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?

Solution:
$n = 35 = 5 \times 7$
$\phi(n) = (5-1)(7-1) = 4 \times 6 = 24$
$e \times d \bmod \varphi(n) = 1$
$5 \times d \bmod 24 = 1$
Using Euler's theorem, we get $d = 5^{(\phi(24)-1)} \bmod 24 = 5^7 \bmod 24 = 5 \times 5^6 \bmod 24 = 5 \times 25^3 \bmod 24 = 5 \times 1^3 \bmod 24 = 5$. (Otherwise use Euclid's extended algorithm)

So $M = C^d \bmod n = 10^5 \bmod 35 = 5$

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

Solution:
Say Bob wants to sign a message and send it to Alice. Using a public-key cryptosystem, Bob would "encrypt" the message by using his private key. By the nature of a public-key cryptosystem, this message can only be "decrypted" using Bob's public key. When Alice gets the message, she can verify that it "decrypts" correctly under Bob's public key. Since such a message could only have been created using Bob's private key, Alice can be confident that the message was created by Bob (or someone with his private key).

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 2 (not true, of course). The same night they intercept his secret message to Ruby Cel: 473669545179282950435445590809
The very next day, Cunning Kay receives the following message from unknown sender:
727791475767108864671088644736695451727791475767108864047366954517277914757513019008215943235496432380513019008248087906256118073106473669545104736695451473669545161180731066710886481920476476625467108864457407768581864666298192

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.)

3. What is the message sent by Cunning Kay?

Solution:
"two"

4. What is the reply sent by Ruby Cel?

Solution:
"meet me at midnight at the cauesrc"

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

Solution:
The primary weakness is that both messages are encrypted with Ruby Cel's Public Key. Since we also roughly know the contents of Cunning Kay's message, we are able to check the encoding scheme used by Ruby Cel in communications. It turns out the ciphertext is obtained by taking each individual character and encrypting it with Ruby Cel's Public key. Thus we can simply build a table mapping each of the plaintext characters to their corresponding ciphertext characters.

P (letter)	P (integer)	C = [MOD(P^13,8251903391)]
a	0	0
b	1	1
c	2	8192
d	3	1594323
e	4	67108864
f	5	1220703125
g	6	4808790625
h	7	6118073106
i	8	5130190082
j	9	279583901
k	10	6944993499
l	11	5000259378
m	12	7277914757
n	13	5496432380
o	14	5445590809
p	15	157398807
q	16	7825084772
r	17	8186466629
s	18	4574077685
t	19	4736695451
u	20	4764766254
v	21	5761438901
w	22	7928295043
x	23	2484436808
y	24	675689369
z	25	5694463753