

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
НН Фізико-технічний інститут
Дисципліна: “Методи реалізації криптографічних механізмів”

ЛАБОРАТОРНА РОБОТА №3

Виконали:
Студенти групи ФБ-21мн

ЩЕРБАКОВ О.К.
КАЗМІДІ І.Д.

Завдання

1. Розробка реалізацій IT-систем (Реалізація Web-сервісу електронного цифрового підпису).

Розв'язок

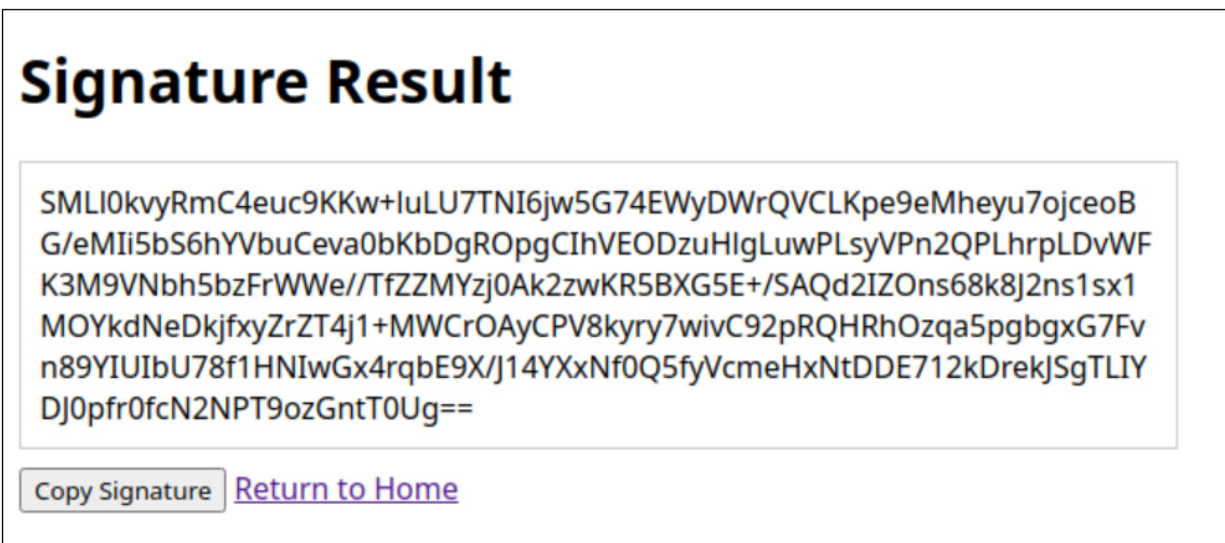
На [Малюнок 1-4] можна побачити “шлях” виконання завдань, зазначених у методичних вказівках. Код програми можна знайти за посиланням

(<https://drive.google.com/drive/folders/11HUk-Ab5Yf9MK3iaFFG8zzalaCDuUhg r?usp=sharing>).



The screenshot shows a web interface titled "Generate and Verify Digital Signature". It contains two main input sections. The first section has a text input field with the placeholder "text" and a button labeled "Create Signature". The second section has an input field with the placeholder "Enter your message" and a button labeled "Verify Signature". There is also a placeholder "Enter signature" next to the "Verify Signature" button.

Малюнок 1: Заповнення форми для створення ЕЦП



The screenshot shows a web interface titled "Signature Result". It displays a long alphanumeric string representing a digital signature: SMLI0kvyRmC4euc9KKw+luLU7TNI6jw5G74EWyDWrQVCLKpe9eMheyu7ojceoB G/eMIi5bS6hYVbuCeva0bKbDgROpgCIhVEODzuHlgLuwPLsyVPn2QPLhrpLDvWF K3M9VNbh5bzFrWWe//TfZZMYzj0Ak2zwKR5BXG5E+/SAQd2IZOns68k8J2ns1sx1 MOYkdNeDkjfyZrZT4j1+MWCrOAyCPV8kyry7wivC92pRQHRhOzqa5pgbgxG7Fv n89YIUIbU78f1HNIwGx4rqbE9X/J14YXxNf0Q5fyVcmeHxNtDDE712kDrekJSgTLIY DJ0pfr0fcN2NPT9ozGntT0Ug==. Below the signature, there is a button labeled "Copy Signature" and a link labeled "Return to Home".

Малюнок 2: ЕЦП для повідомлення “text”

Generate and Verify Digital Signature

Enter your message	Create Signature	
text	SMLl0kvyRmC4euc9KKw+luLU7	Verify Signature

Малюнок 3: Верифікація повідомлення та відповідного підпису

Verification Result

Correct	Back
---------	------

Малюнок 4: Результат верифікації