QUT Faculty of Science, School of Computer Science
IFN648 Applied Cryptography, 2021 Semester 1

Assessment Item 1: Problem Solving Task

Module 3 Task: Asymmetric Ciphers, Digital Signatures, Elliptic Curve Crypto

This is an **individual assessment** task: you may discuss this task with your classmates, but the work you submit must be your own individual effort. There are **50 marks** in this assignment. Your results will form **13.33 % of your final result** in IFN648.

Specifications:

This assessment item contains both concept checking questions and practical exercises using individualised challenges. Your individual challenges will be based on your 8-digit QUT student ID, which we will call ID, padded with leading zeroes if necessary (e.g., if your student number is 12345678, use ID=12345678; if your student number is 1234, use ID=00001234.) Remove any leading “n” or “N” from your ID number, which should then have exactly 8 digits.

- For each task, follow the instructions to derive your individual challenge based on your 8-digit ID.
- Complete the tasks using CrypTool 2, by hand, or even by writing your own computer script, at your option, unless specifically indicated otherwise.

Submission:

Submit a PDF write-up with your specific answers to the questions, showing your work where required. Submission is electronic, via Blackboard, in the Assessment tab. Look for the *Assignment 3: Public-Key Cryptography* submission link (where you found this PDF)*.*

- It is important that your report is written in your own words. You may include duly acknowledged screenshots; for example, of CrypTool outputs. **Do not 'cut and paste' or copy information from any source into your report without acknowledgement: that is considered plagiarism** (a breach of academic integrity) and is not acceptable in Australian universities.
- Remember that late submissions without an approved extension will be given a mark of 0, as per QUT policy. If you require an extension, please apply to Student Services before the task due date.
- Your report need not be long. This is not a project. Focus on giving specific answers to the questions given, and nothing else. (If your your short answer, even if correct, is drowned in a sea of irrelevant text, you will lose marks for not answering the question in specificity.) However, feel free to make use illustrations where appropriate.

Marking Criteria:

The marks assigned for each subsection are indicated with the questions below. Be sure to attempt all questions, and only the questions. Be sure to use your own personalised inputs.

QUT Faculty of Science, School of Computer Science
IFN648 Applied Cryptography, 2021 Semester 1

Question 1: Asymmetric cryptography and Diffie-Hellman [9 marks]

a) Using the modulus M = 101, the generator G = 2, and a personalised exponent E, compute G^E mod M, using the square-and-multiply method, **by hand**, i.e., using pen and paper. For your exponent, take E = 1000 + (ID mod 1000), which is to say that E is a number between 1000 and 1999, written in decimal as 1 followed by the last 3 digits of your QUT ID. Provide your working to show all the steps and intermediate results of the square-and-multiply algorithm, up to your final value.
[**4 marks**, as 3 marks for the calculation steps and 1 mark for the final value]

b) Suppose you are Alice, one of two participants, with Bob being the other, performing an unauthenticated Diffie-Hellman key exchange. Briefly explain the two instances where you, Alice, would use the square-and-multiply algorithm in this key exchange, making sure to describe what inputs each instance would be using (just describe the inputs, no need for actual numbers here).
[**2 marks**, as 0.5 for each correct instance and 0.5 for each set of inputs]

c) * Combining parts a and b above, what can you say about the security of Alice and Bob's Diffie-Hellman key exchange, if they are using the M=101 and G=2 as modulus and generator? Discuss at least two security defects of such a choice; i.e., give two reasons why this is a bad choice, and explain.
[**3 marks**, as 1 mark for the easy reason, and 2 marks for the harder one]

Question 2: Public-key encryption with ElGamal [7 marks]

This task requires you to use an ElGamal cryptosystem with modulus *p* = 23,456,789 and generator *g* = 25 for system parameters. Let the plaintext message P1 be your QUT ID viewed as a numerical value P1 (which should be around 10 millions, and definitely smaller than p: let me know if you have an unusually high ID for whch that is not the case). The recipient is Alice, and her public key is A = 17,189,856.

a) Encrypt the plaintext P with Alice's public key, showing the main steps of the calculation. Attention: if at any point you need to select some random number for your encryption, be sure to pick it *at random* as required by the algorithm, and to specify what number you picked even if it would normally not be included in the final result (you will lose points if your "random" number was, in our estimation, highly unlikely to have been picked at random). You will likely need a computer, so no need to show the internal steps of component calculations, but clearly show the correct execution of all the steps of the algorithm.
[**2 marks**, for correct execution of the right algorithm]

b) Clearly show the ciphertext that will be sent to Alice: all of it, and nothing else.
[**2 marks**, as 1 mark for form, and 1 mark if it decrypts correctly]

c) How does the length of the ciphertext compare to the length of P1? [**1 mark**]

d) Explain how Alice will decrypt the ciphertext. [**2 marks**]

