1. Install Jscript/Cryptool tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures.

Aim :

Demonstration in JavaScript and Cryp tool of asymmetric and symmetric cryptography, hashing, and digital signatures.The goal of the CrypTool is to help and encourage people to understand cryptography and the underlying technologies. It demonstrates current state-of-the-art cryptographic technologies

**CrypTool**

is an open-source software tool for learning about cryptography and cryptanalysis. It provides a hands-on environment for users to experiment with different encryption and decryption algorithms, attack methods, and cryptographic concepts. CrypTool is widely used in educational settings and by those interested in understanding the principles of cryptography.

### Key Features of CrypTool

1. **Interactive Learning Platform**  
   CrypTool offers an interactive and visual environment for learning cryptographic algorithms, allowing users to input data and view step-by-step how the encryption and decryption processes work.
2. **Support for Various Cryptographic Algorithms**  
   CrypTool includes support for a wide range of cryptographic algorithms, including:
   * **Classical Ciphers**: Caesar cipher, Vigenère cipher, Enigma machine, etc.
   * **Modern Symmetric Algorithms**: AES (Advanced Encryption Standard), DES (Data Encryption Standard), etc.
   * **Public-Key Algorithms**: RSA, Diffie-Hellman, ElGamal, ECC (Elliptic Curve Cryptography), etc.
   * **Hash Functions**: MD5, SHA family (SHA-1, SHA-2), etc.
   * **Digital Signatures**: RSA signatures, DSA (Digital Signature Algorithm), etc.
3. **Cryptanalysis Tools**  
   CrypTool enables users to perform cryptanalysis (breaking encryption) on ciphers using various attack techniques, such as frequency analysis, brute force, and pattern recognition.
4. **Tutorials and Exercises**  
   CrypTool provides built-in tutorials and exercises that guide users through different cryptographic concepts, making it an excellent tool for students and professionals looking to strengthen their cryptography skills.
5. **Visualization of Cryptographic Processes**  
   It allows users to visualize the mathematical processes behind encryption algorithms. For example, users can see how key generation works, how ciphertexts are formed, and how they are decrypted.
6. **Multiple Variants**  
   CrypTool is available in multiple versions tailored for different purposes:
   * **CrypTool 1 (CT1)**: A classic version that is highly educational, offering a wide variety of cryptographic algorithms.
   * **CrypTool 2 (CT2)**: Provides a more modern interface and is designed for both beginners and advanced users with additional features like graphical programming of cryptographic processes.
   * **JCrypTool**: A Java-based version with a user-friendly interface, aimed at providing platform independence.
   * **CrypTool Online**: A web-based version that doesn’t require installation and allows users to experiment with cryptographic algorithms directly in a browser.
7. **Security Protocols and Concepts**  
   In addition to cryptographic algorithms, CrypTool supports experimentation with security protocols like SSL/TLS, demonstrating how cryptography is used in practice.
8. **Open Source**  
   Being open-source, CrypTool's code is available for anyone to inspect, modify, or improve. This makes it a transparent and flexible tool for research, development, and learning.

### Typical Uses of CrypTool

* **Educational Use**: It's widely used in schools, universities, and cryptography courses to teach both classical and modern cryptography.
* **Research**: Researchers use CrypTool to test algorithms, simulate attacks, and develop new cryptographic techniques.
* **Practical Use**: Those who want to understand the security behind cryptographic methods can use CrypTool to simulate and understand how encryption algorithms are applied in real-world scenarios.

### Example Scenarios

1. **Classical Cryptography**: You can use CrypTool to encrypt a message using the Caesar cipher, perform frequency analysis on the ciphertext, and break the encryption without knowing the key.
2. **RSA Encryption**: Learn how public and private keys are generated in RSA, encrypt a message using the public key, and decrypt it using the private key.
3. **Hash Functions**: Experiment with hash functions like MD5 or SHA to see how small changes in the input result in vastly different hash outputs (the avalanche effect).
4. **Digital Signatures**: Use CrypTool to create a digital signature and verify it, understanding the principles behind authentication and non-repudiation.

### Getting Started with CrypTool

* **Download**: You can download CrypTool from its official website: [CrypTool.org](https://www.cryptool.org).
* **Use Cases**: After installation, you can start experimenting with its extensive library of algorithms and follow the tutorials for a deeper understanding.

CrypTool is an excellent resource for both beginners wanting to learn the basics of cryptography and for advanced users conducting cryptographic research.