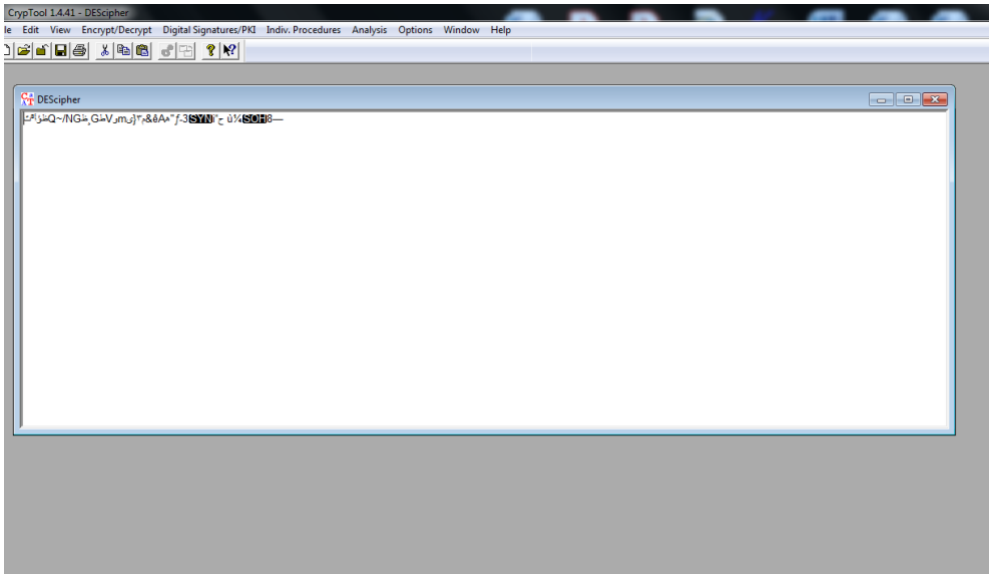
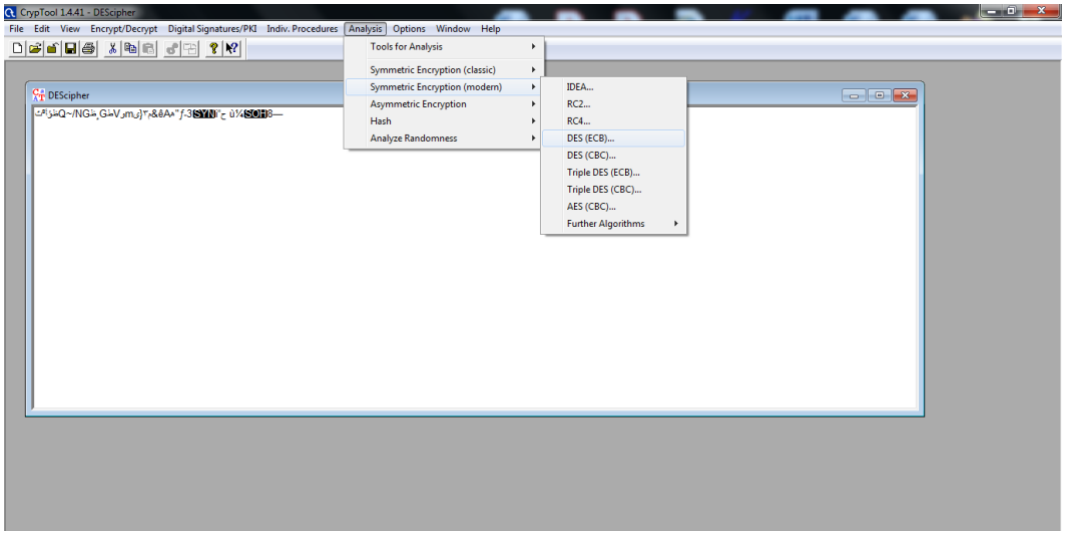
Question 1 **A DES encrypted message is given in the DES_cipher.txt file. You have been lucky; you have seen some part of the key 12 34 56 78 90 ** ** **. With the help of Cryptool 1, break the key and decipher the given text.**

a) How long time will it take you to compromise the complete key by using a brute force attack?
b) What is the complete secret key?
c) What is the decrypted text?

