Understanding Cryptography **Homework No. 5** **Due Date:**

1. It is obvious that in RSA cryptosystem, decrypting an encrypted message always gives back the original message. i.e.: $m^{ed} \mod pq = m$ (the correctness). This will imply from the following more general lemma:
   Lemma 1. Let n be a product of distinct primes and $a = 1 \bmod \varphi(n)$ for some nonnegative integer a. Then:
   $$m^a = m \bmod n.$$
   a) Explain why Lemma 1 implies that k and k^5 have the same last digit, For example:
   $$2^5 = 3\mathbf{2}, \quad 79^5 = 3077056039\mathbf{9}$$
   Hint: Consider $\varphi(10)$.
   b) Explain why Lemma 1 implies the correctness of RSA?
   c) Prove that if p is a prime, then
   $$m^a = m \bmod p,$$
   For all nonnegative integers $a = 1 \bmod (p-1)$.
   d) Prove that if n is a product of distinct primes, and $a = b \bmod p$, for all prime factors p of n, then $a = b \bmod n$.
   e) Combine the previous parts to complete the proof of Lemma 1.

2. We have a few blocks of cipher text encrypted by a RSA cryptosystem with public key (e, n).
   a) Does it help to break the cipher if we knew that one of the message blocks has a common factor with n?
   b) Suppose that n is a $2t$-bits number ($t > 500$), where p and q are t-bits prime numbers. What would be the message length in bits if the expected number of occurrences for the above phenomena is 1?

3. In the DHKE protocol, the private keys are chosen from the set $\{2, \dots, p-1\}$. Why are the values 1 and $p-1$ are not considered?

4. Encrypt the following message with the Elgamal scheme ($p = 467$, $\alpha = 2$).
   $$k_{pr} = d = 105, \; i = 213, \qquad x = 33$$
   Now decrypt the ciphertext and show all steps.

5. Write a program which computes the discrete logarithm in $\mathbb{Z}_p^*$ by exhaustive search. The input parameters for your program are p, α, β . The program computes x where $\beta = \alpha^x \bmod p$. Compute the solution to log_{106}^{12375} in $\mathbb{Z}_{24691}^*$.

6. In this problem, we want to use the RSA toolbox in CrypTool. You can either open a text file as your plaintext or you may use the software's default text which is initially open. You can find the RSA toolbox from the following menu:

Indiv. Procedures: RSA Cryptosystem

You are provided with the following tools:

(1) Prime Number Test
(2) Generate Prime Number
(3) Factorization of a Number
(4) RSA Demonstration
(5) Signature Demonstration (Signature Generation)

These tools are provided to work with near-real values hence you can use it for large numbers. This is a kind of useful calculator since even powerful mathematic soft-wares have problems to deal with large numbers in the scale which is needed for real world secure cryptosystems. Most of the times, you need to develop personalized programs to work with those numbers in your cryptanalysis projects. But this toolbox helps you overcome this problem.

The first three items, does not need more explanations. The forth one is a complete RSA simulator. You can simulate the whole process of a RSA cryptosystem and employ it to encrypt and decrypt short example. The last one simulates the procedure you can make a certified signature for your RSA cryptosystem.

a) Follow the steps in the last item to make a certified signature. (all steps are visually explained in the soft-ware) Please note that your signature is personal, you ought to use your own name and family name when you want to provide certificate for your signature. Use your student number as your PIN CODE. If you follow all steps successfully, a congratulation message will appear and then the settings of your signature will be shown in a separate text window.
b) Now, you can select yourself as the recipient by using this signature to encrypt a text with RSA algorithm. Refer to the following menu:

   Crypt/Decrypt: Asymmetric: RSA Encryption

   A dialogue box with the title "Selection of a key for RSA encryption of…" will appear on your screen. Now you can select "yourself" you made before as the key. It means that you are encrypting the text for someone you know his public key (The one you yourself made in the previous step). The result is a little bit strange and confusing at the first look! Can you explain it?
c) Decrypt the encrypted text by the following menu:

   Crypt/Decrypt: Asymmetric: RSA Decryption
d) Save settings of the signature and the encrypted file and document them with a brief explanation of what you observed.