Питання до іспиту з навчальної дисципліни «Прикладна криптологія та безпека ПЗ»
для студентів спеціальностей 121 «Інженерія програмного забезпечення»
та 122 «Комп'ютерні науки»
(2021-2022 н. р., І семестр)

Теоретичні основи криптології. Класичні алгоритми шифрування

1. У чому полягає забезпечення конфіденційності, цілісності, дійсності, доступності, інформаційних ресурсів?
2. Дайте визначення поняттям: криптологія, криптографія та криптоаналіз.
3. Що таке криптографічний алгоритм та шифр?
4. Що таке криптографічний ключ?
5. Розкрийте поняття зашифрування та дешифрування даних.
6. Дайте визначення відкритого та закритого тексту.
7. Назвіть складові криптографічної системи.
8. У чому полягає криптостійкість криптографічної системи?
9. Дайте коротку класифікацію шифрів.
10. Опишіть алгоритм шифрування Цезаря.
11. До якого виду шифрів заміни (підстановки) відносять шифр Цезаря?
12. У чому суть методу частотного криптоаналізу?
13. Опишіть алгоритм шифру частоколу.
14. У чому суть шифру скитали?
15. Опишіть алгоритм шифру Полібія.
16. Опишіть алгоритм шифру Плейфера.
17. Опишіть алгоритм шифрування криптосистемою Хілла.
18. Що являє собою ключ в криптосистемі Хілла?
19. Поясніть відмінність між шифрами моноалфавітної та поліалфавітної заміни.
20. У чому полягає основна слабкість шифрів простої моноалфавітної заміни?
21. Опишіть алгоритм шифрування Віженера.
22. Які кроки потрібно виконати для визначення довжини ключа у шифрі Віженера методом Казіскі?
23. Що таке індекс збігу?
24. Яка літера найчастіше зустрічається у текстах українською (англійською) мовою?
25. Який загальний вигляд мають функції зашифрування та дешифрування в симетричних криптографічних системах?

Блокові та потокові симетричні алгоритми шифрування

26. У чому полягає алгоритм одноразового блокноту (Вернама)?
27. Що являє собою операція XOR?
28. Дайте визначення поняттю «гама». Якими властивостями повинна володіти гама?
29. Які переваги і недоліки шифрування методом одноразового блокноту?
30. До яких шифрів належить стандарт шифрування даних DES?
31. Що таке мережа Фейстеля?
32. Яка довжина ключа у шифрі DES?
33. Яка довжина блоку у шифрі DES?
34. З яких кроків складається алгоритм шифрування DES?
35. Скільки раундів виконується шифрування за алгоритмом DES?
36. Назвіть основні кроки функції Фейстеля.
37. Скільки S-боксів у DES та для чого вони використовуються?
38. Які модифікації DES ви знаєте?
39. Назвіть основні режими роботи блокових симетричних алгоритмів шифрування.
40. Поясніть принцип роботи режиму простої заміни (ECB).
41. Поясніть принцип роботи режиму зв'язування блоків (CBC).

42. Для чого використовується вектор ініціалізації у режимі зв’язування блоків (CBC)?
43. Поясніть принцип роботи режиму зі зворотнім зв’язком по шифротексту (CFB).
44. Поясніть принцип роботи режиму зі зворотнім зв’язком по виходу (OFB).
45. Поясніть принцип роботи режиму лічильника (CTR).
46. Чим потоковий шифр відрізняється від блокового?
47. Яка різниця між синхронними потоковими шифрами та потоковими шифрами, що самосинхронізуються?
48. З якою метою використовують генератори псевдовипадкових чисел при потоковому шифруванні?
49. Які числа називають псевдовипадковими?
50. Які властивості повинен мати ГПВЧ для використання з криптографічною метою?
51. Поясніть принцип роботи лінійного конгруентного ГПВЧ.
52. Поясніть принцип роботи ГПВЧ на основі регістрів зсуву з лінійним зворотним зв’язком.
53. Поясніть принцип роботи ГПВЧ на основі алгоритму BBS.
54. З яких кроків складається алгоритм шифрування RC4?
55. Який шифр має теоретичну (абсолютну) стійкість?

Сучасні стандарти шифрування

56. Який алгоритм лежить в основі стандарту шифрування AES?
57. Опишіть основні кроки зашифрування за алгоритмом AES.
58. Від чого залежить кількість раундів шифрування за алгоритмом AES?
59. Яка довжина ключа в AES?
60. Яким чином генеруються ключі в AES?
61. Скільки слів можуть мати раундові ключ в AES?
62. Яка довжина блоку в AES?
63. Як називають матрицю проміжного результату при шифруванні за допомогою алгоритму AES?
64. Який розмір має матриця стану у алгоритмі AES?
65. Як подати байт у вигляді многочлена скінченого поля $GF(2^8)$?
66. Як виконується додавання і множення елементів поля $GF(2^8)$ у алгоритмі AES?
67. Опишіть операцію підстановки байтів у алгоритмі AES.
68. Опишіть операцію зсуву рядків у алгоритмі AES.
69. Опишіть операцію перемішування стовпців у алгоритмі AES.
70. Опишіть операцію додавання раундового ключа у алгоритмі AES.
71. Які особливості дешифрування за алгоритмом AES?
72. Як називають властивість шифру, при якій невеликі зміни в початкових даних (чи в ключі) можуть викликати значні зміни в зашифрованих даних?
73. Яким стандартом визначається криптографічний блоковий симетричний алгоритм перетворення даних «Калина»?
74. Від чого залежить кількість раундів шифрування за алгоритмом «Калина»?
75. Яка довжина ключа в алгоритмі «Калина»?
76. Як генерується допоміжний ключ в алгоритмі «Калина»?
77. Яким чином генеруються ключі з парними індексами в алгоритмі «Калина»?
78. Яким чином генеруються ключі з непарними індексами в алгоритмі «Калина»?
79. Скільки рядків має матриця стану в алгоритмі «Калина»?
80. Якою може бути кількість стовпців у матриці стану в алгоритмі «Калина»?
81. Яким чином відбувається операція побітового додавання за модулем 2^{64} в алгоритмі «Калина»?
82. Скільки таблиць замін використовується в криптографічному алгоритмі перетворення даних «Калина»?
83. Опишіть операцію підстановки байтів у алгоритмі «Калина».
84. Опишіть операцію зсуву рядків у алгоритмі «Калина».

