VE203
Assignment 8

Jiang Yicheng
515370910224

November 24, 2016

Exercise 8.1

$19-A, 17-T, 14-C, 20-K, 23-P, 18-E, 19-A, 8-R, 12-L, 16-H, 3-B, 21-O, 25-D, 6-M, 15-S, 22-V, 11-N$ So the message is

$$ATTACK\ \ PEARL\ \ HARBOR\ \ DECEMBER\ \ SEVEN$$

Exercise 8.2

$n = p \cdot q = 7 \cdot 11 = 77, e = 7, m = 23$, so

$$c \equiv m^e \equiv 23^7 \equiv 23 \cdot (-10)^3 \equiv (-10) \cdot 23 \cdot 23 \equiv 100 \equiv 23\ (mod\ 77)$$

So the number $m = 23$ is encrypted as $c = 23$.

Exercise 8.3

Since $(G, \circ)$ is cyclic g is a generator of G, then $(G, \circ)$ is group already and $\forall x \in G, \exists k \in \mathbb{N}, g^k = x$.

$\forall x, y \in G$, we can set $x = g^{k_1}, y = g^{k_2}$, then

$$x \circ y = g^{k_1} \circ g^{k_2} = \underbrace{g \circ g \circ \cdots \circ g}_{k_1+k_2\ \ times} = g^{k_2} \circ g^{k_2} = y \circ x$$

so the group $(G, \circ)$ satisfies community. So $(G, \circ)$ is abelian.

Exercise 8.4

According to the question, we can set that

$$3^a \equiv 6\ (mod\ 7), 3^b \equiv 5\ (mod\ 7)$$

and we can find that

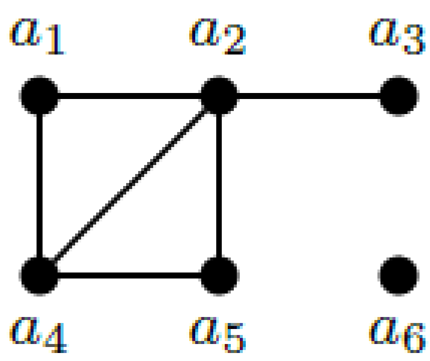
$$3^5 \equiv 4 \cdot 3 \equiv 5\ (mod\ 7), 3^3 \equiv 6\ (mod\ 7), 3^6 \equiv 5 \cdot 3 \equiv 1\ (mod\ 7)$$

so $a = 3, b = 5$ and $3^{ab} = 3^{15}$.

So their common secret key is 3^{15}.

Exercise 8.5

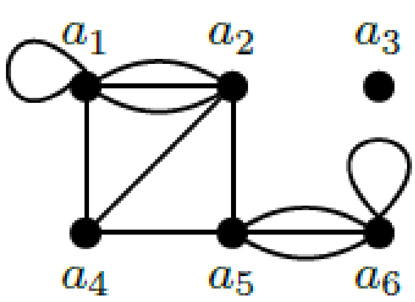
i)



1. The number of vertices: 6
2. The number of edges: 6
3. $deg(a_1) = 2, deg(a_2) = 4, deg(a_3) = 1, deg(a_4) = 3, deg(a_5) = 2, deg(a_6) = 0$
4. Isolated vertices: a_6
5. Pendant vertices: a_3
6. It is a simple graph.
7. The adjacency matrix is

$$A_G = \begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{array} \begin{array}{c} \begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

ii)

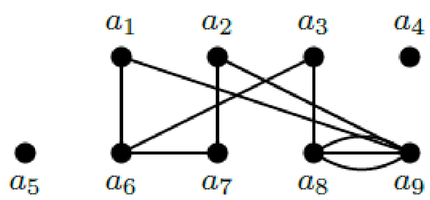


1. The number of vertices: 6

2. The number of edges: 12
3. $deg(a_1) = 6, deg(a_2) = 5, deg(a_3) = 0, deg(a_4) = 3, deg(a_5) = 5, deg(a_6) = 5$
4. Isolated vertices: a_3
5. Pendant vertices: no
6. It is a multigraph and also a pseudograph.
7. The adjacency matrix is

$$A_G = \begin{array}{cc} & \begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array} \\ \begin{array}{c} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{array} & \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

iii)

