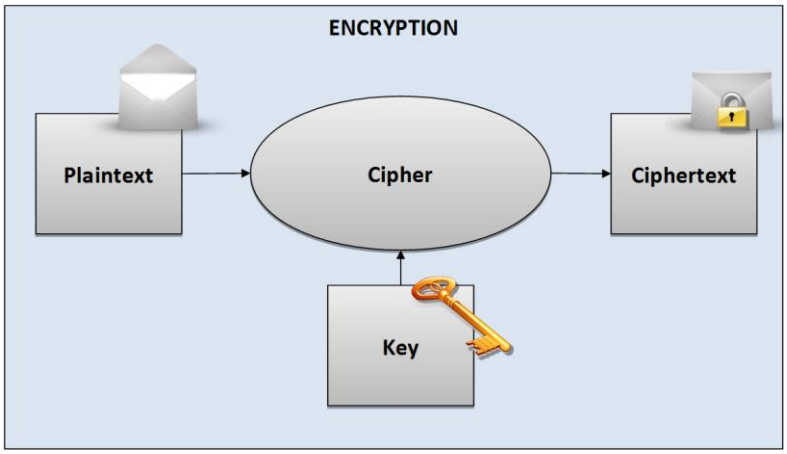
1 Introduction

The purpose of encryption is to change data in such a way that only an authorized recipient can reconstruct the plaintext. This allows us to transmit data without worrying about it getting into unauthorized hands. Authorized recipients possess a piece of secret information called the key which allows them to decrypt the data while it remains hidden from everyone else.



2 Security definitions and the importance of cryptology

2.1 Computational, conditional or practical security

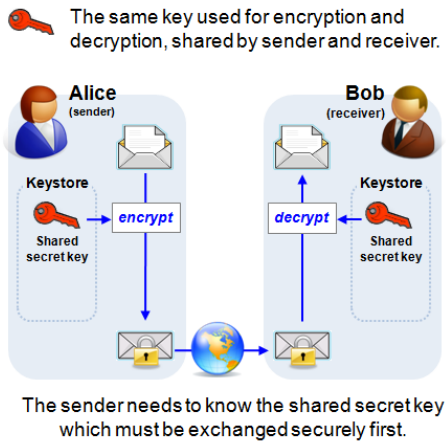
A cipher is computationally secure if it is theoretically possible to break such a system but it is infeasible to do so by any known practical means. Theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these solutions to be continually adapted.

2.2 Information-theoretical or unconditional security

A cipher is considered unconditionally secure if its security is guaranteed no matter how much resources (time, space) the attacker has so even in the case where the adversary has unlimited resources for breaking a cipher. Even with unlimited resources, an adversary is unable to gain any meaningful data from a ciphertext.

3 Symmetric encryption

For symmetric encryption sender and recipient must have a common (secret) key which they have exchanged before actually starting to communicate. The sender uses this key to encrypt the message and the recipient uses it to decrypt it.



The advantages of symmetric algorithms are the high speed with which data can be encrypted and decrypted. One disadvantage is the need for key management. To communicate with one another confidentially, sender and recipient must have exchanged a key using a secure channel before actually starting to communicate.

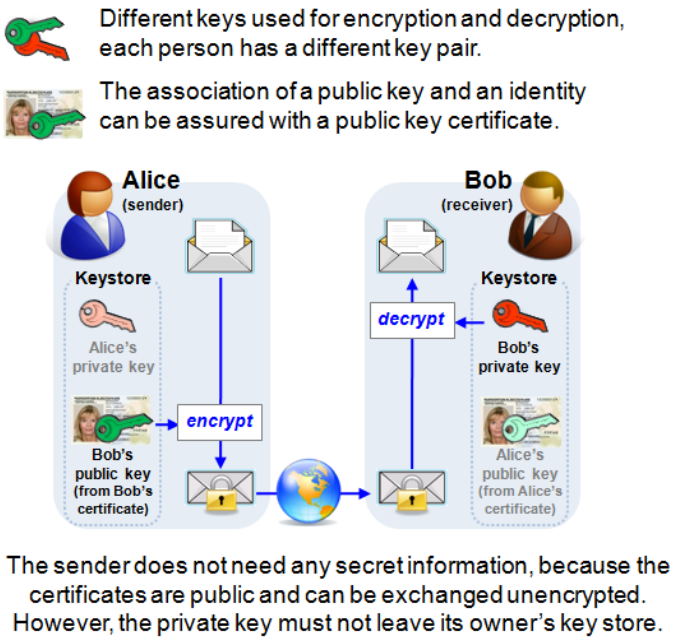
3.1 AES (Advanced Encryption Standard)