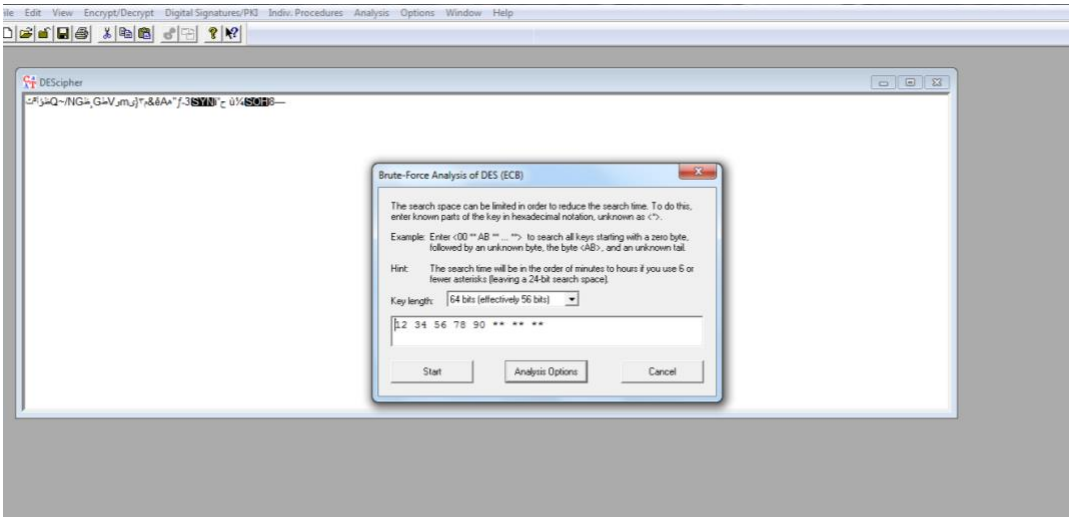
The first step was to use the text



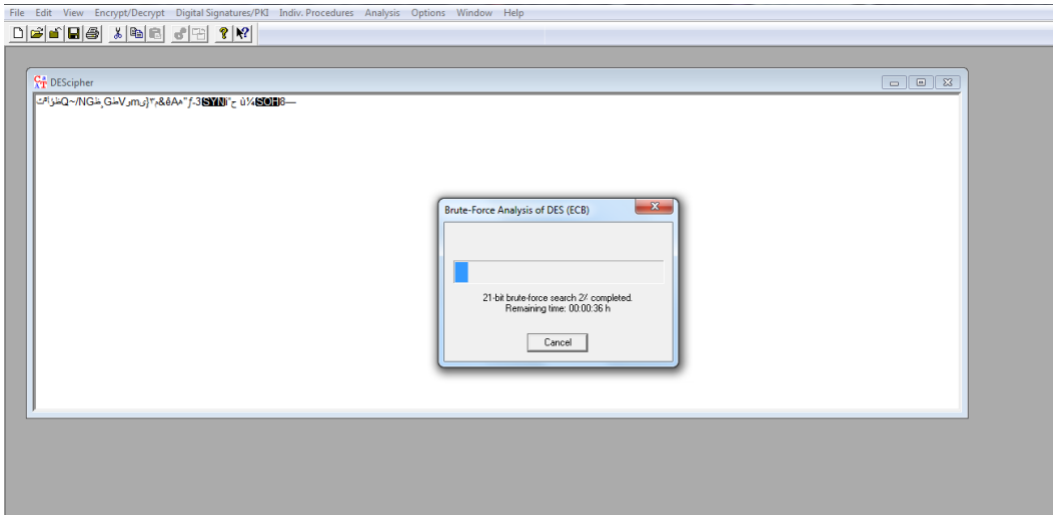
Use from a list (analysis) – (symmetric encryption modern) – (DES (ECB)).



