出席番号：　　氏名：

演習問題 2：公開鍵暗号のトイモデル I

隣の席の人と、$p = 17$ の場合のアリス側、ボブ側となって n' を聞き、元のデータ n を複合せよ．それぞれ 2 回

演習問題 2：解答 A　自分がアリスのとき

1. 1 回目

   $q =$ _____, $q' =$ _____,

   ボブから送られてきたもの：$n' =$ _____,

   複合したもの：$n =$ _____,

2. 2 回目

   $q =$ _____, $q' =$ _____,

   ボブから送られてきたもの：$n' =$ _____,

   複合したもの：$n =$ _____,

演習問題 2：解答 B　自分がボブのとき

1. 1 回目

   $q =$ _____, $p =$ _____,

   自分のデータ：$n =$ _____,

   暗号化したデータ：$n' =$ _____,

   複合したものは一致したか？　_____,

2. 2 回目

   $q =$ _____, $q' =$ _____,

   $q =$ _____, $p =$ _____,

   自分のデータ：$n =$ _____,

   暗号化したデータ：$n' =$ _____,

   複合したものは一致したか？　_____

演習問題 3：公開鍵暗号のトイモデル I

隣の席の人と、$32 > p > 17$ の素数で、上記のトイモデル I による公開鍵暗号による暗号化されたデータ通信を実施せよ。各 2 回

演習問題 3：解答 A　自分がアリスのとき

1. 1 回目

   $p =$ _____,

   $q =$ _____, $q' =$ _____,

   ボブから送られてきたもの：$n' =$ _____,

   複合したもの：$n =$ _____,

2. 2 回目

   $p =$ _____,

   $q =$ _____, $q' =$ _____,

   ボブから送られてきたもの：$n' =$ _____,

   複合したもの：$n =$ _____,

演習問題 3：解答 B　自分がボブのとき

1. 1 回目

   $q =$ _____, $p =$ _____,

   自分のデータ：$n =$ _____,

   暗号化したデータ：$n' =$ _____,

   複合したものは一致したか？　_____,

2. 2 回目

   $q =$ _____, $q' =$ _____,

   $q =$ _____, $p =$ _____,

   自分のデータ：$n =$ _____,

   暗号化したデータ：$n' =$ _____,

   複合したものは一致したか？　_____

演習問題 4：公開鍵暗号のトイモデル I

隣の席の人と、$p > 22$ の素数で、上記のトイモデル I による公開鍵暗号による暗号化されたデータ通信を実施せよ。 各 2 回

演習問題 4：解答 A　自分がアリスのとき

1. 1 回目

   $p =$ _____,

   $q =$ _____, $q' =$ _____,

   ボブから送られてきたもの：$n' =$ _____,

   複合したもの：$n =$ _____,

2. 2 回目

   $p =$ _____,

   $q =$ _____, $q' =$ _____,

   ボブから送られてきたもの：$n' =$ _____,

   複合したもの：$n =$ _____,

演習問題 4：解答 B　自分がボブのとき

1. 1 回目

   $q =$ _____, $p =$ _____,

   自分のデータ：$n =$ _____,

   暗号化したデータ：$n' =$ _____,

   複合したものは一致したか？　_____,

2. 2 回目

   $q =$ _____, $q' =$ _____,

   $q =$ _____, $p =$ _____,

   自分のデータ：$n =$ _____,

   暗号化したデータ：$n' =$ _____,

   複合したものは一致したか？　_____