Experiment no.: 03

Title: Create Digital Signature document using Cryptool.
Course outcome: Demonstrate the use of cryptool.
Theory:

A **digital signature** is a cryptographic technique used to verify the **authenticity, integrity, and non-repudiation** of a digital document. It ensures that the document has not been altered after signing and that it truly originates from the claimed sender.

CrypTool is an educational software that demonstrates various cryptographic algorithms and techniques, including the creation of digital signatures. In this process, the sender generates a **hash value** of the document using a hashing algorithm (like SHA-256) and then encrypts this hash with their **private key**. The resulting encrypted hash is the **digital signature**. The receiver can verify the signature by decrypting it with the sender's **public key** and comparing the hash values.

This method ensures secure communication by confirming the sender's identity and maintaining document integrity. Using CrypTool helps visualize and understand how real-world digital signatures function in cybersecurity and electronic authentication systems.

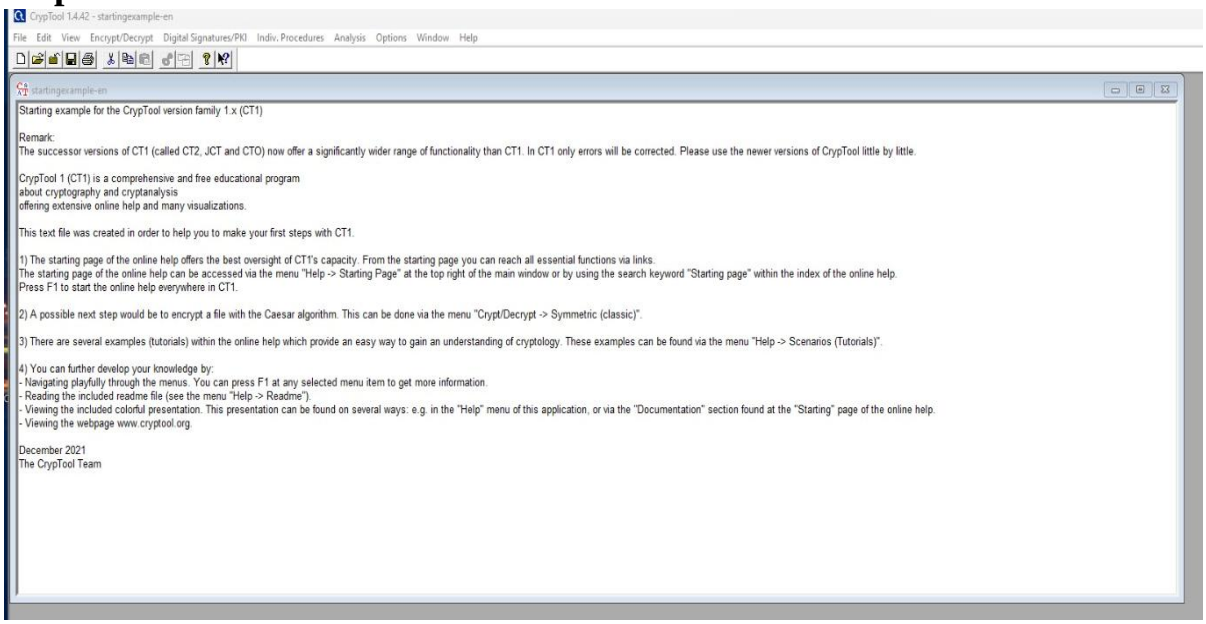
Advantages:

