Предмет Защита информации

1. Шифр Вернама применяется для шифрования сообщения 0110 с ключом 1100. Найдите зашифрованную последовательность среди приведенных:

 а) 0000

 б) 1010

 в) 1110

 г) 0111

2. Шифр Эль-Гамаля

 а) c открытым ключом

 б) совершенный

 в) блоковый

3. В системе шифрования с открытым ключом найти сообщение без знания ключа

 а) невозможно

 б) возможно при полном переборе ключей

 в) возможно при наличии генератора случайных чисел

4. В протоколе "электронные деньги" используется

 а) стандартная цифровая подпись

 б) нотариальная подпись

 в) слепая подпись

 г) взаимная подпись

5. Количество операций при возведении числа в степень n не превосходит

 а) 0.5 log n

 б) log n

 в) 2 log n

6. Найти наименьшее число, взаимно простое с 756

7. Генератор RC4 имеет начальную установку S = (3, 2, 1, 0, 4, 5, 6, 7), i = j = 0, n = 3. Записать (в десятичном виде) первые 4 элемента порождаемой последовательности.

8. Расшифровать слово, зашифрованное шифром Цезаря, описанным во Введении (k = 3): ЛРЧИНЩЛВ

9. Вычислить y = 9 25771 mod 31991

10. Вычислить y = 10 –1 mod 31013

11. Российский стандарт на электронную подпись использует два модуля p и q для

 а) сокращения длин чисел при вычислениях

 б) уменьшения величины показателей степени

 в) упрощения операции вычисления модуля

12. Пользователю системы RSA с открытыми параметрами N и d передано зашифрованное сообщение e. Расшифровать это сообщение (взломав систему RSA). N = 4061, d = 7, e = 2054, m = ?