The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 9

16th and 17th May 2019

Number of Questions: 5
Time allowed: 50min
Total mark: 5

Calculators not allowed.

	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. Consider a Diffie-Hellman scheme with a common prime $q=11$ and a primitive root $\alpha=2$.

a. Show that 2 is a primitive root of 11.
b. If user A has public key $Y_A=9$, what is A's private key X_A?
c. If user B has public key $Y_B=3$, what is the secret key K shared with A?

Solution:

a. $\varphi(11) = 10$
$2^{10} = 1024 = 1 \bmod 11$
If you check 2^n for $n < 10$, you will find that they are all distinct. In fact, it is sufficient to show that none of the values is $1 \bmod 11$.
b. $X_A = 6$, because $2^6 \bmod 11 = 9$
c. $K = 3^6 \bmod 11 = 3$

2. In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant $\alpha^x \bmod q$ for some public number α. What would happen if the participants sent each other x^α for some public number α instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers?

Solution:
For example, the key could be $x_A^\alpha x_B^\alpha = (x_A x_B)^\alpha$. Of course, Eve can find that trivially just by multiplying the public information. In fact, no such system could be secure anyway, because Eve can find the secret numbers x_A and x_B by using Fermat's Little Theorem to take α-th roots.

3. Consider an ElGamal scheme with a common prime $q=71$ and a primitive root $\alpha=7$.
a. If B has public key $Y_B=3$ and A chose the random integer $k=2$, what is the ciphertext of $M=30$?
b. If A now chooses a different value of k so that the encoding of $M=30$ is $C=(59, C_2)$, what is the integer C_2?

Solution:
a. $(49, 57)$
b. $C_2 = 29$

4. Last month you successfully retrieved the 12 purple rubies from the evil empress Ruby Cel, and you are now in high demand in the galaxy. There are rumours that Ruby Cel is planning to attack either Planet 6 to steal their precious 6000 rubies, or Planet 1 to steal their 1000 rubies. The Great Council is only able to defend one of the planets and not both. They are calling on you to predict where Ruby Cel will attack. During your time at the Ruby's empire, you know that she is superstitious and that she has a bag with 9 red rubies and 1 black ruby. She draws one, and if it is black, she goes for the bigger gain; if it is red, she goes for the smaller gain. Will you tell the Great Council to defend the Planet 6 or the Planet 1? You need to prove to the Great Council that your decision will minimise the expected gain to Ruby Cel.

Solution:

The probability that Ruby Cel will attack Planet 6 is $P(P6) = \frac{1}{10}$, while the probability that she will attack Planet 1 is $P(P1) = \frac{9}{10}$.
If you defend Planet 6, Ruby's expected gain is:

$$E(G_6) = \frac{1}{10} \times 0 + \frac{9}{10} \times 1000 = 900$$

If, on the other hand, you defend Planet 1, Ruby's expected gain is:

$$E(G_6) = \frac{1}{10} \times 6000 + \frac{9}{10} \times 0 = 600$$

Therefore, it is better to defend Planet 1 as that minimises Ruby's expected gain.

5. As you successfully minimised the damage from the attack, you reputation is bigger than ever. Ruby Cel offers you a following deal: you can either choose to draw (without replacement) a black ruby from a bag of 20 black rubies and 40 red rubies, or to draw (without replacement) 3 black rubies from a bag with of 40 black rubies and 20 red rubies? You can choose a task and Ruby Cel is going to take the other one. The one who completes the task in smaller number of draws wins. If you win, for any planet in your Galaxy, if you are there when Ruby Cel's men attack, they will abort the attack and go back home empty handed. Which task should you choose (and why)?

Solution:
The probabilities
p_1^i of drawing a black ruby from a bag of 20 black rubies and 40 red rubies in *i* draws and p_3^i of drawing 3 black rubies from a bag with of 40 black rubies and 20 red rubies in *i* draws, both without replacement, are given in the table below.

i	$\boldsymbol{p_1^i}$	$\boldsymbol{p_3^i}$
1	$\frac{20}{60} = \frac{1}{3}$	0
2	$\frac{40}{60} \times \frac{20}{59} = \frac{20}{60} \times \frac{40}{59}$	0
3	$\frac{40}{60} \times \frac{39}{59} \times \frac{20}{58} = \frac{20}{60} \times \frac{40}{59} \times \frac{39}{58}$	$\frac{40}{60} \times \frac{39}{59} \times \frac{38}{58}$
…	…	
i	$\frac{40}{60} \times \frac{39}{59} \times \ldots \times \frac{40-i+2}{60-i+2} \times \frac{20}{60-i+1} = \frac{20}{60} \times \frac{40}{59} \times \frac{39}{58} \times \ldots \times \frac{40-i+2}{60-i+1}$	$\frac{20}{60} \times \frac{19}{59} \times \frac{18}{58} \times \ldots \times \frac{40}{60-i+3} \times \frac{39}{60-i+2} \times \frac{38}{60-i+1}$
…	…	…
23		$\frac{20}{60} \times \frac{19}{59} \times \frac{18}{58} \times \ldots \times \frac{40}{40} \times \frac{39}{39} \times \frac{38}{38}$
…	…	…
41	$\frac{20}{60} \times \frac{40}{59} \times \frac{39}{58} \times \ldots \times \frac{1}{20}$	0

Note that $p_1^i > p_3^i$ for $i > 3$. Also note that $p_1^i = 0$ for $i > 41$ and $p_3^i = 0$ for $i > 23$.
The expected number $E(N_1)$ of draws to draw one black ruby is:

$$E(N_1) = p_1^1 \times 1 + p_1^2 \times 2 + p_1^3 \times 3 + \cdots + p_1^{41} \times 41$$

The expected number $E(N_3)$ of draws to draw three black rubies is:

$$E(N_3) = p_3^1 \times 1 + p_3^2 \times 2 + p_3^3 \times 3 + \cdots + p_1^{41} \times 41$$

As $p_1^i > p_3^i$ for $i > 3$, we have

$$E(N_1) - (\, p_1^1 \times 1 + p_1^2 \times 2 + p_1^3 \times 3) > E(N_3) - (\, p_3^1 \times 1 + p_3^2 \times 2 + p_3^3 \times 3)$$

$$E(N_1) - \left(\frac{20}{60} \times 1 + \frac{20}{60} \times \frac{40}{59} \times 2 + \frac{20}{60} \times \frac{40}{59} \times \frac{39}{58} \times 3 \right)$$

$$> E(N_3) - (\, 0 \times 1 + 0 \times 2 + \frac{40}{60} \times \frac{39}{59} \times \frac{38}{58} \times 3)$$

$$E(N_1) - E(N_3) > \frac{20}{60} \times 1 + \frac{20}{60} \times \frac{40}{59} \times 2 + \frac{20}{60} \times \frac{40}{59} \times \frac{39}{58} \times 3 - \frac{40}{60} \times \frac{39}{59} \times \frac{38}{58} \times 3 = 0.378$$

Thus we have $E(N_1) > E(N_3)$. As the expected number of draws to draw a black ruby from a bag of 20 black rubies and 40 red rubies in *i* draws is greater than the expected number of draws to draw 3 black rubies from a bag with of 40 black rubies and 20 red rubies in *i* draws, both without replacement, you should choose the latter.