

**Системи безпеки програм і даних.  
КР№1-2. ABCD – цифри заліковки.**

**1. Конфіденційність. Цілісність. Доступність (2 бали).**

- Напишіть есе (200-500 знаків), щодо основних проблеми безпеки програм і даних, опишіть, як розумієте авторизацію та аутентифікацію, можна навести приклад.

**2. За допомогою сайту [jwt.io](https://jwt.io) створить JWT токен з наступними клеймами (2 бали):**

- name - ім'я та прізвище;
- sub (subject) – email;
- iat (issued at time) – час, коли токен було створено;
- exp (expiration time) – час, коли токен стане не валідним.

**3. Назвіть приклади алгоритмів та надайте пояснення, для чого вони можуть використовуватись (6 балів):**

- Вільне кодування\декодування інформації. Закодуйте повідомлення, яке містить наступний текст: емейл-адреса.
- Симетричні алгоритми шифрування. Зашифруйте і розшифруйте повідомлення, яке містить цифри ABCD.
- Асиметричні алгоритми шифрування. Згенеруйте відкритий і секретні ключі. Зашифруйте і розшифруйте повідомлення, яке містить цифри ABCD.
- Односторонні хеш функції. Згенеруйте хеш для повідомлення, яке містить наступний текст: емейл-адреса.

**4. Опишіть, що таке uuid та для чого його використовують (4 бали):**

- Які версії знаєте?
- Згенеруйте приклади.

**5. Перерахуйте основні grant types у OAuth2 протоколи (4 бали).**

- Дайте стислий опис, для чого вони використовуються.
- Наведіть приклади.

**6. Назвіть який формат даних використовується для передачі інформації в SAML протоколі (2 бали)?**

- Стисло опишіть, як ви розумієте різницю SP-initiated, IDP-initiated підходах SAML.

Оформіть відповідь у вигляді одного файлу:  
CW\_Ix9x\_ПрізвищеІм'яПобатькові.pdf

**Консультації:** telegram @avolokyta та в чатах лабораторних робіт.