Завдання на контрольну роботу з дисципліни

 "Сучасна криптографія "

Скласти криптографічний протокол:

1. Передачі даних (ЕЦП) на основі асиметричного шифрування.

2. Ідентифікації користувача системи на основі ЕЦП.

3. Ідентифікації користувача системи на основі хеш-функції.

4. Передачі даних (хеш-коду).

5. Шифрування даних на основі хеш-функції.

6. Шифрування даних на основі ЕЦП.

7. Автентифікації пароля на основі хеш-функції.

8. Ідентифікації користувача системи на основі розділення секрету (знання з нульовим розголошенням).

9. Передачі даних (ключової інформації або зашифрованого повідомлення).

10. Шифрування даних на основі симетричного алгоритму.

11. Шифрування даних на основі асиметричного алгоритму.

12. Автентифікації пароля на основі асиметричного алгоритму.

13. Автентифікації (перевірки) ключа на основі асиметричного алгоритму.

14. Ідентифікації користувача системи на основі асиметричного алгоритму.

Кожен крок протоколу представити в описовій формі та формально.