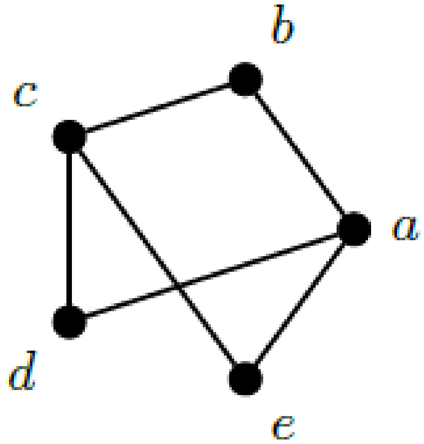


1. The number of vertices: 9
2. The number of edges: 10
3. $deg(a_1) = 2, deg(a_2) = 2, deg(a_3) = 2, deg(a_4) = 0, deg(a_5) = 0, deg(a_6) = 3,$
   $deg(a_7) = 2, deg(a_8) = 4, deg(a_9) = 5$
4. Isolated vertices: a_4, a_5
5. Pendant vertices: no
6. It is a multigraph.
7. The adjacency matrix is

$$A_G = \begin{array}{cc} & \begin{array}{ccccccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{array} \\ \begin{array}{c} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \end{array} & \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

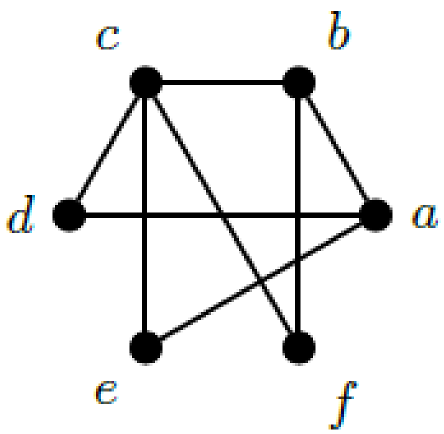
Exercise 8.6

i)



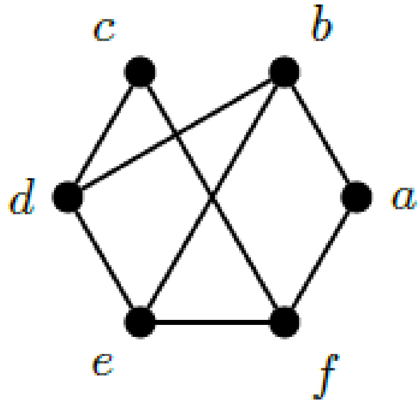
This graph is bipartite and a bipartition of it is $(\{a, c\}, \{b, d, e\})$

ii)



If d is in color 1, then c is in color 2, b and f have to be in color 1, and therefore f and b are in the same color while they are connected together. So this graph is not bipartite.

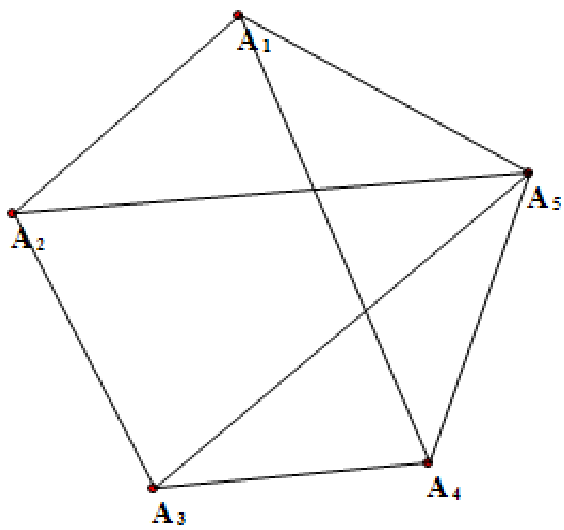
iii)



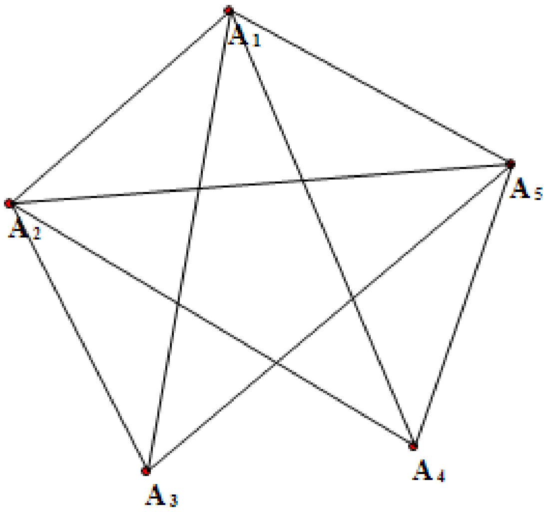
If d is in color 1, then c and e are in color 2, f have to be in color 1, a should be in color 2 and b should be in color 1. Then b and d are in the same color while they are connected together. So this graph is not bipartite.

Exercise 8.7

i)



ii)



iii)