



Міністерство освіти і науки України  
КПІ ім. Ігоря Сікорського

**Звіт**

З дисципліни “Безпека інформаційних систем”  
студента III курсу ФІОТ  
групи ІК-12  
**Логвіна Максима**

Перевірив:  
Викладач кафедри  
Інформаційних систем та технологій  
Шимкович Л.Л.

Київ 2023

## Тема 7. Система цифрового підпису DSA

### Частина 1. Тестування

Тестирование

Вопрос

К каким видам шифров относится алгоритм ЭЦП?


Варианты ответов:


- ☒ асимметричным
- ☐ симметричным
- ☐ гибридным


Верных ответов: 0

Неверных ответов: 0

Всего вопросов 10

Осталось:  16 сек.

 Далее

 Закончить

Тестирование

Вопрос

Для чего используется алгоритм ЭЦП?


Варианты ответов:


- ☐ для шифрования/дешифрования сообщений
- ☒ для проверки целостности сообщения
- ☐ для передачи секретного ключа по каналу


Верных ответов: 1

Неверных ответов: 0

Всего вопросов 9

Осталось:  14 сек.

 Далее

 Закончить

Вопрос

Почему схема Эль-Гамаль является одной из самых распространенных схем ЭЦП?

Варианты ответов:



- ☐ схема не использует хеш-сумму
- ☒ схема имеет хорошую скорость вычисления
- ☐ схема содержит только операции сложения и умножения

Верных ответов: 2

Осталось:  14 сек.

Неверных ответов: 0

Всего вопросов 8

 Далее Закончить


Вопрос

Кто знает секретный ключ  $x$ ?

Варианты ответов:



- ☐ абонент, получающий документ
- ☒ абонент, подписывающий документ
- ☐ абонент, не имеющий отношения к документу

Верных ответов: 3

Осталось:  13 сек.

Неверных ответов: 0

Всего вопросов 7

 Далее Закончить


Вопрос

Для чего служит секретный ключ  $x$ ?

Варианты ответов:



- ☐ для аутентификации документа
- ☒ для получения открытого ключа
- ☐ для вычисления хеш-суммы

Верных ответов: 4

Осталось:  15 сек.

Неверных ответов: 0

Всего вопросов 6

 Далее Закончить


Вопрос

На каком этапе проверки можно узнать число  $x$ ?

Варианты ответов:



- ☐ при аутентификации
- ☒ ни на каком
- ☐ при передаче по открытому каналу

Верных ответов: 5

Осталось:  16 сек.

Неверных ответов: 0

Всего вопросов 5

 Далее Закончить

Вопрос

Каким должно быть число  $a$  по отношению к  $p$ ?

Варианты ответов:


- ☐ больше  $p$
- ☒ меньше  $p$
- ☐ не имеет значения

Верных ответов: 6

Осталось:  13 сек.

Неверных ответов: 0

Всего вопросов 4

 Далее Закончить


Вопрос

Каким должно быть число  $k$  по отношению к  $p$ ?

Варианты ответов:


- ☒ не имеет значения
- ☐ меньше  $p$
- ☐ больше  $p$

Верных ответов: 7

Осталось:  16 сек.

Неверных ответов: 0

Всего вопросов 3

 Далее Закончить

Тестирование

Вопрос

По какой формуле вычисляется открытый ключ?

Варианты ответов:

☒  $a^x \bmod p$

☐  $a^k \bmod p$

☐  $a^h \bmod p$

Верных ответов:

8

Неверных ответов:

0

Всего вопросов

2

Осталось:  15 сек.

Далее

Закончить

Тестирование

Вопрос

Что означает равенство значений  $u = v$ ?

Варианты ответов:

☐ документ сфальсифицирован

☒ подпись верна

☐ не имеет значения

Верных ответов:

9

Неверных ответов:

0


Всего вопросов

1

Осталось:  14 сек.


Далее

Закончить

 Итог тестирования ✕

Количество верных ответов:	10	(100 %)
Количество неверных ответов:	0	(0 %)

Оценка: 5


 Продолжить

## Частина 2. Перевірка підпису

Введите текст ✕

Введите текст сообщения:

Подпись

 Продолжить

## Отправитель

Хеш-сумма исходного текста:

8B276AF88D4CB73B78879914C141266D

$h = 49485$ , hex:9914 (разряды 12-11-10-9)

Число  $p =$



Генерировать

$p$  - простое число, размером от 128 до 256

Число  $a =$



Генерировать

$a$  - любое число, меньше  $p$  и больше 2

Число  $k =$





Генерировать

$k$  - любое число, размером от 2 до 32



Передать данные



Свободный доступ	Получатель
Параметры: $a = 35$ $p = 167$	Хеш-сумма полученного текста: 8B276AF88D4CB73B78879914C141266D $h = 49485$ , hex:9914 (разряды 12-11-10-9)
Открытый ключ $b =$ <input type="text" value="33"/>	Введите число $u$ : <input type="text" value="39"/>
Текст сообщения: Подпись	$u = (b^r) * (r^s) \mod p$
Введите число $r$ : <input type="text" value="13"/>	Введите число $v$ : <input type="text" value="39"/>
$r = a^k \mod p$	$v = a^h \mod p$
Число $s =$ <input type="text" value="109"/>	 Проверить подпись
	 Выход