Question 3: Public-key encryption with ElGamal and RSA [6 marks]

To use RSA, you need an RSA key pair. The table below shows values of p and q indexed by digits I and j ranging from 0 to 9. Your indices i and j are, you guessed it, to be found in your QUT ID, as the two middle digits (i.e., the 4th and 5th digit from the left) of your full 8-digit ID including any leading zero. In other words, your QUT ID has the form ***ij***, so for example if your ID is 01234567, then I = 3 and j = 4. Once you have figured out your indices I and j, find your primes p and q using the table below. For the example with i = 3 and j = 4, you would use p = p[3] = 23 and q = q[4] = 71.

a) Choose your own value for *e* in any way you like and form the public key. Show that your choice of *e* is suitable for the particular *p* and *q* you were assigned.
[**3 marks**, as 1 mark for a valid key, and 2 marks for proof of validity]

b) Derive the corresponding private key exponent *d*.
[**3 marks**, as 1 mark for the correct value, and 2 marks for its derivation]

i or j	0	1	2	3	4	5	6	7	8	9
p[i]=	13	17	19	23	29	31	37	41	43	47
q[j]=	53	59	61	67	71	73	79	83	89	97

Question 4: Digital Signatures [8 marks]

Let the plaintext message P2 be your full name as written on your student card (write it down so there is no ambiguity). Use the RSA Key Generator in CrypTool to generate an RSA Key pair. Then use the SHA-256 hash function along with the RSA algorithm to form signature generation and verification tools to complete the parts of this task listed below.

a) Compute the RSA signature for P2. In your report, briefly explain the steps involved in the process, and the inputs and outputs for each step.
[**3 marks**]

b) Suppose you sent someone the message and the signature. What do they need to have in order to verify the signature you have created for this message?
[**1 mark**]

c) Verify the RSA signature you formed for this message. In your report, explain the steps involved in the verification process, and the inputs and outputs for each step.
[**2 marks**]

d) If the signature is verified, what assurance does this give the message recipient? What assumptions does this rely on?
[**2 marks**]

QUT Faculty of Science, School of Computer Science
IFN648 Applied Cryptography, 2021 Semester 1

Question 5: Elliptic curves [20 marks]

Consider the elliptic curve E/F_p : $y^2 = x^3 + ax + b$, for the modulus p = 17, and individualised values a = ((ID div 100,000) mod 10) and b = ((ID div 100) mod 10) where div is integer division and mod is modular reduction. That is to say, a and b are respectively the 3nd and 6th digits of your 8-digit ID, i.e., your ID has the form **a**b**. For example, if your ID is 01234567, you'll use a=2 and b=5.

a) Make a list of all the points on your curve, writing them all out on a list (in any order), designating each of them with their (x,y) coordinates i*f appropriate* (hint...).
[**3 marks**]

b) Draw a graph and plot your elliptic curve points on the graph.
[**2 marks**]

c) What is the order of the curve? Be sure to count all the points (oh, that hint again…)
[**1 mark**]

d) Are there any points that share the same x value? Were you expecting this?
[**1 mark**, only for the justification]

e) * Are there any x values for which there are no points on the curve? Provide some reasoning why your answer here is what you expect. You should be able to make this argument from facts about curves we have seen in the lecture, including a fact about the number of points, and a counting argument.
[3 **marks**, only for the reasoning]

f) Choose any of the points which you plotted on your graph, making note of its x and y coordinates, and label this point S.

i. Calculate the point 2S, showing your work. If you are using a formula based on the x and y coordinates of S, show the computation. If you are attempting to work directly on your graph, precisely explain what you are doing (hint: you will have to think out of the box if you choose to use the latter approach; remember that you have almost complete freedom to pick any S you like).
[5 **marks**, as 1 mark for the result, and 4 marks for the work]

ii. Calculate the point 3S, working using either a formula, or a graphical method. Showing your work.
[**2 marks**, as 1 mark for the result, and 1 mark for the method]

iii. Calculate the points 4S and 5S in any way you like. No need to show your work here.
[**1 mark**, as 0,5 mark per point]

iv. Show all five points on your graph by labelling them S, 2S, …, 5S, connecting them using arrows in the following order: S -> 2S -> 3S -> 4S -> 5S.
[**2 marks**]

End of paper