|  |  |
| --- | --- |
| **Задание 1**  1. Показать на примере с использованием алгоритма RSA передачи стороной А зашифрованного сообщения (первые две буквы Вашей фамилии), обеспечив возможность другой стороне (В) точно идентифицировать отправителя и получить подтверждение целостности полученного сообщения.  Начальные параметры для генерации Вашего ключа:  p= 13, q= 19.  Подробно описать каждый шаг используемых алгоритмов.  2 Показать структурную схему регистра сдвига с линейной обратной связью, заданного неприводимым многочленом **430;** представить таблицу состояний регистра при ненулевых ненулевом начальном состоянии; определить период последовательности.  3. Используя шифр множественной перестановки, зашифровать/расшифровать сообщение «множественная перестановка». Ключи: «связь», «ключи».  Подробно описать каждый шаг используемого алгоритма и его криптостойкость. | **Задание 4**  1. Показать на примере с использованием алгоритма RSA передачи стороной А зашифрованного сообщения (первые две буквы Вашей фамилии), обеспечив возможность другой стороне (В) точно идентифицировать отправителя и получить подтверждение целостности полученного сообщения.  Начальные параметры для генерации Вашего ключа:  p= 13, q= 19.  Подробно описать каждый шаг используемых алгоритмов.  2 Показать структурную схему регистра сдвига с линейной обратной связью, заданного неприводимым многочленом **430;** представить таблицу состояний регистра при ненулевых ненулевом начальном состоянии; определить период последовательности.  3. Используя шифр множественной перестановки, зашифровать/расшифровать сообщение «множественная перестановка». Ключи: «связь», «ключи».  Подробно описать каждый шаг используемого алгоритма и его криптостойкость. |
| **Задание 2**  1. Показать на примере с использованием алгоритма RSA передачи стороной А зашифрованного сообщения (первые две буквы Вашей фамилии), обеспечив возможность другой стороне (В) точно идентифицировать отправителя и получить подтверждение целостности полученного сообщения.  Начальные параметры для генерации Вашего ключа:  p= 17, q= 19.  Подробно описать каждый шаг используемых алгоритмов.  2 Показать структурную схему регистра сдвига с линейной обратной связью, заданного многочленом **4310;** представить таблицу состояний регистра при ненулевых ненулевом начальном состоянии; определить период последовательности.  3. Используя шифр множественной перестановки, зашифровать/расшифровать сообщение «Потоковые синхронные шифры». Ключи: «сдвиг», «…» (выбрать и обосновать).  Подробно описать каждый шаг используемого алгоритма и его криптостойкость. | **Задание 5**  1. Показать на примере с использованием алгоритма RSA передачи стороной А зашифрованного сообщения (первые две буквы Вашей фамилии), обеспечив возможность другой стороне (В) точно идентифицировать отправителя и получить подтверждение целостности полученного сообщения.  Начальные параметры для генерации Вашего ключа:  p= 17, q= 19.  Подробно описать каждый шаг используемых алгоритмов.  2 Показать структурную схему регистра сдвига с линейной обратной связью, заданного многочленом **4310;** представить таблицу состояний регистра при ненулевых ненулевом начальном состоянии; определить период последовательности.  3. Используя шифр множественной перестановки, зашифровать/расшифровать сообщение «Потоковые синхронные шифры». Ключи: «сдвиг», «…» (выбрать и обосновать).  Подробно описать каждый шаг используемого алгоритма и его криптостойкость. |
| **Задание 3**  1. Используя шифр множественной перестановки, зашифровать/расшифровать сообщение «Симметричная и асимметричная криптография». Ключи: «регстр», «…» (выбрать и обосновать).  Подробно описать каждый шаг используемого алгоритма и его криптостойкость.  2. Показать структурную схему регистра сдвига с линейной обратной связью, заданного многочленом **5210;** представить таблицу состояний регистра при ненулевых ненулевом начальном состоянии; определить период последовательности  3.. Показать на примере с использованием алгоритма RSA передачи стороной А зашифрованного сообщения (первые две буквы Вашей фамилии), обеспечив возможность другой стороне (В) точно идентифицировать отправителя и получить подтверждение целостности полученного сообщения.  Начальные параметры для генерации Вашего ключа:  p= 11, q= 23. Подробно описать каждый шаг используемых алгоритмов. | **Задание 6**  1. Используя шифр множественной перестановки, зашифровать/расшифровать сообщение «Симметричная и асимметричная криптография». Ключи: «регстр», «…» (выбрать и обосновать).  Подробно описать каждый шаг используемого алгоритма и его криптостойкость.  2. Показать на примере с использованием алгоритма RSA передачи стороной А зашифрованного сообщения (первые две буквы Вашей фамилии), обеспечив возможность другой стороне (В) точно идентифицировать отправителя и получить подтверждение целостности полученного сообщения.  Начальные параметры для генерации Вашего ключа:  p= 11, q= 23. Подробно описать каждый шаг используемых алгоритмов.  3.Показать структурную схему регистра сдвига с линейной обратной связью, заданного многочленом **5210;** представить таблицу состояний регистра при ненулевых ненулевом начальном состоянии; определить период последовательности |
|  |  |
|  |  |
|  |  |