Методы и средства криптографической защиты информации.фип_БАК

1. Наука о способах сохранения секретности информации это …
2. Процесс преобразования открытого текста в зашифрованный текст с использованием специального ключ это …
3. Процесс, позволяющий превратить зашифрованный текст обратно в исходный открытый текст это …
4. Специальные параметры, используемые для шифрования и дешифровки данных это…
5. Шифры, которые используют один и тот же ключ для шифрования и дешифровки, называются …
6. Шифры, которые используют два разных ключа, открытый и закрытый, называются …
7. Электронный инструмент, подтверждающий подлинность документа или сообщения, это …
8. Математическая функция, преобразующая входные данные произвольной длины в выходное значение фиксированной длины, это …
9. Атака, предполагает последовательное тестирование всех возможных комбинаций ключа до тех пор, пока не будет найден правильный, называется …
10. Научный подход к взлому шифров путем поиска слабостей в их конструкции, это …
11. Симметричный шифр, в котором данные делятся на блоки фиксированного размера, и каждый блок шифруется отдельно, называется …
12. Симметричный шифр, в котором данные шифруются побайтно или побитово, называется …
13. Ключ при ассиметричном шифровании, который доступен всем, называется …
14. Ключ при ассиметричном шифровании, который известен только владельцу, называется …

15. Свойство хэш-функций, которое подразумевает, что одинаковые входные данные всегда дают одно и то же хэш-значение, называется ...
16. Свойство хэш-функций, которое подразумевает, что хэш-значение легко вычислить по данным, но практически невозможно восстановить исходные данные по хэш-значению, называется ...
17. Шифр, в котором каждая буква заменялась другой буквой, смещённой на определённое число позиций в алфавите, был назван в честь ...
18. Наиболее известная шифровальная машина нового времени называлась ...
19. Шифры Blowfish и Twofish были разработаны Брюсом ...
20. Открытый и закрытый ключи используются для следующего типа шифрования:
21. Вид постквантовых алгоритмов, основанный на проблемах решетки это:
22. Вид постквантовых алгоритмов, основанный на проблемах декодирования линейных кодов:
23. Вид постквантовых алгоритмов, основанный на проблемах решения многочленов над конечными полями:
24. Симметричные шифры применяют в:
25. Хэш-функции применяют в:
26. Асимметричные шифры применяют в:
27. Хэш-функция MD5 генерирует:
28. Хэш-функция SHA-1 генерирует:
29. Неверно, что к преимуществам современных хэш-функций относится:
30. К классическим хэш-функциям относится:
31. Хэш-функцией является:
32. К классическим асимметричным шифрам относится:

33 К современным асимметричным шифрам относится:

34 Неверно, что к свойствам асимметричных шифров относят:

35 Неверно, что к симметричным шифрам относится:

36 Неверно, что к свойствам симметричных шифров относят:

37 Неверно, что хэш-функции должны обладать следующим свойством:

38 К недостаткам классических хэш-функций относится:

39 Для аутентификации при отправке документов, а также для защиты от подделки этих документов используют:

40 Расположите по порядку шаги создания цифровой подписи:

41 Расположите по порядку шаги проверки цифровой подписи:

42 Расположите в правильном порядке шаги реализации алгоритма асимметричного шифрования:

43 Расположите по порядку события в истории криптографии

44 Расположите типы шифра в порядке надежности

45 Расположите виды хеш-функций по дате выхода:

46 Расположите виды шифрования по периоду создания:

47 Расположите хэш-функции в порядке роста размера хэш-значения

48 Сопоставьте тип шифрования и его пример:

49 Сопоставьте тип шифрования с его недостатком:

50 Сопоставьте вид шифрования с его применением

51 Сопоставьте тип шифрования с его преимуществом:

52 Сопоставьте вид асимметричного шифрования с математическим принципом, лежащим в его основе

53 Сопоставьте алгоритмы Post-Quantum Cryptography с проблемами, но которых основана их реализация:

54 Сопоставьте хэш-функции с максимальным размером генерируемого хэш-значения:

55 Сопоставьте тип криптографической атаки со способом его реализации: