11111

by C P

Submission date: 18-Apr-2022 12:20PM (UTC-0500)
Submission ID: 1813664048
File name: cryptography.docx.docx (19.53K)
Word count: 504
Character count: 3006

This is a console based application which showcase the use of the following cryptographic functions:

- **Public Key Generation –** The algorithms using this type of cryptography uses the different keys for encryption and decryption.
- **Symmetric Key Encryption –** The algorithms using this type of cryptography uses the similar key for encryption as well as decryption.
- **Cryptographic Hashes** – It is an algorithm that takes an arbitrary amount of data input, a credential and produces a fixed-size output of enciphered text called a hash value.
- **Digital Signatures** – It is a mechanism to check the authentication of the sender.
- **Base64 Encoding -** Base64 encoding converts every three bytes of data (three bytes is 3*8=24 bits) into four base64 characters.

These cryptographic functions are being useful for securely transmission of data. Due to the cryptography user's data will be secure enough. Different cryptographic functions are used in the different situations such as cryptographic hashes can be used where user's password is to be saved, digital signatures for the authentication of the user, etc.

The four main benefits of using the cryptographic functions are :

- **Confidentiality** – Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** – The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** – The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

About code :

The above described five cryptographic functions are implemented in the single java file attached with it.

When the application starts, users will be asked to choose which cryptographic functions is to be used. It is implemented with the switch case.

If user enters ,

1 then public key cryptography will be used for encryption and decryption.

2 then symmetric key cryptography will be used for encryption and decryption.

3 then cryptographic hashes will be used for encryption.

4 then digital signatures will be used for authentication of sender.

5 then Base64 encoding technique will be used for encoding and decoding.

In the implementation, RSA algorithm is used.

- `KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance("RSA");`

KeyPairGenerator class is used to create the pair of keys used for public key cryptography. getInstance() is used to define the cryptographic algorithms to be used such as RSA.

- `KeyPair keyPair = keyPairGenerator.genKeyPair();`

KeyPair class is being used to generate the public key and private key. KeyPairGenerator class has the method genKeyPair() to generate the keys.

- `byte[] plainTextInByte = plainText.getBytes();`

This line of code converts the plain text to binary form.

- `Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");`

Cipher class is used in the public key cryptography.

- ```
  cipher.init(Cipher.ENCRYPT_MODE, publicKey);
  ```

ENCRYPT_MODE is used for encryption process.

- ```
  cipher.init(Cipher.DECRYPT_MODE, privateKey);
  ```

DECRYPT_MODE is used for decryption process.

- ```
  String encodedText = Base64.getEncoder().encodeToString(plainText.getBytes(
  "UTF-8"));
  ```

To encode the text in base64 encoded format.

- ```
  byte[] decodedArray = Base64.getDecoder().decode(encodedText);
  ```

To decode the text form base64 encoded format.

11111

ORIGINALITY REPORT

27%	24%	3%	21%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

20%

★ www.coursehero.com

Internet Source

Exclude quotes	Off	Exclude matches	< 10 words
Exclude bibliography	On		