Before AES, the most well-known modern symmetric encryption procedure was the DES algorithm. The DES algorithm has been developed by IBM in collaboration with the National Security Agency (NSA) and was published as a standard in 1975. Even though the procedure is relatively old, no effective attack on it has yet been detected. The most effective way of attacking consists of testing (almost) all possible keys until the right one is found (brute-force-attack).

Due to the relatively short key length of effectively 56 bits (64 bits, which however include 8 parity bits), numerous messages encrypted using DES have in the past been broken. Therefore, the procedure cannot be considered secure any longer. Alternatives to the DES procedure include IDEA, Triple-DES (TDES) and especially AES.

4 Asymmetric encryption

In the case of asymmetric encryption, each subscriber has a personal pair of keys consisting of a secret key and a public key. The public key, as its name implies, is made public (e.g. in a key directory on the Internet (this kind of bill-board" is also called a directory or public keyring) or within a so-called public-key cate.

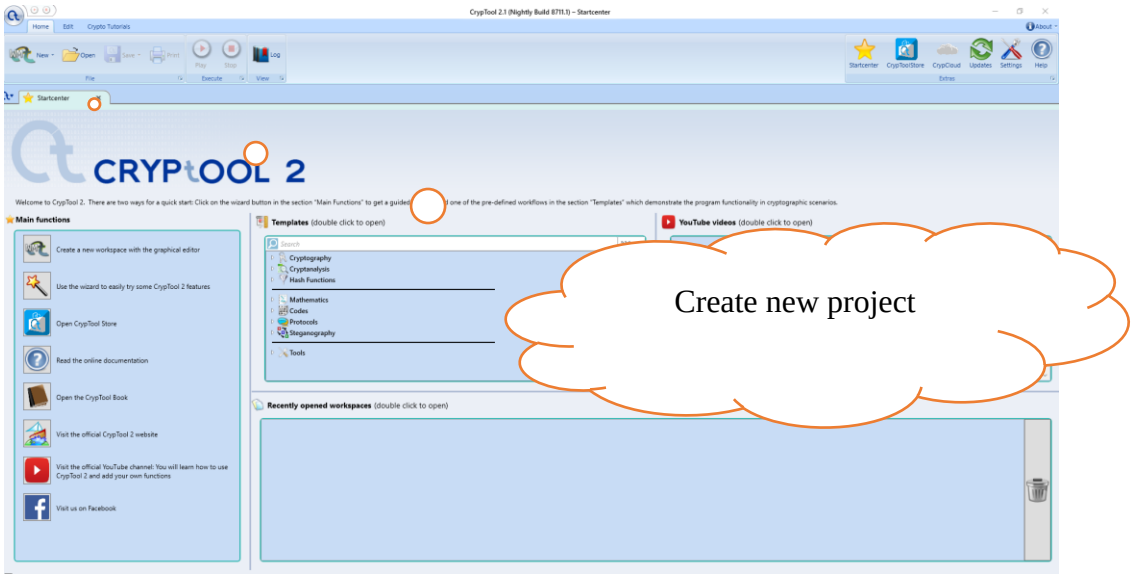


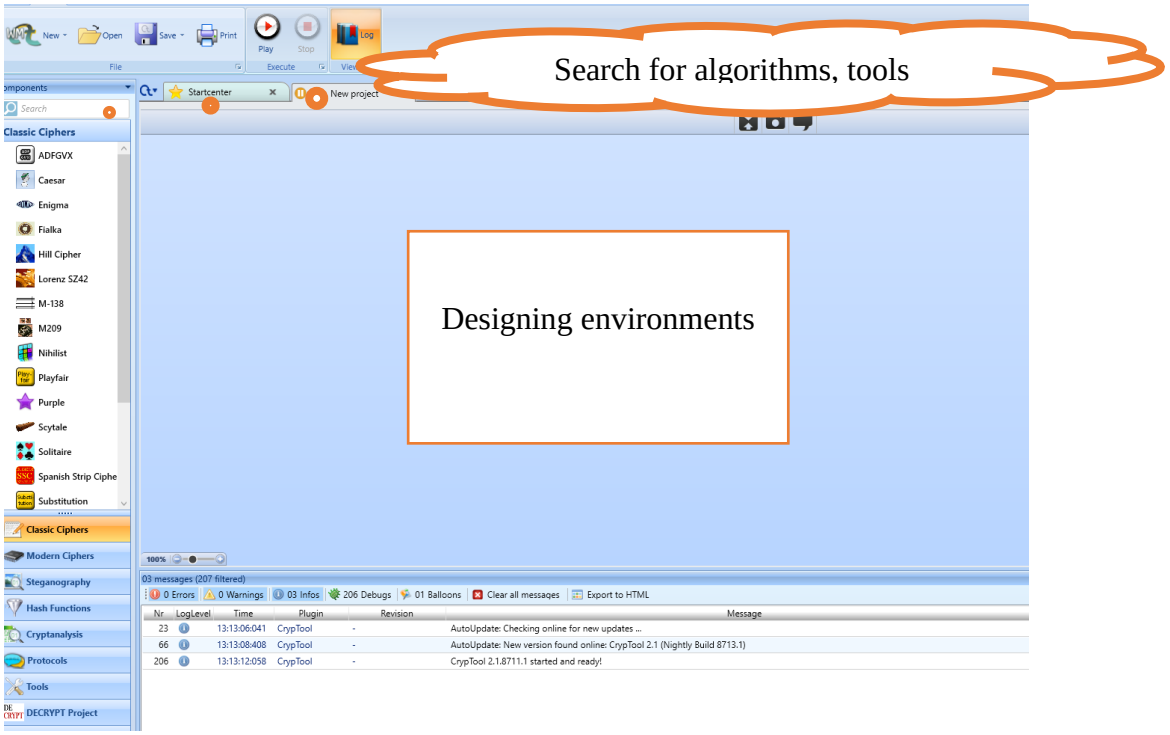
If Alice wants to communicate with Bob, then she looks for Bob's public key and uses it to encrypt her message to him. She then sends this ciphertext to Bob, who is then able to decrypt it again using his secret key. As only Bob knows his secret key, only he can decrypt messages addressed to him. Even Alice who sends the message cannot restore plaintext from the (encrypted) message she has sent. Of course, you must first ensure that the public key cannot be used to derive a private key.

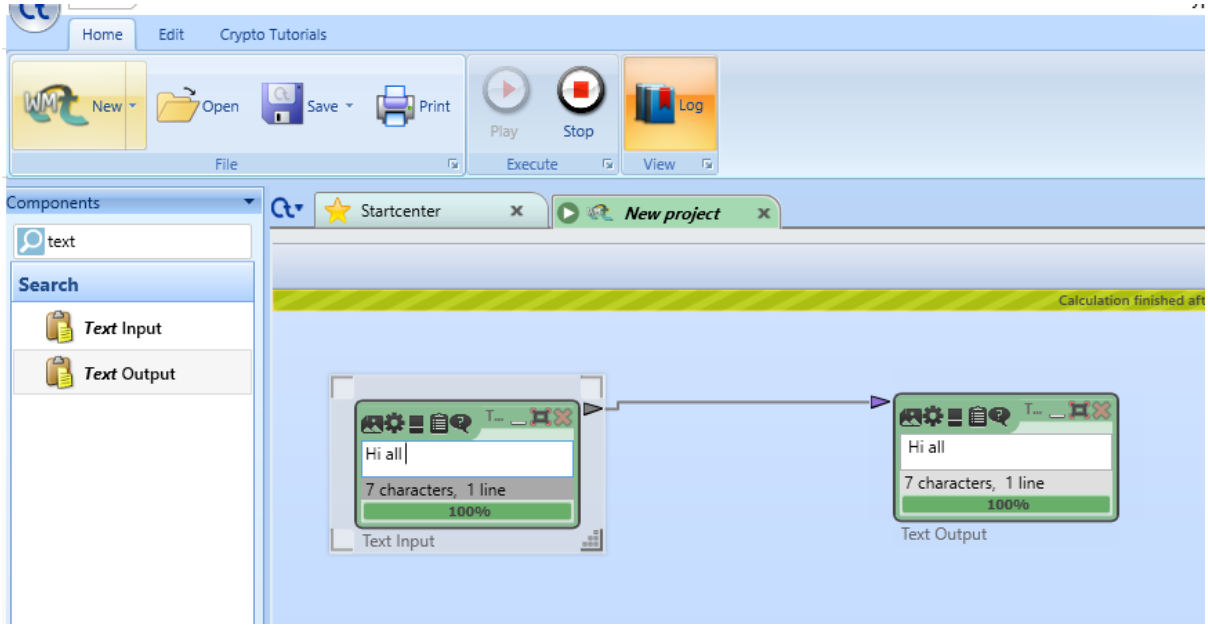
4.1 RSA (Rivest, Shamir and Adleman)

