The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 6 Solutions

11th and 12th April 2019

Number of Questions: 4
Time allowed: 50min
Total marks: 5

In order to score marks you need to show all working/reasoning and not just the end result.

	Student Number	*Student Name*
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

Question 1	Question 2	Question 3	Question 4	Total

An evil empress Ruby Cel who owns the larges ruby mines in the Galaxy is doing what it takes to ensure her dominance in the ruby market. To that end, she has recently stolen 12 precious rubies that have a purple hue. You are hired you to retrieve the rubies from Ruby Cel and they gave you the remaining 13th purple ruby as it may come in handy.

As soon as you enter Ruby Cel's empire you were caught by the guards and taken to the empress, who is well known not only for her business ruthlessness but also for her love of good puzzles. She tells you that she will let you go and even give you the 12 rubies if you can solve all of the following puzzles – otherwise you will end up as a slave in one of her mines.

1. How old am I? I am between 3 and 4 million hours old. If you multiply my hours by 4 and divide it by 993737 you get remainder 1. (1 mark)

Solution:
This is equivalent to asking $(4x)\text{mod}993737 = 1, \quad 3000000 < x < 4000000$
Using euclid's extended algorithm for gcd to calculate the multiplicative inverse:

i	y	g	u	v
0	-	993737	1	0
1	-	4	0	1
2	248434	1	1	**-248434**
3	4	0		

To get x in the right range, simply add 993737 to the solution until you get the solution in the desired range: $-248434 + (993737 * 4) = 3726514$

Thus Ruby Cel is 3726514 hours old.

2. People call me Ruby Cel but what is my real name? My age will give you a clue. (1 mark)

Solution:
Using her age as the key to a transposition cipher (3,7,2,6,5,1,4), we can re-arrange the letters in her name to get "Blue Cry" (letter 3 in position 1, letter 7 in position 2, etc.)

3. What mood am I in? I have 3 moods: cranky, sad and bored. My true mood is twice as likely as the other two moods together. You can ask me yes or no question(s), but ask too many and you go to the mines. (i.e. make a question tree) (1 mark)

Solution:
Based on her name, she is most likely sad – thus the probability of her being sad is 2/3, the probability of her being cranky is 1/6, and for bored 1/6 as well. Ask her the yes/no questions based on these probabilities.
Therefore, ask her: "Are you sad?" if no, then ask her "Are you cranky?" – at which point you should know her mood anyway.

4. The 12 purple rubies that you are after are guarded in the cellar with 12 red rubies. You can take them if you can recognise which ones they are.
Tonight, my 24 sisters will go to the cellar, and the oldest sister will touch the first ruby, the second oldest will touch the second ruby, and so on. Some of my sisters can switch the ruby hue from red to purple or from purple to red, and some can't. (The same thing will always happen when my sisters touch the rubies – the colour will always switch or not switch. Also, the change in colour only lasts for a day, after which it will revert to its original colour)

Tomorrow morning, you can go to the cellar alone and look at the rubies. (The rubies will return to their original colours after you have left)

Tomorrow evening, after the rubies have reverted to their natural colour, my sisters will go to the cellar again and touch the rubies.

The morning after that, you have to go to the cellar again and choose 12 rubies – choose right and you can take them and leave. Choose wrong and you go to the mines. (You must choose before the rubies revert to their original colours)

(2 marks – explain how you know which 12 are the purple ones)

Solution:
The situation with the 24 sisters and the swapping colours is meant to be analogous to a Synchronous Stream Cipher.
The intended solution is to use an insertion attack to determine which 12 rubies are the correct rubies.

In traditional terms, the 24 sisters are the key, the original colours are the plaintext, and the colours after the sisters have touched the rubies are the ciphertext.

Let the original colours of the rubies be P1 to P24.
Let the sisters be K1 to K24 (K1 being the oldest, K24 being the youngest).
Let the colours after the sisters have touched them be C1 to C24, such that $C1=P1 \oplus K1$ and so on.

P1	P2	P3	P4	P5	P6	P7	P8	P9	…
K1	K2	K3	K4	K5	K6	K7	K8	K9	…
C1	C2	C3	C4	C5	C6	C7	C8	C9	…

When you go alone to see the rubies on the first morning, you can see C1 to C24. Further, you know that K1 to K24 does not change.

Since you are alone, you can swap one of the rubies with the one in your pocket (you were given one when you were sent). To perform an insertion attack, you could put your ruby in the first spot, then put the first ruby in the second spot and so on (thus the last ruby, P24, ends up in your pocket).
After doing this, when you have to choose the 12 rubies, the situation is as follows:

Let X be the (colour of the) ruby from your pocket.
Let C1'-C24' be the colours that you see this time around.

X	P1	P2	P3	P4	P5	P6	P7	P8	…
K1	K2	K3	K4	K5	K6	K7	K8	K9	…
C1'	C2'	C3'	C4'	C5'	C6'	C7'	C8'	C9'	…

Now, you have the following information:

- You know C1 to C24 from the day before.
- You can see C1' to C24'.
- You also know that K1 to K24 has not changed.
- Finally, you know X, as it was the ruby from your pocket.

The method for determining P1 to P23 is as follows:

For P, C and X, let 0 mean purple, and 1 mean red
For K, let 1 mean that the sister swaps the colour, and 0 mean that the sister does not swap the colour

K1 = C1' $\oplus$ X (we know that X = 0, so K1 = C1' $\oplus$ 0)
P1 = C1 $\oplus$ K1

K2 = C2' $\oplus$ P1
P2 = C2 $\oplus$ K2

K3 = C3' $\oplus$ P2
P3 = C3 $\oplus$ K3

And so on for K4 to K24 and P3 to P23.

As for the ruby that you swapped out and put in your pocket (P24), you know that there were originally 12 of each colour, so you know the colour of the one in your pocket simply by elimination. (i.e. if there are 11 red and 12 purple, the one in your pocket must be red). In addition, the one in your pocket would be its original colour by the time you had to choose, as the sisters have not touched it since the first time.