ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНОЕ УЧРЕЖДЕНИЕ КОЛЛЕДЖ СВЯЗИ № 54

ИМЕНИ П.М. ВОСТРУХИНА

|  |  |
| --- | --- |
| **РАССМОТРЕНО:**  Предметно-цикловой комиссией  ПЦК ОПД и ПМ специальности 10.02.02 Информационная безопасность телекоммуникационных систем  Протокол № \_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2017 г.  \_\_\_\_\_\_\_\_\_\_О.В. Пешкина | **УТВЕРЖДАЮ:**  **Заместитель директора по УР**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Бозрова И.Г.  от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2017 г. |

**Экзаменационные вопросы**

**По МДК02.01 «Криптографическая защита информации»**

**Специальность: «Информационная безопасность телекоммуникационных систем»**

**Для групп: ИТС 9-6, ИТС 9-7, ИТС11-5.**

**Преподаватель: Пешкина О.В.**

***Теоретические вопросы:***

1. Базовые криптографические понятия.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Классическая и математическая криптография.
4. Эпоха донаучной криптографии
5. Криптография ХХ века.
6. Симметричные криптосистемы
7. Шифрование методами замены (подстановки)и перестановки
8. Шифрование методом гаммирования.
9. Блочные и поточные криптосистемы.
10. Алгоритм симметричного шифрования DES
11. Алгоритм симметричного шифрования АES
12. Отечественный стандарт шифрования.
13. Асимметричные криптосистемы
14. Алгоритм Диффи-Хеллмана.
15. Алгоритм Эль-Гамаля
16. Алгоритм Шамира.
17. Алгоритм RSA
18. Схема электронной подписи
19. Алгоритм цифровой подписи DSA.
20. Алгоритм цифровой подписи RSA
21. Алгоритм цифровой подписи Эль-Гамаля
22. Инфраструктура открытых ключей PKI
23. Электронно-цифровая подпись
24. Отечественный стандарт цифровой подписи.
25. Основные методы стеганографии.
26. Принципы и методы компьютерной стеганографии.
27. Криптографические протоколы
28. Протоколы аутентификации.
29. Протоколы распределения ключей.
30. Разновидности криптографических протоколов
31. Протоколы электронной подписи
32. Банковские криптографические протоколы
33. Протоколы конфиденциальных вычислений
34. Отечественная криптография и инновации в ее сфере.
35. Нормативное обеспечение в области криптографической

защиты информации

1. Отечественные программные продукты криптографической защиты информации
2. Квантовая криптография.

***Практические вопросы:***

1. Сообщество пользователей ГОСТа 34.10-2012 имеют общие параметры q=11, p=67. Вычислить открытый ключ (y) и построить подпись для сообщения m при следующих секретных параметрах 𝑑=5, h=m=5, k=9
2. Для указанных открытых ключей (𝑄) пользователей ГОСТа 34.10-2012 с общими параметрами q=11, p=67 проверить подлинность подписанного сообщения 𝑄=64: (8;7,5)
3. Построить подпись RSA для сообщения m при следующих параметрах пользователя: p=3, q=11, y=7, m=35
4. Для указанного открытого ключа пользователя RSA проверить подлинность подписанных сообщений: n=33, x=3: (24,18)
5. Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами p=23, g=5. Для указанных секретных параметров абонентов найти открытый ключ (y) и построить подпись для сообщения m: x=9, k=19, m=h=25
6. Для указанных открытых ключей (y) пользователей системы Эль-Гамаля с общими параметрами p=23, g=5 проверить подлинность подписанных сообщений: y=11: [10,15,3]
7. Абоненты некоторой сети применяют цифровую подпись по алгоритму Эль-Гамаля с общими параметрами Р = 17, g = 3. Найдите открытый ключ абонента Петрова для Х = 11.
8. В системе связи, применяющей шифр Эль-Гамаля, пользователь 1 желает передать сообщение m пользователю 2. Найдите недостающие параметры при следующих заданных параметрах p = 23, g = 6, x = 9, k = 7, m = 13.
9. Для шифра Эль-Гамаля с заданными параметрами p= 19, g=2, x=11, k=4, m=10 найти недостающие параметры и описать процесс передачи сообщения m пользователю В.
10. В системе связи, применяющей шифр Эль-Гамаля, пользователь 1 желает передать сообщение m пользователю 2. Найдите недостающие параметры при следующих заданных параметрах p = 19, g = 2, x= 3, k = 5, m = 10
11. Вычислить общий и секретный ключ для системы Диффи-Хеллмана с параметрами n=11, q=7, x=3, y=9
12. Вычислите закрытые ключи  и общий ключ  для системы Диффи-Хеллмана с параметрами n=3, q=7, x=3, y=6
13. Вычислите закрытые ключи  и общий ключ  для системы Диффи-Хеллмана с параметрами n=19, q=10, x=4, y=8
14. Вычислить общий и секретный ключ для системы Диффи-Хеллмана с параметрами n=21, q=2, x=11, y=15

Преподаватель \_\_\_\_\_\_\_\_\_ О.В. Пешкина