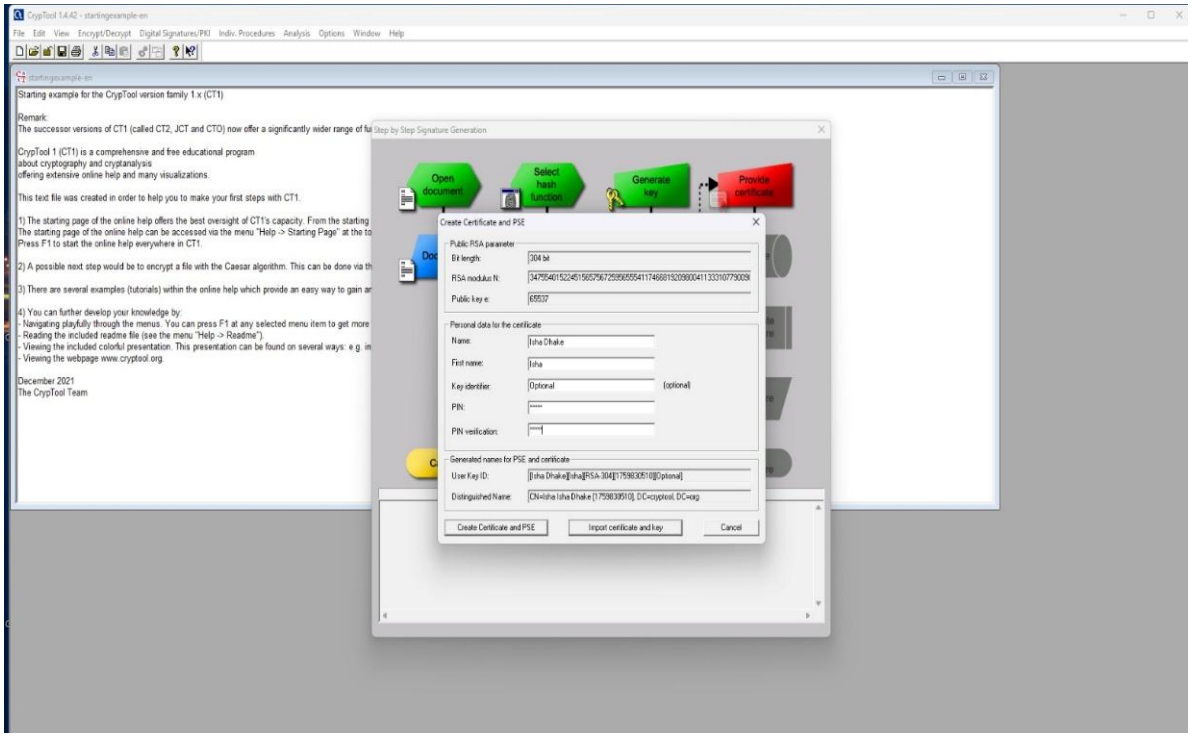
- **Authenticity:** Confirms the identity of the sender.
- **Integrity:** Ensures that data has not been changed during transmission.
- **Non-repudiation:** Prevents the sender from denying ownership of the signature later.
- **Security:** Protects against tampering and forgery.

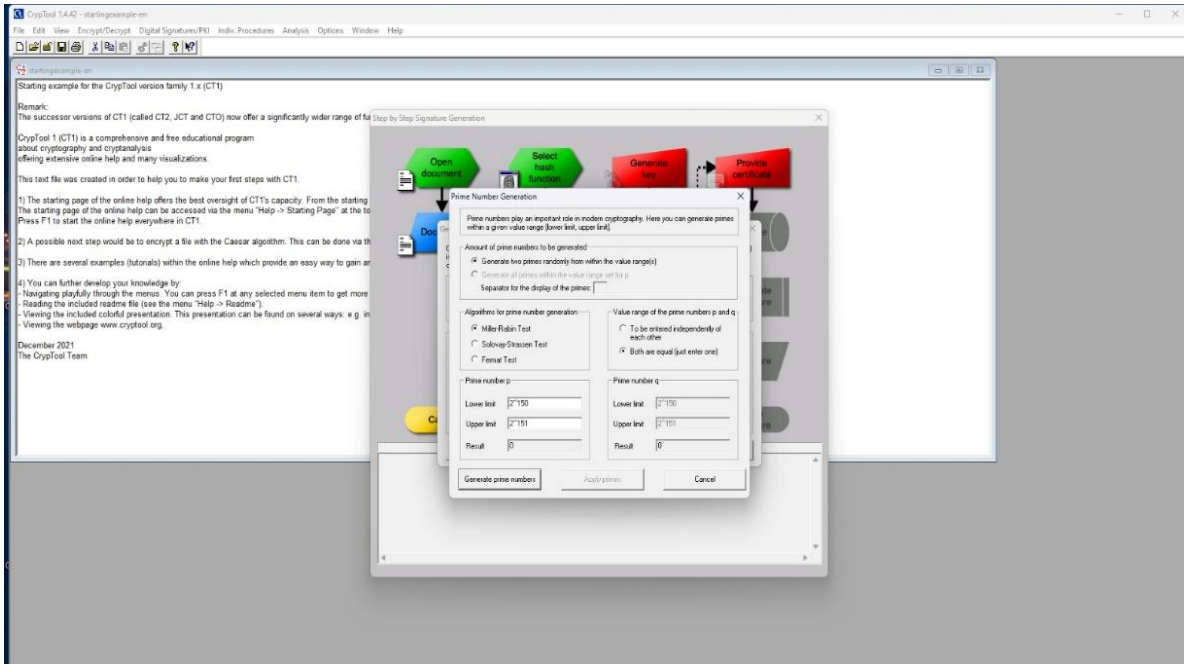
Applications:

