Лабораторна робота №3

Програмна реалізація MD 5, SHA 3 і ДСТУ 7564:2014.

*Мета роботи:* створити програму, яка обчислює профіль початкового тексту. Надалі програму можна використати для виконання лабораторної роботи при реалізації електронного цифрового підпису(ЭЦП).

**Завдання до роботи**

Програмна реалізація має бути оформлена як деяка програмна оболочка, яка

включає два алгоритми MD 5, SHA 3 і ДСТУ 7564:2014 для обчислення профілю початкової інформації.

Підготувати звіт по роботі. У звіті описати алгоритми MD 5, SHA 3 і ДСТУ 7564:2014 описати структуру алгоритмів. Представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій. Підготувати для демонстрації програми контрольний приклад.

Контрольні запитання

1.Основне призначення хеш-функції ?

2. Перерахувати клас завдань, які вирішуються із застосуванням хеш-функції.

3. Перерахувати, які основні властивості повинна мати хеш-функція.

4. Довжина вхідного блоку у бітах для функції стискування алгоритму.

5. Назвати число раундів в алгоритмі.

6. Назвати число кроків в кожному раунді алгоритму.

7.Назвати, які операції використовуються у функції стискування алгоритму MD 5.

8. Перерахувати основні постійні дані, які використовуються в алгоритмі MD 5.

9. Скільки примітивних функцій використовуються в алгоритмі MD 5?

10. Назвати, які операції використовуються у функції стискування алгоритму SHA 3.

11. Перерахувати основні постійні дані, які використовуються у алгоритмі SHA 3.

12. Назвати число раундів в алгоритмі SHA 3.

13. Скільки примітивних функцій використовуються в алгоритмі SHA 3?

14. Довжина вхідного блоку у бітах для функції стискування алгоритму SHA 3.

15. Число кроків в кожному раунді алгоритму SHA 3.

16. Назвати, які операції використовуються у функції стискування алгоритму ДСТУ 7564:2014.

17. Перерахувати основні постійні дані, які використовуються у алгоритмі ДСТУ 7564:2014.

18. Назвати число раундів в алгоритмі ДСТУ 7564:2014.

19. Скільки примітивних функцій використовуються в алгоритмі ДСТУ 7564:2014?

20. Довжина вхідного блоку у бітах для функції стискування алгоритму ДСТУ 7564:2014.

21. Число кроків в кожному раунді алгоритму ДСТУ 7564:2014.