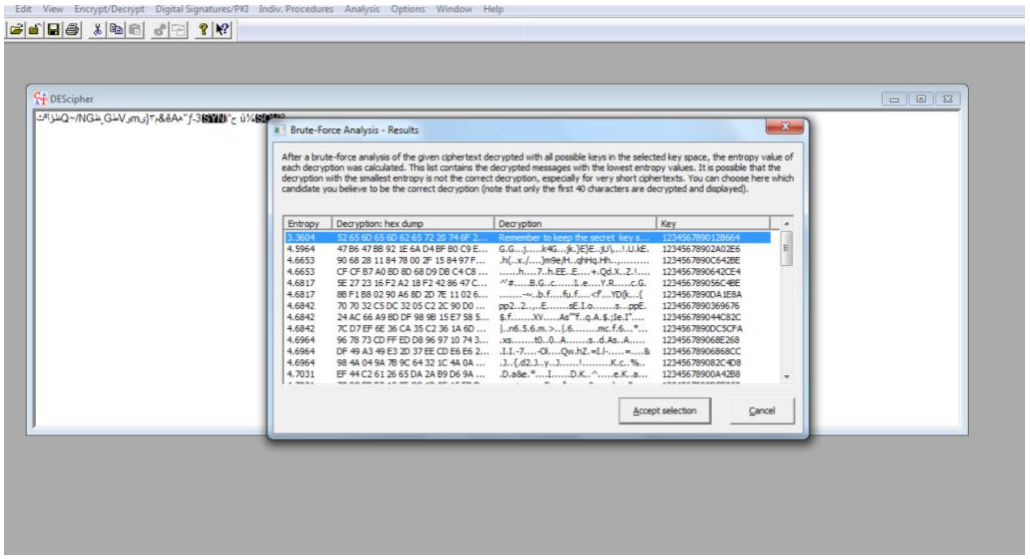
And add the existing key



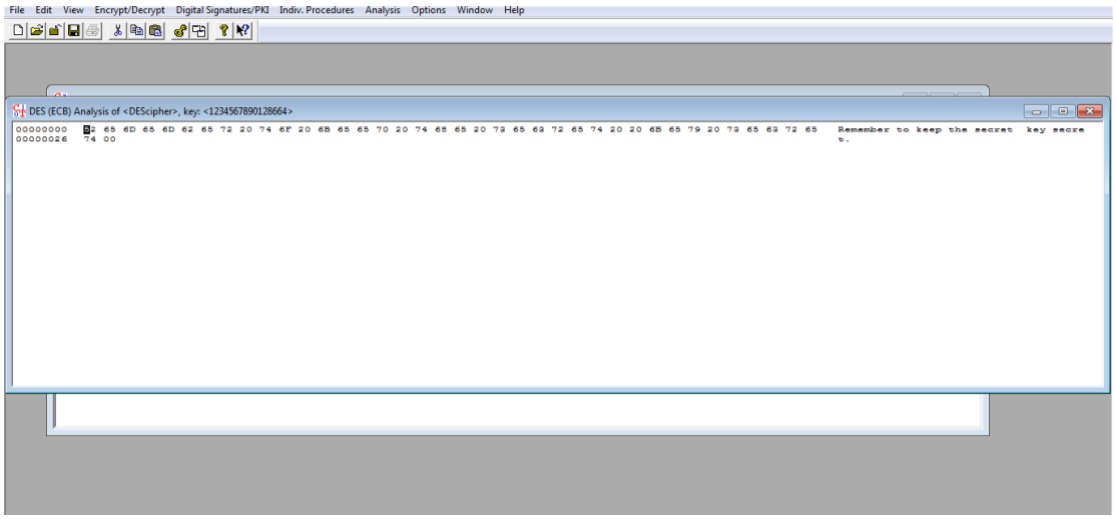
Brute force analysis of DES and remaining time 36s .



Results



Finally its DES cipher from key .



