

# Discrete Mathematics, 2016 Spring - HW 13

December 7, 2016

**Instructor: Zsolt Pajor-Gyulai**

Courant Institute of Mathematical Sciences, NYU

To get full credit in all of the problems, use rigorous justification and unless otherwise indicated, make sure that your solution reads as a perfect English sentence. You should only assume integers, operations and order relations as given. If you use a statement or a definition from the textbook, make sure to indicate it.

## Section 44

- 4) Let's assume Alice and Bob both have public encryption functions  $E_A$  and  $E_B$ , respectively, and closely guarded, private decryption functions  $D_A$  and  $D_B$ . Alice and Bob each know the other's public function, and presumably Eve knows  $E_A$  and  $E_B$  too.

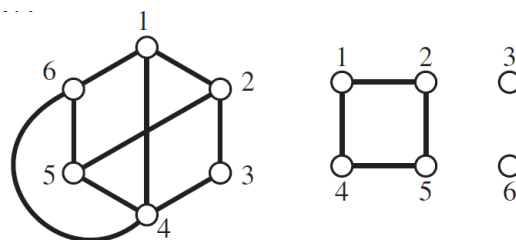
Here is an alternative way to the protocol we learned about in class Alice can use. She first encrypts the message  $M$  by computing  $D_A(M)$  and then sends the result to Bob. Let's explore the implications of her following this alternative protocol.

- (a) Alice has sent  $D_A(M)$  to Bob. How does he recover the original message  $M$ ?
- (b) Eve intercepts the transmission  $D_A(M)$ . Can she also decrypt this message?
- (c) The message Alice sent to Bob was nasty and she tries to claim that Eve sent the message. How does Eve defend herself?

The point of (c) is that Alice cannot deny having sent the message; in that sense, she has put her digital signature on the message.

## Section 47

- 1) The following pictures represent graphs. Please write each of these graphs as a pair of sets  $(V, E)$ .



2) Draw pictures of the following graphs.

(a)  $(\{a, b, c, d, e\}, \{\{a, b\}, \{a, c\}, \{b, c\}, \{b, d\}, \{c, d\}\})$

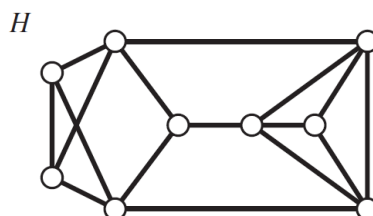
(b)  $(\{a, b, c, d, e\}, \{\{a, c\}, \{b, d\}, \{b, e\}\})$

15) Let  $G$  be a simple graph. Prove that there must be an even number of vertices with odd degree.

16) Prove that in any graph with two or more vertices, there must be two vertices of the same degree.

### Section 48

5) Let  $G$  be the graph in the picture.



(a) Draw the complement graph  $\bar{G}$ .

(b) Find  $\alpha(G)$  and  $\omega(G)$ .

12) This problem is in connection with Proposition 48.13 on p342. Find a graph on five vertices for which  $\omega(G) < 3$  and  $\omega(\bar{G}) < 3$ . This shows that the number six in the proposition is the best possible.