**Темы контрольных работ по дисциплине «Электронная цифровая подпись»**

Контрольная работа структурно состоит из двух теоретических вопросов и задачи. Номер первого вопроса определяется последней цифрой зачётки; 2-й вопрос – путём прибавления к номеру первого вопроса 9.

**Теоретические вопросы**

1. Структурные составляющие организационной основы системы обеспечения информационной безопасности Российской Федерации.
2. Условия использования электронной цифровой подписи.
3. Необходимость использования средств аутентификации в системах электронной коммерции на основе электронных цифровых подписей.
4. Способы и приемы несанкционированного доступа и модификации электронных документов в электронной коммерции.
5. Назначение хэш-функции, условия необходимости и достаточности, принцип построения хэш-функции, алгоритмы безопасного хэширования.
6. Принцип построения хэш-функции на основе симметричных блочных алгоритмов.
7. Отечественный стандарт хэш-функции.
8. Характеристика и сравнительный анализ между отечественными криптографическими системами аутентификации электронных документов.
9. Технология формирования открытых и закрытых ключей аутентификации электронных документов.
10. Требования к формированию ключевой информации на сменных носителях.
11. Как вычисляется функция Эйлера, ее физико-математический смысл?
12. Как формируются открытые и закрытые ключи для формирования и проверки ЭЦП?
13. Что представляет собой ЭЦП в алгоритме RSA и как производится аутентификация электронного сообщения?
14. Какие множества параметров в системе аутентификации электронных сообщений в алгоритме RSA являются открыто распределяемыми, а какие секретными?
15. Условия задания числового значения закрытого ключа КЗ и его функциональное назначения в алгоритме электронной подписи Эль Гаиаля?
16. Каким образом производится вычисление открытого ключа КО и его функциональное назначение в алгоритме Эль Гамаля?
17. Математическая модель процессов формирования электронной подписи и аутентификации электронного документа в алгоритме Эль Гамаля.
18. Обмен открытыми ключами шифрования данных и аутентификации электронной цифровой подписи в сетевых компьютерных корпоративных системах. Импортирование открытых ключей.
19. Формирование электронных цифровых подписей открытых электронных сообщений, передача электронного документа по системам теледоступа к вычислительным ресурсам, аутентификация принятого электронного документа.
20. Шифрование открытого электронного сообщения, передача по каналам теледоступа, дешифрование принятой криптограммы получателем.

**Задачи**

1. Вычислить модуль, функцию Эйлера и закрытый ключи ЭЦП при следующих условиях: - число Р = 23; число Q = 47; Ко = 37. На основании полученных данных вычислить значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
2. По заданным исходным данным Р=23, G =7, Кз = 2 вычислить значение открытого ключа Ко и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
3. По заданным исходным данным Р=23, g =2, d =5, Кз = 4 вычислить значение открытого ключа Ко и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
4. Задана эллиптическая кривая Е7(2,6):Y2=X3+2X+6(mod7), задается случайная точка х=5. Определить две точки (x1,y1), (x2,y2), затем еще две точки путем вычисления композиции первых двух. Вычислить ЭЦП при хэш-значении h(m)=3.
5. Вычислить модуль, функцию Эйлера и закрытый ключи ЭЦП при следующих условиях: - число Р = 21; число Q = 45; Ко = 37. На основании полученных данных вычислить значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
6. По заданным исходным данным Р=23, G =7, Кз = 2 вычислить значение открытого ключа Ко и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
7. По заданным исходным данным Р=23, g =2, d =5, Кз = 4 вычислить значение открытого ключа Ко и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
8. Задана эллиптическая кривая Е7(2,6):Y2=X3+2X+6(mod7), задается случайная точка х=5. Определить две точки (x1,y1), (x2,y2), затем еще две точки путем вычисления композиции первых двух. Вычислить ЭЦП при хэш-значении h(m)=3.
9. По заданным исходным данным Р=23, g =2, d =5, Кз = 4 вычислить значение открытого ключа Ко и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «финансирование».
10. По заданным исходным данным Р=23, g =2, d =5, Кз = 4 вычислить значение открытого ключа Ко и значение ЭЦП для слова «кредитование», хэш-функция которого определиться как: 5; 13; 7; 3. Аутентифицировать слово «кредитование».