Compulsory Assignment 2

**Question 1.**

**a)**

**b)**

***1)***

Now, let represent the salary of the employee some years after the year 2017.

Each year the employee’s salary is increase with 10’000 NOK plus an extra 5% of the salary from the year before. With this information we can set up a recurrence relation which looks something like this:

***2)***

To find an explicit formula we use the recurrence relation from the last question.

Then, given:

We can try to find a pattern when we add enough years.

Then we can use this general sum to find the explicit formula:

**Question 2.**

**a)**

Now in the book it states:  
*Let be a positive integer and let and be integers. Then  
and*

Therefore, we can split up the equation to look like this:

With this much simpler equation we can calculate

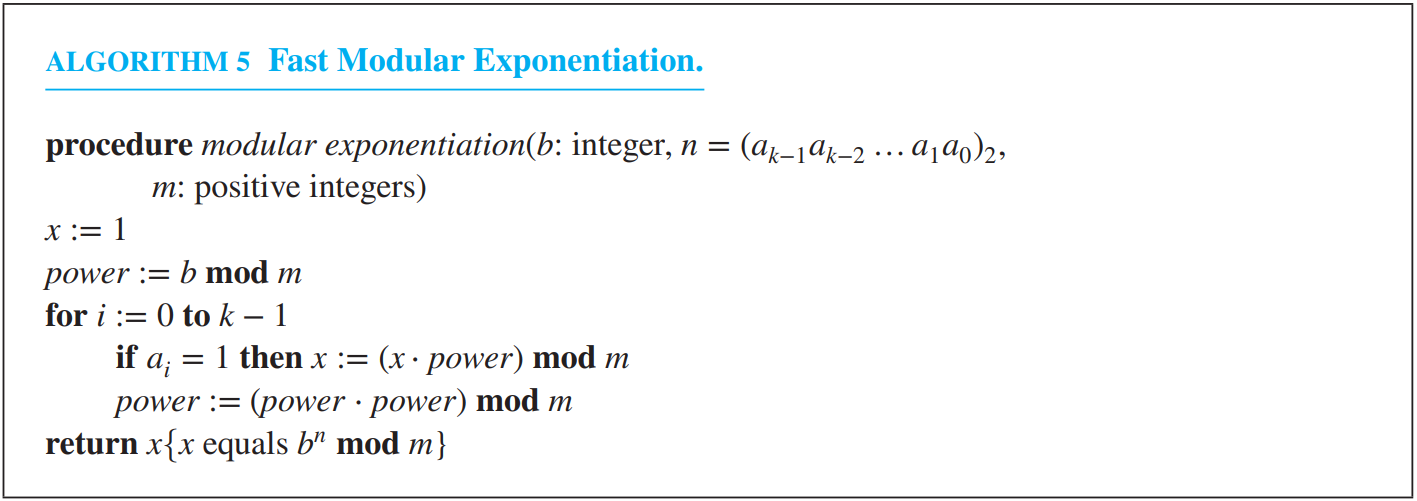
We can look how many times 13 goes into 32 and find the remainder.

So, now our equation looks like this:

Again, we can look how many times 11 goes into 216, and the remainder *y* is our answer.

**b)**

To complete this equation, we use the algorithm for fast modular exponentiation which we can find in the book:



In the start, , and our is

Then, we need to convert the exponent (644) to binary:

Now we can read the remainders of each equation from bottom to top, and we get our binary number of 244 which is (1010000100)2 this will act as our in this algorithm.

To be clear we start at and work our wat up to , and in our instance .

This means our answer to the equation .

**c)**

If and are relatively prime integers and , then a unique inverse of exists and is denoted with < m and

The first step is to show, using the Euclidean algorithm that a and m are relatively prime.

So, the greatest common divider is the last nonzero remaining integer, which is 1.

Next, we write the *gcd*. as a multiple of and :

Now we can see that the inverse of *a* modulo *m* is the integer .

**Question 3.**

To encrypt this message using RSA we use the formula:

We start by dividing the message: “ATTACK” into pairs like such: “AT TA CK”. Then we convert the letters to number where A=0, B=1, C=2, etc.

The highest value we can have in one pair is 2525 and since this is valid.

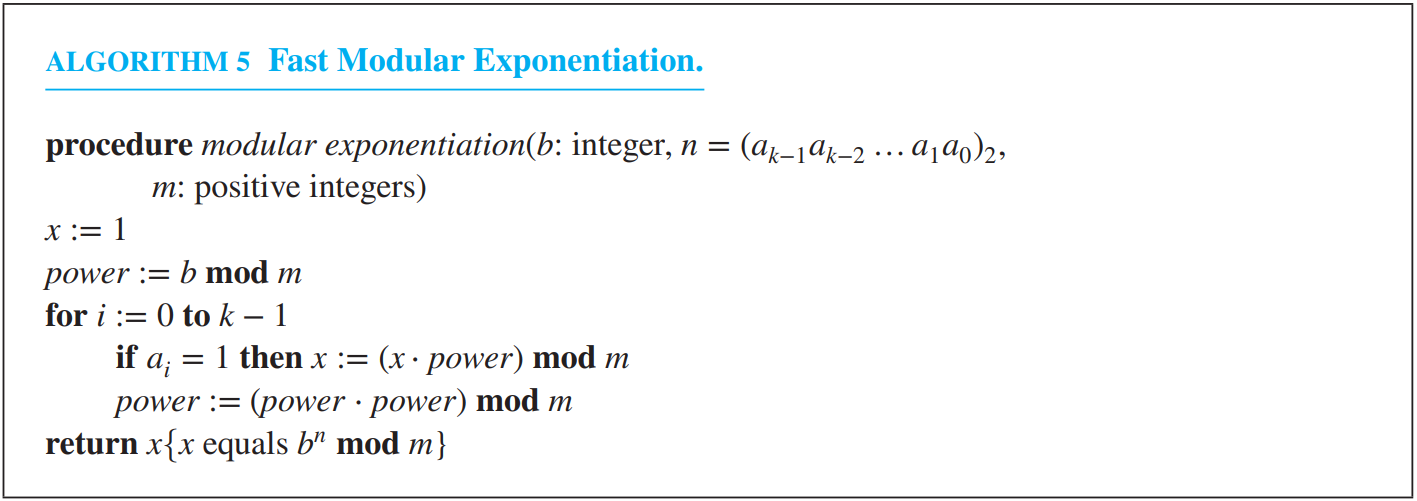
Our messages will then be: .

Then for each pair we use it in the encryption algorithm. Our three equations look like this:

Then we need to change the exponent from decimal to binary:

Then reading from bottom to top we get the number (1101)2, and since all the equations have the same exponent, we do not need to repeat this for each equation.

Then again using the 5th algorithm from the book:



After using the RSA encryption algorithm for each group of four integer we get the new value of: , which is the encrypted message.

**Question 4.**

**a)**

To show that is true we just plug just plug it in .

Thus making true.

**b)**

The inductive hypothesis is where , and

**c)**

To prove the inductive step, we look at the function .