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption and was one of the first great advances in public-key cryptography. RSA is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

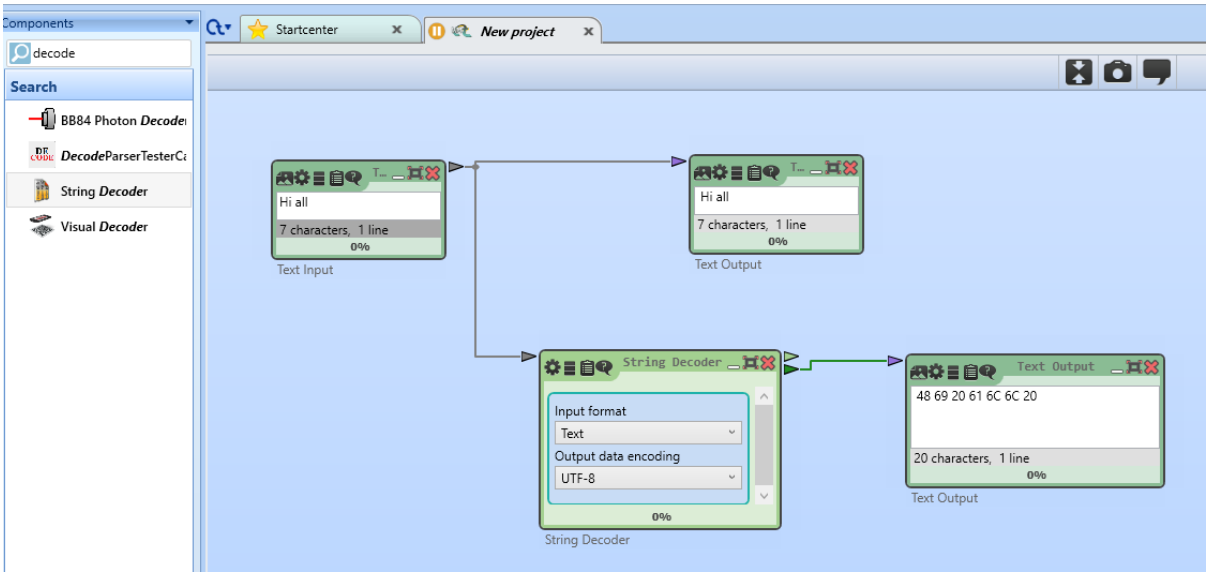
1 Cryptool 2 environment and cryptographic algorithms



