rok

1. **Wstęp**
   1. **Cel:** celem zadania jest napisanie prostego programu szyfrującego zawartość przy użyciu krzywych eliptycznych z użyciem wybranej biblioteki kryptograficznej. Program ma umożliwiać ustawienie własnych parametrów dla EC. Należy ustawić parametry inne niż domyślne dla biblioteki ale prawidłowe dla EC.
   2. **Wykorzystana technologia:** skrypt został zaimplementowany w Python.
2. **Opracowanie wyników**
3. **Podsumowanie**

Zaimplementowano metodę batchGCD. Dla wybranych kluczy publicznych nie udało się uzyskać private key.