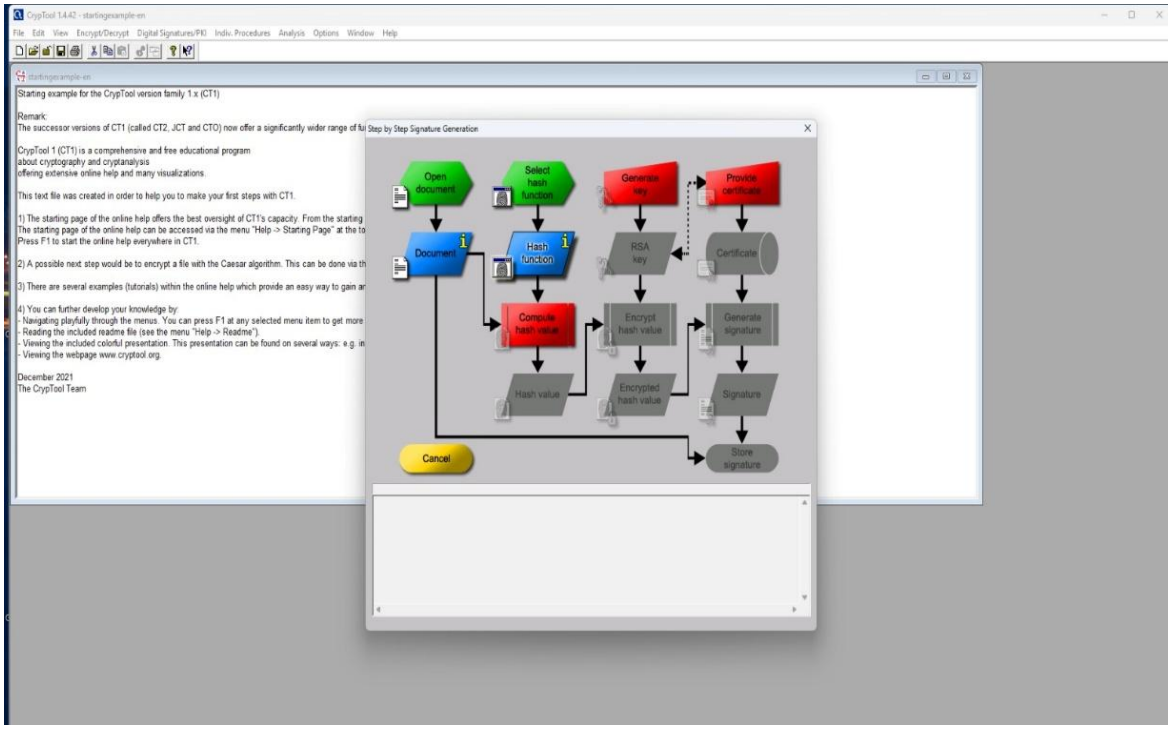
Digital signatures are widely used in **online banking, government services, legal contracts, and e-commerce** to secure communications and verify identities.

Steps:


CrypTool 1.4.42 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
Remark:
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.
CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.
This text file was created in order to help you to make your first steps with CT1.
1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CT1.
2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (classic)".
3) There are several examples (tutorials) within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".
4) You can further develop your knowledge by:
- Navigating playfully through the menus. You can press F1 at any selected menu item to get more information.
- Reading the included readme file (see the menu "Help -> Readme").
- Viewing the included colorful presentation. This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help.
- Viewing the webpage www.cryptool.org.
December 2021
The CrypTool Team


Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Create Certificate and PSE
Public RSA parameter
Bit length:
304 bit
RSA modulus N:
Public key e:
65537
Personal data for the certificate
Name:
Isha Dhake
First name:
Isha
Key identifier:
Optional
(optional)
PIN:
PIN verification:
Generated names for PSE and certificate
User Key ID:
Distinguished Name:
Create Certificate and PSE
Import certificate and key
Cancel





Conclusion:

I have successfully created and verified a digital signature, ensuring the authenticity and integrity of the message.