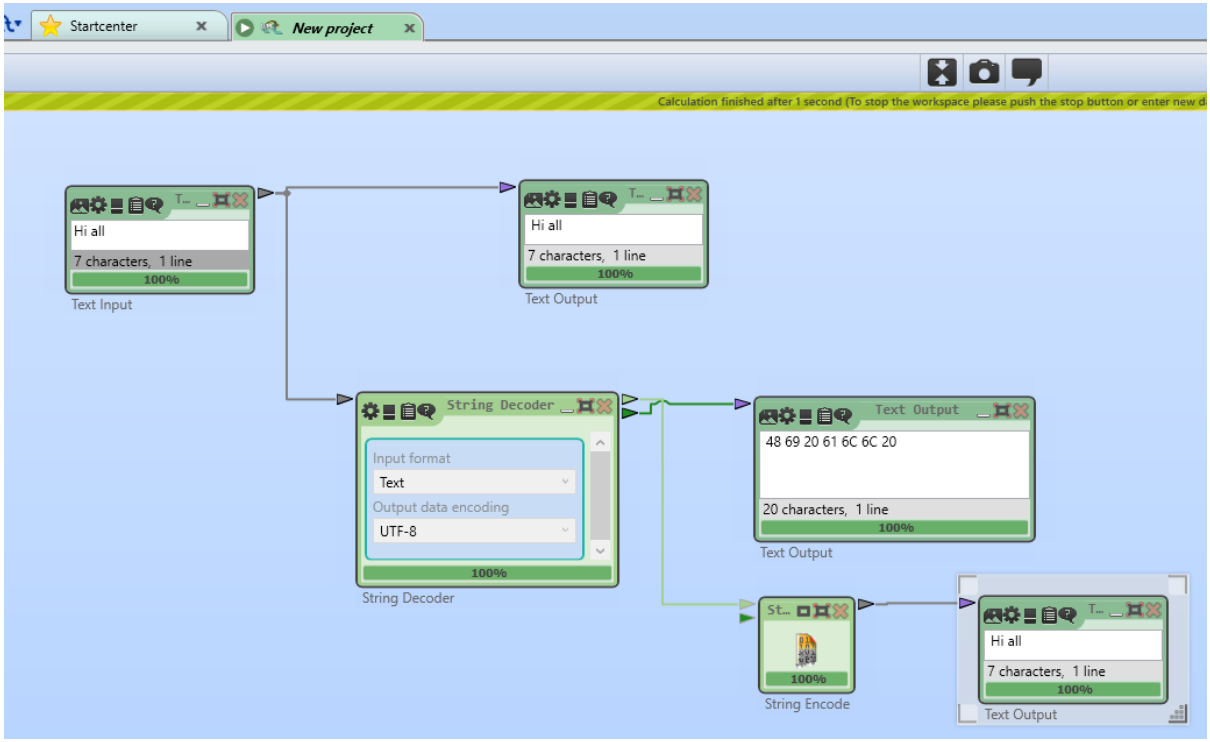




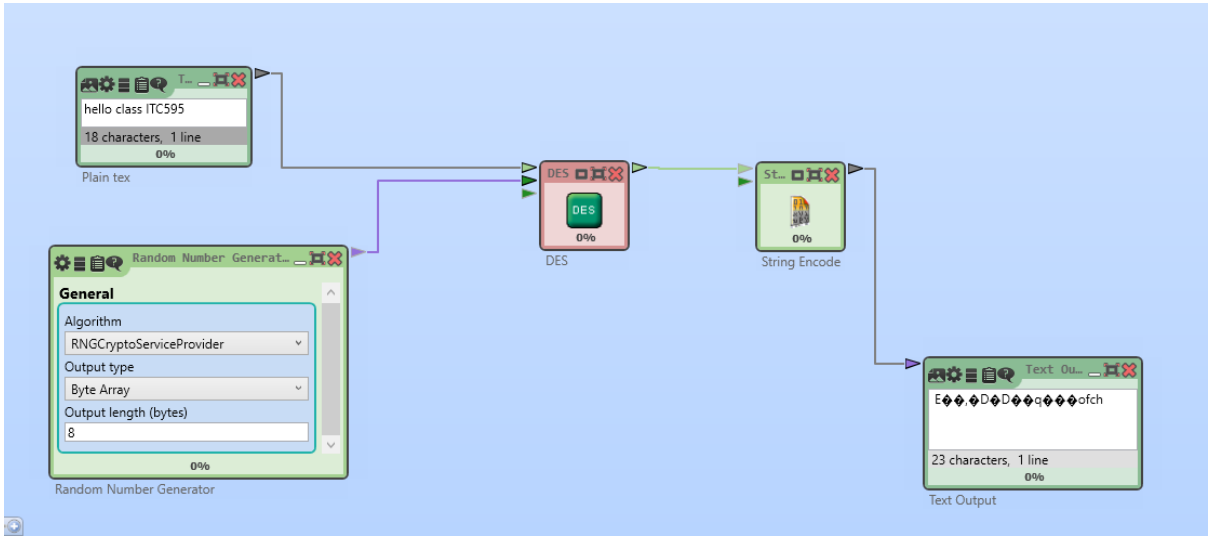
Search for text input and output, link them, run Cryptool.



