CSE 350/550: Network Security,
Correct answer to Question 3, Quiz 2

3. Take a look at table below that describes a message together with the hash function/value. Here characters x_0, x_1, … x_6 are message characters. The 8-bits of any character x_j are shown as: xj7, xj6, …, xj0, where xj7 is the (EVEN) parity bit. That is
x07 + x06 + … + x00 = 0; x17 + x16 + … + x10 = 0; …, x67 + x66 + … + x60 = 0

A last character x_7 is added and forms part of the hash value. It is obtained by computing:
x70 + x60 + … + x00 = 0; x71 + x61 + … + x01 = 0; …; x77 + x67 + … + x07 = 0

	(parity) bit_7	bit_6	bit_5	bit_4	bit_3	bit_2	Bit_1	bit_0
x_0	x07	x06	x05	x04	x03	x02	x01	x00
x_1	x17	x16	x15	x14	x13	x12	x11	x10
x_2	x27	x26	x25	x24	x23	x22	x21	x20
x_3	x37	x36	x35	x34	x33	x32	x31	x30
x_4	x47	x46	x45	x44	x43	x42	x41	x40
x_5	x57	x56	x55	x54	x53	x52	x51	x50
x_6	x67	x66	x65	x64	x63	x62	x61	x60
(parity) x_7	x77	x76	x75	x74	x73	x72	x71	x70

To summarize, the sum of all bits in a given row is 0. And the sum of all bits in a given column is 0. The hash function consists of all the shaded bits from the table, viz. the bit_7 in each character, and the 8 bits in char_7. The rest is the original text.

I prepare a message consisting of 7 characters, "I O U 1 2 0 0", where the characters in the message are encoded as 8-bits including the parity bit. An 8 th character is added to complete the hash function/value. I now create a digital signature using the above hashing function, H(x), and RSA with my private key PR-BNJ.

a. Is it possible to replace the message to something else without this change being detected at the receiver's end? YES
And why do you think so? For example, IOU1200 & IOU2100 result in the same row-wise parity bit and column –wise parity bit. To be sure a limited amount of rearranging the letter would not disturb the parity bits. See answers to part b. and c. below.

2 marks

b. Give one more example where it is possible to replace "IOU1200" without this change being detected at the receiver's end?
IOU1233. HERE the row-wise and column-wise parity bits are the same as those for IOU1200.

2 marks

c. Give one example where a change will in fact be detected at the receiver's end?
IOU1020 will result in different row-wise parity bits

2 marks

d. What change in the IOU note can be made by an intruder that will result in the largest value being owed by me, the sender?
Message IOU8865 and IOU1200 have the same row=wise and column-wise parity bits. Any attempt to send message IOU9xxx or IOU89xx will change the row-wise parity bits. So it has to be IOU88xx. It can be argued that IOU8865 does not change the parity bits at all, and anything larger than 8865 will change the row-wise OR column-wise parity bits.
Above 'x' is any digit.

2 marks

Instructor to TA grading this question: If a student has given an answer such as IOU88xx or even IOU44xx or something that looks significantly larger than IOU1200. Given him/her full marks, viz. 2 marks for this d. section.