85. Опишіть операцію перемішування стовпців у алгоритмі «Калина».
86. Опишіть операцію додавання раундового ключа у алгоритмі «Калина».
87. Які особливості дешифрування за алгоритмом «Калина»?
88. Назвіть основні режими роботи алгоритму шифрування «Калина».

Асиметричні алгоритми шифрування

89. У чому полягає ідея криптосистеми з відкритим ключем?
90. Хто є основоположниками криптографії з відкритим ключем?
91. Яка основна перевага асиметричних шифрів над симетричними?
92. Що таке одностороння функція?
93. У чому полягає задача пакування рюкзака?
94. Що таке суперзростаюча послідовність?
95. Опишіть алгоритм розв'язання задачі суперзростаючого рюкзака.
96. Назвіть кроки генерування відкритого ключа із закритого в алгоритмі Меркла-Хелмана.
97. Як відбувається шифрування у криптосистемі Меркла-Хелмана?
98. Як відбувається дешифрування у криптосистемі Меркла-Хелмана?
99. На чому ґрунтується криптостійкість алгоритму шифрування даних RSA?
100. В алгоритмі RSA обираються 2 випадкові великі значення p та q. Якою властивістю мають володіти ці числа?
101. Як знайти n – модуль криптосистеми RSA?
102. Чому дорівнює $\varphi(n)$ в алгоритмі RSA?
103. Що визначає функція Ейлера $\varphi(n)$ в алгоритмі RSA?
104. Яким чином у алгоритмі RSA отримуються відкритий та закритий ключі?
105. Якою властивістю має володіти відкритий ключ e в алгоритмі RSA?
106. Дати визначення поняттю «взаємно прості числа». Наведіть приклади взаємно простих чисел.
107. Який алгоритм зашифрування в алгоритмі RSA?
108. Який алгоритм дешифрування в алгоритмі RSA?
109. На чому ґрунтується криптостійкість алгоритму шифрування даних Ель-Гамаля?
110. Яким чином у алгоритмі Ель-Гамаля отримуються відкритий та закритий ключі?
111. Опишіть алгоритм шифрування Ель-Гамаля.
112. Яке призначення алгоритму Діффі-Хеллмана?
113. Опишіть алгоритм обміну ключами Діффі-Хелмана.
114. На чому базується криптостійкість протоколу обміну ключами Діффі-Хелмана?
115. Що таке первісний корінь за модулем простого числа?

Хешування та ЦП. Криптографічні системи на еліптичних кривих

116. Дайте визначення поняттям «хешування», «хеш-функція».
117. Що таке дайджест повідомлення?
118. Які основні вимоги висуваються до криптографічної хеш-функції?
119. Назвіть основні кроки алгоритму хешування SHA-256.
120. Назвіть основні кроки алгоритму хешування «Купина».
121. Що являє собою (електронний) цифровий підпис?
122. Опишіть схему створення і перевірки ЦП.
123. Який порядок використання відкритого та закритого ключів при створенні і перевірці ЦП?
124. Які схеми цифрового підпису існують?
125. Для чого потрібна сертифікація відкритих ключів?
126. Як здійснюється підпис RSA? Яка відмінність підпису RSA від шифру RSA?
127. Як здійснюється підпис Ель-Гамаля?
128. Як здійснюється перевірка на дійсність підпису Ель-Гамаля?

129. Стандарт цифрового підпису DSS.
130. Який розмір хешу генерує хеш-функція SHA-1?
131. Які переваги мають криптосистеми на еліптичних кривих над звичайними асиметричним алгоритмами?
132. Який загальний вигляд має крива, що використовується в криптографічних системах, заснованих на еліптичних кривих?
133. Дайте визначення порядку групи точок еліптичної кривої.
134. Дайте визначення порядку точки еліптичної кривої.
135. Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих?
136. Як перевірити, що точна належить еліптичній кривій?
137. Які основні операції виконуються над точками еліптичних кривих при їх використанні в криптографічних системах?
138. Опишіть алгоритми додавання та подвоєння точки.
139. Опишіть алгоритм скалярного множення точки на число.
140. Опишіть алгоритм Діффі-Хелмана на еліптичних кривих.

Також у тестах будуть запитання **практичного змісту**, на використання формул, обчислень тощо.