10. Use the Following Tools for Cryptography

10(i) Cryptographic Hashing using HashCalc

Aim

To generate cryptographic hash values using HashCalc.

Tools Used

• HashCalc Tool
• Windows Operating System

Theory

HashCalc is a hashing utility used to calculate hash values such as MD5, SHA-1, and SHA-256. Hash functions are used to ensure data integrity by generating a fixed-length digest for any input data.

Steps / Procedure

1. Download and install HashCalc.
2. Launch the HashCalc application.
3. Select the file or enter the text to be hashed.
4. Choose the hashing algorithms (MD5, SHA-1, SHA-256).
5. Click on **Calculate**.
6. Observe the generated hash values.
7. Modify the input data slightly.
8. Recalculate and compare hash values.

Result

Hash values were successfully generated and data integrity was verified using HashCalc.

10(ii) Encryption and Decryption using Advanced Encryption Package (AEP)

Aim

To encrypt and decrypt files using Advanced Encryption Package.

Tools Used

- Advanced Encryption Package (AEP)
- Windows Operating System

Theory

Advanced Encryption Package is a cryptographic tool used to secure data using strong encryption algorithms such as AES. It ensures confidentiality by converting plain data into unreadable ciphertext.

Steps / Procedure

1. Download and install Advanced Encryption Package.
2. Launch the AEP application.
3. Select the file to be encrypted.
4. Choose the encryption algorithm.
5. Set a strong password or key.
6. Click on **Encrypt** to secure the file.
7. Select the encrypted file.
8. Enter the password to decrypt the file.
9. Verify the decrypted file content.

Result

Files were successfully encrypted and decrypted using Advanced Encryption Package.

10(iii) Disk Encryption using TrueCrypt

Aim

To secure data using disk encryption with TrueCrypt.

Tools Used

- TrueCrypt
- Windows Operating System

Theory

TrueCrypt is a disk encryption software that creates encrypted volumes to protect sensitive data from unauthorized access.

Steps / Procedure

1. Download and install TrueCrypt.
2. Launch the TrueCrypt application.
3. Click on **Create Volume**.
4. Select **Create an encrypted file container**.
5. Choose encryption algorithm.
6. Set volume size.
7. Create a strong password.
8. Mount the encrypted volume.
9. Store files inside the encrypted volume.
10. Dismount the volume after use.

Result

Encrypted storage volume was successfully created using TrueCrypt.

10(iv) Cryptography Demonstration using CrypTool

Aim

To demonstrate cryptographic algorithms using CrypTool.

Tools Used

- CrypTool
- Windows Operating System

Theory

CrypTool is an educational cryptography tool used to demonstrate classical and modern encryption algorithms, hash functions, and digital signatures.

Steps / Procedure

1. Download and install CrypTool.
2. Launch the CrypTool application.
3. Enter plaintext message.
4. Select encryption algorithm (AES, RSA, DES).
5. Encrypt the plaintext.
6. Observe the ciphertext.
7. Decrypt the ciphertext using the same key.
8. Verify the original message.

Result

Cryptographic algorithms were successfully demonstrated using CrypTool.

Final Conclusion

Practical No. 10 successfully demonstrated the use of cryptographic tools for hashing, encryption, disk security, and cryptography concepts.