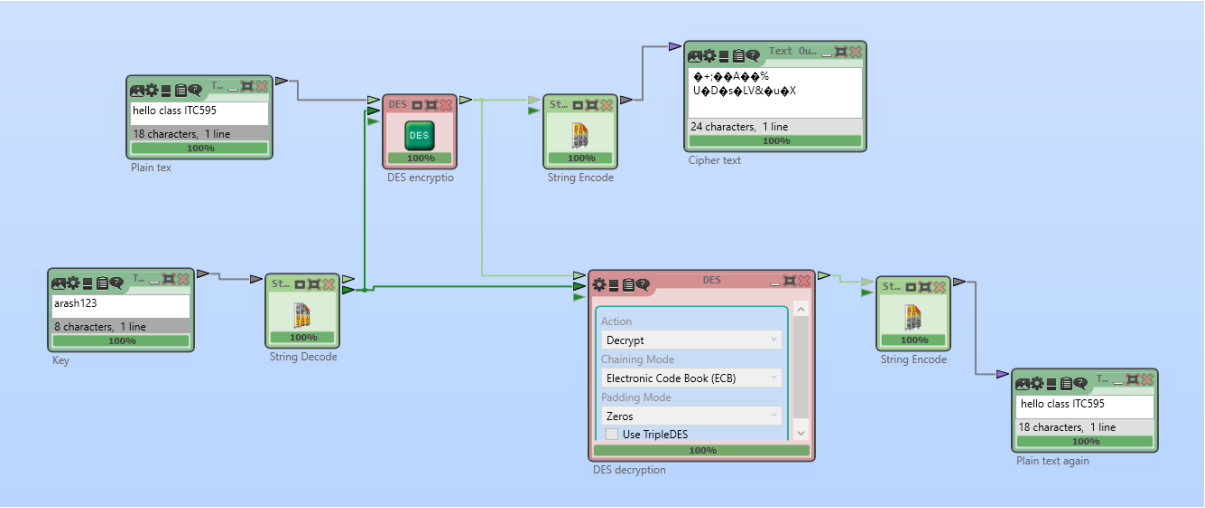
Convert string to UTF-8



Convert back UTF-8 to a string using string encode.



Search for DES algorithm, search for random number tool with 8 bytes to encrypt a string



Decrypt ciphertext using the same key using 8 bytes string.

1 Question:

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

1.1 In this task, you are required to decipher the following ciphertext using the Caesar cipher technique.

Ciphertext = MN JAJWDTSJ N FR AJWD MFUUD YT YFPJ NHY595 MTUJ YT LJY MNLM XHTWJ NS YMNX XZGOJHY

1.2 Breaking the cipher

1. Use the CryptoTool2 software to find the substitution cipher in the Cyphertext above in this task. To find the shift value, you should use the frequency analysis.

2. Now try deciphering the Ciphertext using the following table:

0		9	I	18	R
1	A	10	J	19	S
2	B	11	K	20	T
3	C	12	L	21	U
4	D	13	M	22	V
5	E	14	N	23	W
6	F	15	O	24	X
7	G	16	P	25	Y
8	H	17	Q	26	Z

3. What is the plain text?
4. In CrypTool 2, create a Caesar cipher with 13 shift values for the message "I have fun".

2 Question 2

Design software to encrypt a text file with an Advanced Encryption Standard (AES) algorithm in CrypTool2.

1. Encryption of a file with the AES cipher using the content of the component "Key" as key and the parameters of the AES component for key size, block mode and padding. For 128 bit AES, you should enter 32 hex characters as the key. Non-hex characters are extracted by the "StringDecoder" component.
   First, you have to open a file using the component "File Input": To do so you can either click within this component on the icon "Maximize" or "Fullscreen" (which is the same as double-clicking this component). Alternatively, you can select the "File Input" component and open a file with the button in its parameter bar.

2. Now keep the key, and develop a system to decrypt the file/message

3 Question 3:

Design software to encrypt a message with RSA algorithm using an RSA key generator.

3.1 Encrypt the message with RSA public

3.2 Decrypt message with a private key

END of Tutorial