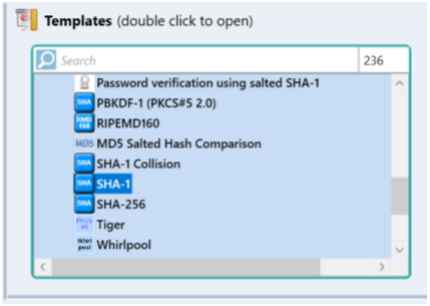
Question 1 **In the Cryptool 2, develop your own RSA digital signature generation and verification component.**

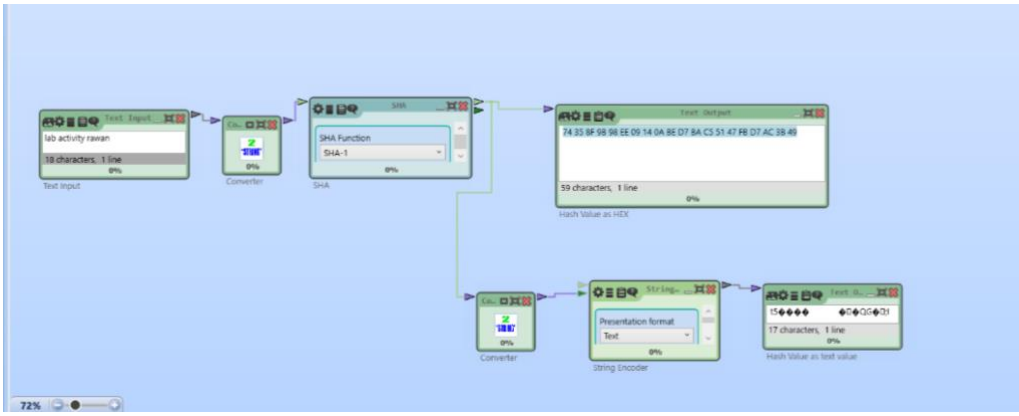
a) Generate the hash value using built-in SHA-1 module .
b) Generate public and private key using built-in RSA Key Generation module .
c) Encrypt has value using built-in RSA Cipher module .
d) Display Signature in text format.
e) Develop Signature Verification component and display result in text format

A) Generate the hash value using built-in SHA-1 module

message is " lab activity rawan "

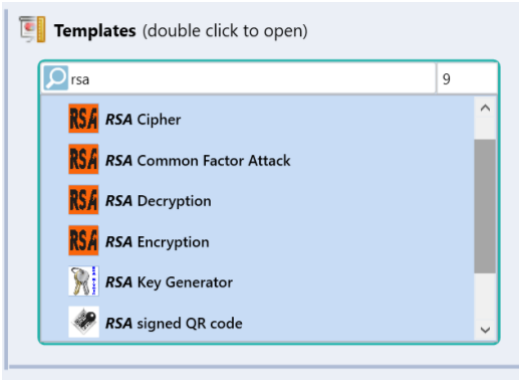
In template search choose for SHA1 Generating the hash value as HEX and text value is an shown below:

