The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 8

3rd May 2019

Number of Questions: 5
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	Question 5	Total

1. In a public-key system using RSA, you intercept the ciphertext C=10 sent to a user whose public key is (5, 35). What is the plaintext M?

2. How does a public-key cryptosystem provide authenticity? (How can a public-key system be used to implement digital signatures?)

Unfortunately, (some of) you could not beat Ruby Cel last week in her little game, so the trouble goes on… You know from the time you spent in Ruby Cel's empire that she uses RSA for all her communication with public key (13, 8251903391). You also know that she doesn't understand how to use public key encryption correctly, as she keeps her both her public and private keys secret from outsiders.

The Great Council top officials suspects that one of their senior members, Cunning Kay, has teamed up with Ruby Cel, and that he will try to send her confidential information about the location for the secret ruby mines. They set him a trap and announce in the Council Meeting that the mines are located at Planet 1 (not true, of course). The same night they intercept his secret message to Ruby Cel: 5445590809549643238067108864
The very next day, Cunning Kay receives the following message from unknown sender:
72779147576710886467108864473669545172779145757671088640473669545172779147
57513019008215943231594323067568936904736695451473669545161180731066710886481920476476625467108864457407768581864666298192

The Great Council hires you to decode the messages.
(Note: the intended method of solving this problem expects you to use a spreadsheet, or at least a calculator that can compute modular arithmetic accurately. If you don't have access to either of those, join a group that does have them.) Note on the note: use Microsoft Excel or Apple Numbers if you have access to those spreadsheet programs otherwise you may run into rounding issues.

3. What is the message sent by Cunning Kay?

4. What is the reply sent by Ruby Cel?

5. What were the weaknesses in Ruby Cel's communication scheme that allowed you to decrypt the messages?