Note on integrity: You may discuss problems with fellow students, but all written work must be entirely your own, and should not be from any other course, present or past. If you use a solution from another source you must cite it, including from other people who help you.

Questions

For both of these questions, show the work you do to decode the messages. If you use software, make sure you wrote it and provide source code.

(1) Stinson (3rd edition), Exercise 5.12, decode the first ciphertext only.

   Photocopy of the question attached.

(2) Stinson (3rd edition), Exercise 6.9.

   Decrypt the ElGamal ciphertext presented in the following table. The parameters of the system are $p = 31847$, $\alpha = 5$, $a = 7899$ and $\beta = 18074$. Each element of $\mathbb{Z}_n$ represents three alphabetic characters as in Exercise 5.12 (e.g., DOG is represented by $3 \times 26^2 + 14 \times 26 + 6$, since D is 0, O is 14, and G is 6).

   The plaintext was taken from "The English Patient", by Michael Ondaatje, Alfred A. Knopf, Inc., New York, 1992.

$(3781, 14409)$	$(31552, 3930)$	$(27214, 15442)$	$(5809, 30274)$
$(5400, 31486)$	$(19936, 721)$	$(27765, 29284)$	$(29820, 7710)$
$(31590, 26470)$	$(3781, 14409)$	$(15898, 30844)$	$(19048, 12914)$
$(16160, 3129)$	$(301, 17252)$	$(24689, 7776)$	$(28856, 15720)$
$(30555, 24611)$	$(20501, 2922)$	$(13659, 5015)$	$(5740, 31233)$
$(1616, 14170)$	$(4294, 2307)$	$(2320, 29174)$	$(3036, 20132)$
$(14130, 22010)$	$(25910, 19663)$	$(19557, 10145)$	$(18899, 27609)$
$(26004, 25056)$	$(5400, 31486)$	$(9526, 3019)$	$(12962, 15189)$
$(29538, 5408)$	$(3149, 7400)$	$(9396, 3058)$	$(27149, 20535)$
$(1777, 8737)$	$(26117, 14251)$	$(7129, 18195)$	$(25302, 10248)$
$(23258, 3468)$	$(26052, 20545)$	$(21958, 5713)$	$(346, 31194)$

(8836, 25898)   (8794, 17358)   (1777, 8737)   (25038, 12483)
(10422, 5552)   (1777, 8737)   (3780, 16360)   (11685, 133)
(25115, 10840)   (14130, 22010)   (16081, 16414)   (28580, 20845)
(23418, 22058)   (24139, 9580)   (173, 17075)   (2016, 18131)
(19886, 22344)   (21600, 25505)   (27119, 19921)   (23312, 16906)
(21563, 7891)   (28250, 21321)   (28327, 19237)   (15313, 28649)
(24271, 8480)   (26592, 25457)   (9660, 7939)   (10267, 20623)
(30499, 14423)   (5839, 24179)   (12846, 6598)   (9284, 27858)
(24875, 17641)   (1777, 8737)   (18825, 19671)   (31306, 11929)
(3576, 4630)   (26664, 27572)   (27011, 29164)   (22763, 8992)
(3149, 7400)   (8951, 29435)   (2059, 3977)   (16258, 30341)
(21541, 19004)   (5865, 29526)   (10536, 6941)   (1777, 8737)
(17561, 11884)   (2209, 6107)   (10422, 5552)   (19371, 21005)
(26521, 5803)   (14884, 14280)   (4328, 8635)   (28250, 21321)
(28327, 19237)   (15313, 28649)