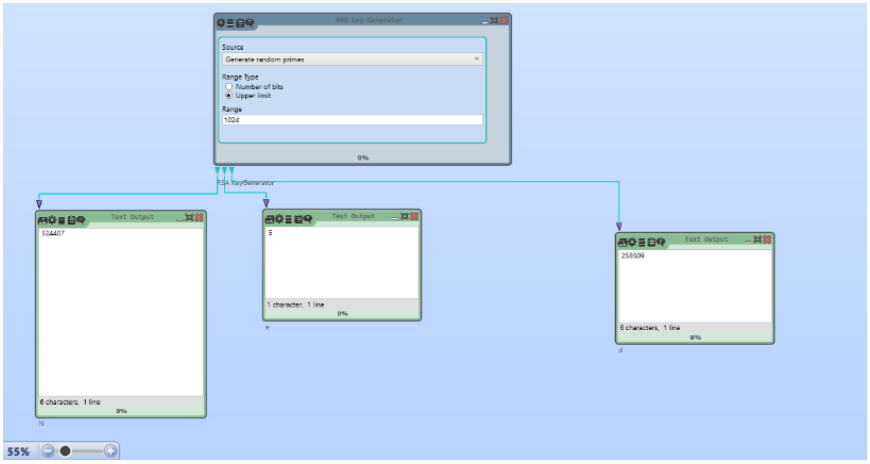




B) Generate public and private key using built-in RSA Key Generation module

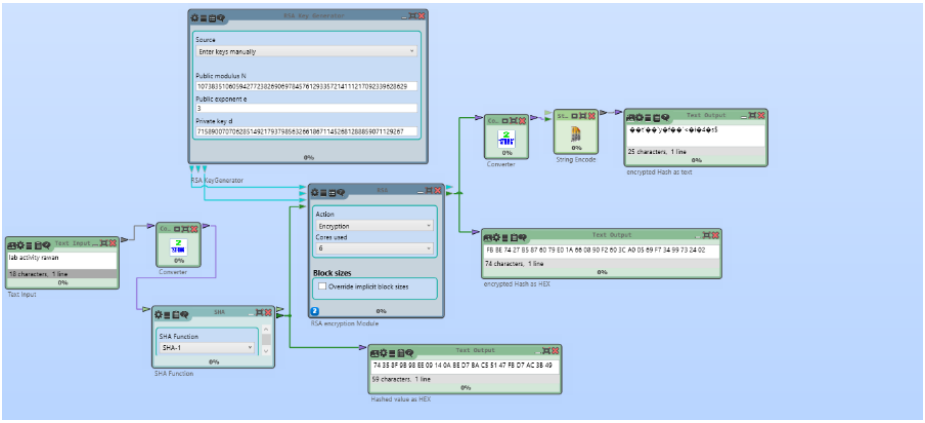
In template search choose for RSA ,using the RSA key generator we generate the following output





C) Encrypt has value using built-in RSA Cipher module

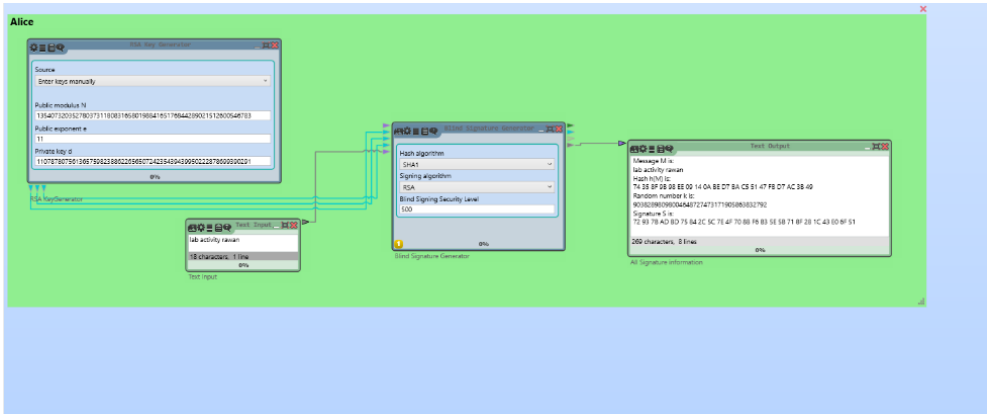
In template search choose for RSA and need to change all the parameter to match Q2.B , and to change the input of the RES encryption, add converter after RES module and connect the string encoder to encrypted hash value as text than play to result .



D) Display Signature in text format.

Signature is the hash value of message that encrypted using RSA encpryption module that be send to reciver and the reciver will get the message and encrypted hash value t1hat he will decrypt it by using sender public key and generate hash value the message then reciver will compare both hash the message verified as genuine message .

In template search for signature RSA , change the signature generator to be hash algorithm = SHA1 , signing algorithm = RSA and leave the signing security level is =500



E) Develop Signature Verification component and display result in text format

Change the signature generator to be hash algorithm , SHA1

Add SHA1 module and connected it to BS generator

Add comparators module and connect the two values need to compare original hash value of the message coming from converter and BS verifier value that coming from the converter .