1. Дать определение хеш-функции.

2. Что такое ≪однонаправленность≫ хеш-функций и какова роль

этого свойства хеш-функций в криптографии?

3. Что такое ≪коллизия≫? Типы коллизий хеш-функций.

4. Сформулировать в общем виде парадокс ≪дней рождений≫.

5. Как парадокс ≪дней рождений≫ используется в криптографии?

6. Сколько попыток нужно сделать, чтобы с вероятностью более

0,5 (0,7; 0,8; 0,9) обнаружить коллизию при длине хеша (l) 64 (128;

256; 512) бит?

7. Дать общую характеристику алгоритмам хеширования семейств MD и SHA. Из каких основных стадий состоит алгоритм хеширования сообщения?

8. Рассчитать общую длину (L') хешируемого сообщения после

предварительной стадии на основе алгоритма MD, если объем (L) ис-

ходного сообщения составлял: 0; 484; 512; 1000; 2000; 16000 бит. Ка-

кова в каждом случае будет длина хеша?

9. Входное сообщение (прообраз) состоит из

а) вашего имени,

б) ваших фамилии\_имени\_отчества (алфавит – на свой выбор).

Используя представление сообщения в кодах ASCII, представить

в табличной форме (как выше в примере 5) содержание каждого 32-

битного подблока расширенного входного сообщения.

10. Представить и охарактеризовать структурную схему одного

раунда алгоритмов хеширования на основе MD4; MD5; SHA-1.

11. На чем основан ≪лавинный эффект≫ в алгоритмах хеширова-

ния. В чем состоит цель его реализации.

12. В чем состоят основные структурные и функциональные осо-

бенности алгоритма хеширования SHA-3?

13. Охарактеризовать структурные, функциональные особенности

и криптостойкость белорусского государственного стандарта хеширо-

вания (СТБ 34.101.77-2016).