MATH324
CRYPTOGRAPHY

Assignment 1 **Due 3pm on Friday 5 August 2016**

STAPLE this page to the front of your assignment.

Name:	Nikolaj Dybdahl Rathcke
Student ID:	74763954

MATH324

Cryptography

Assignment 1 **Due 3pm on Friday 5 August 2016**

This assignment is based entirely on the ElGamal cryptosystem. As part of this assignment, you are expected to research how this cryptosystem works for yourself. However, the following brief outline of the system along with material covered in the second set of lecture notes (The Discrete Logarithm Problem) may be useful to you.

The ElGamal Cryptosystem:

1. Alice chooses a large finite cyclic group G and a generator $g \in G$. She chooses a random integer $a \in \{0, 1, 2, \ldots, |G|-1\}$, which she keeps secret. She computes $A = g^a$. Her public key is (G, g, A).
2. Bob wants to send Alice a message $m \in G$. He obtains a copy of her public key and chooses a random $b \in \{0, 1, 2, \ldots, |G|-1\}$, then computes $B = g^b$ and $c = A^b m$. The ciphertext is the pair $(B, c) \in G \times G$. He sends this to Alice.
3. To decrytp Bob's message, Alice computes $(B^a)^{-1}c = m$.

1. (i) What common elements do the ElGamal cryptosystem and Diffie-Hellman key exchange share?

   (ii) What are the encryption and decryption functions in the ElGamal Cryptosystem? Prove that encryption and decryption are inverse operations.

   (iii) Is it necessary for the element g chosen by Alice to be a generator in G? Why/why not?

   (iv) The Discrete Logarithm Problem is believed to be hard (that is, no efficient algorithm currently exists). Explain how the ElGamal Cryptosystem uses this to ensure key security.

2. Set up your own ElGamal Cryptosystem in the finite cyclic group $G = (\mathbb{Z}_p^*, \times)$ by following the steps belows.

   (i) Choose a suitable prime p from the list below:

   $$411,\ 503,\ 527,\ 1107,\ 1729,\ 1915,\ 2043.$$

   One of the integers in the list is prime. Find prime p, showing the methods you used to test for primality. Why is it important to make sure that p is prime?

   (ii) Find a primitive element of $g \in G$. Explain the method you used to find g. (Note that "The Internet told me." is *not* a valid method for finding generators.)

   (iii) Choose an integer $a \in \{0, 1, 2, \ldots, p{-}1\}$ and compute your public key.

3. (i) Suppose that Bob wishes to send Alice two separate messages m_1 and m_2. He uses element $b \in G$ to encipher both messages obtaining ciphertexts c_1 and c_2 respectively. Unfortunately for him, Eve has been watching him and knows m_1, c_1 and c_2. Can Eve recover m_2 with the information she has? Why/why not?

   (ii) You are hired to work over the summer at the University and your boss has just emailed Human Resources with your salary details (which you do not yet know). You manage to launch a successful man-in-the-middle attack and intercept the encrypted message. You know that the original plaintext m consists of a single number – your salary – which has been encrypted using the ElGamal Cryptosystem in $(\mathbb{Z}_p^*, \times)$. Explain how you can use the ciphertext you have intercepted to encrypt and send the message $2m$ to Human Resources.

4. Even though the Discrete Logarithm Problem is believed to be hard (in that no efficient algorithm currently exists), there are many (inefficient) algorithms for computing the discrete logarithm. One example is the Baby-step Giant-step Algorithm we covered in lectures. Write a short report (1–2 pages) outlining some of the other algorithms used for finding discrete logarithms, including information about their runtime complexity. Your report need not cover the algorithms in mathematical detail. Please cite any references you use.