Протоколы всемирной паутины.
Экзаменационные вопросы за весенний семестр 2022 года.

1. Всемирная паутина: определение, значение в жизни общества. Понятие гипертекста. Основные свойства технологии.

2. Основные компоненты архитектуры всемирной паутины.

3. Обзор протоколов всемирной паутины.

4. URL/URI и MIME.

5. Протокол HTTP 1.1: Назначение, основные свойства. Формат сообщений. Типы сообщений (методы) и коды возврата.

6. Протокол HTTP 1.1: Специальные функции: аутентификация сторон, поддержка сеансов (cookie).

7. Протокол HTTP 1.1: Специальные функции: согласование содержания, кэширование.

8. Симметричные шифры. Основные понятия. Примеры. Режимы применения.

9. Криптографические контрольные суммы и хэш-функции. Определения. Примеры. Примеры использования.

10. Асимметричые криптографические алгоритмы. Основные понятия. Принципы использования. Электронная цифровая подпись.

11. Аутентификация сторон при сетевых соединениях.

12. Распределение открытых ключей. Инфраструктура открытых ключей X.509, основные понятия. Операционные протоколы.

13. Протокол SSL/TLS. Назначение. История. Архитектура, внутренние протоколы. Record Layer (SSL 3.0 – TLS 1.2)

14. Сценарии установления защищенного соединения в SSL 3.0 – TLS 1.2. Атаки на протокол Handshake: Renegotiation, снижение версии протокола.

15. Протокол SSL 3.0 – TLS 1.2: Атаки BEAST, POODLE.

16. Режимы применения AEAD, CCM, GCM.

17. Протокол TLS 1.3. Внутренние протоколы Record Layer, Alert, CCS.

18. Протокол TLS 1.3. Расширения (Extensions) в протоколе Handshake.

19. Протокол TLS 1.3. Внутренний протокол Handshake: Общая схема взаимодействий. Выработка общего секрета по методу Diffie-Hellman. Сообщения ClientHello, ServerHello, HelloRetryRequest, EncryptedExtensions.

20. Протокол TLS 1.3. Внутренний протокол Handshake: Сокращенная схема взаимодействий с использованием предварительно согласованного секрета (PreSharedSecret). Сообщения ClientHello, ServerHello, EncryptedExtensions, NewSessionTicket.

21. Протокол TLS 1.3. Внутренний протокол Handshake: Общая схема взаимодействий. Аутентификация сторон. Сообщения CertificateRequest, Certificate, CertificateVerify, Finished.

22. Протокол TLS 1.3: Расчеты ключей.

23. Протоколы HTTP/2 и HTTP/3.

24. Языки разметки HTML и XML. Основные понятия. История. Новое в HTML 5.

25. Язык HTML: Специальные элементы: ссылки, карты, формы, скрипты, объекты.

26. Язык XML: Принципы разбора. Основные приложения.

(См. также примерный список дополнительных вопросов - со следующего листа.)

Примерный список вопросов, которые могут быть заданы в качестве дополнительных.

1. Что такое гипертекст?
2. Для чего используется интерфейс CGI. Расшифровать название.
3. Перечислить языки для разработки скриптов на клиентской и серверной стороне.
4. Что такое DOM?
5. Перечислить протоколы всемирной паутины.

6. Разобрать на компоненты URL, предложенный экзаменатором.
7. Перечислить базовые типы MIME.
8. Перечислить типы MIME, введенные специально для HTTP.

9. Перечислить методы HTTP.
10. Перечислить группы кодов возврата HTTP.
11. Что такое Cookie?
12. Перечислить схемы аутентификации сторон в HTTP, дать им краткие характеристики.
13. Для чего используется поле заголовка Content-Type: | Length: | Host: | Vary: ?
14. Для чего используются поля заголовка Last-Modified:, E-Tag: If-Modified-Since:, If-None-Match:?

15. В чем разница между симметричными и асимметричными алгоритмами шифрования?
16. В чем разница между блочными и потоковыми алгоритмами шифрования?
17. Перечислить известные алгоритмы шифрования.
18. Перечислить известные режимы применения алгоритмов шифрования.
19. Что такое вектор инициализации?
20. Нужно передать информацию от абонента А к абоненту Б так, чтобы никто посторонний не мог с ней ознакомиться. Указать хотя бы 1 способ как это сделать, описать подробно.
21. В чем заключается алгоритм 3DES?
22. Почему невозможен алгоритм 2DES?
23. Что такое сеть Фейштеля?

24. Хэш-функция - определение.
25. Криптографическая контрольная сумма - определение.
26. Message Authentication Code (MAC) - определение.
27. Что такое HMAC?
28. Нужно передать информацию от абонента А к абоненту Б так, чтобы никто посторонний не мог ее изменить. Указать хотя бы 1 способ как это сделать, описать подробно.

29. Перечислить известные алгоритмы асимметричной криптографии.
30. Какие задачи можно решать алгоритмом RSA|DH|DSA?
31. Какими асимметричными алгоритмами можно решать задачи выработки общего секрета| ЭЦП | шифрования данных.
32. Привести порядок действий и формулы в алгоритме DH.
33. Привести порядок действий и формулы обмена ключами при помощи RSA.
34. Привести порядок действий и формулы ЭЦП при помощи RSA.

35. ЭЦП – определение.

36. Два абонента А и Б установили соединение. Как абоненту А убедиться, что абонент Б – действительно тот, за кого себя выдает? Указать хотя бы 1 способ сделать это, описать подробно.

37. Инфраструктура открытых ключей – определение.
38. Что такое сертификат открытого ключа?
39. Что такое список отзыва сертификатов?
40. Что такое Удостоверяющий Центр (CA)?
41. Что такое сертификационный путь?
42. Что такое кросс-сертификат?
43. Перечислить протоколы, которые используются в инфраструктуре открытых ключей.
44. Для чего используется протокол OCSP?

45. Перечислить внутренние протоколы SSL/TLS.
46. Описать назначение внутреннего протокола SST/TLS, указанного экзаменатором.
47. Перечислить подуровни протокола Record Layer.
48. Что такое заполнитель (Pad) в Record Layer?
49. Перечислить известные атаки на SSL/TLS.
50. В чем заключается атака BEAST?
51. В чем заключается атака POODLE?
52. Какая защита от BEAST предусмотрена в TLS 1.1?
53. Почему TLS 1.0-1.2 неуязвим к атакам типа Padding Oracle?

54. В чем основная идея AEAD?

55. Перечислить сообщения протокола Handshake в TLS 1.3.
56. Для чего используется расширение supported_versions | supported_groups | key_share | signature_algorithms | pre_shared_key | certificate_authorities | server_name
57. Для чего используется поле cipher_suites в сообщении ClientHello?
58. Что передается в сообщении Certificate? В каких случаях посылается такое сообщение?
59. Что такое DANE?
60. Как выполняется аутентификация сторон при полном сценарии Handshake в TLS 1.3?
61. Как выполняется аутентификация сторон при сокращенном сценарии Handshake в TLS 1.3?

62. Что такое DTD?
63. Перечислить известные элементы HTML, кроме HTML5, не менее 5.
64. Перечислить известные элементы HTML5, не менее 5.
65. Охарактеризовать назначение HTML-элемента <a> | <map> | <form> | <script> | <object>.

66. В чем разница между DOM-разбором и SAX-разбором XML.
67. Перечислить известные приложения XML, не менее 5.
68. Охарактеризовать назначение приложения XML XHTML | XML Schema | SVG | MathML | XForms | XQuery | SOAP | XSLT | XSL-FO.