ASYMMETRIC ENCRYPTION AND DECRYPTION

Blockchain Technology

Time: 60 mins

Introduction

In this class, the student/s will learn to secure the access by encrypting and decrypting the data using the keys generated with complex algorithms.

New Commands Introduced

● random.randint(2**8, 2**9)	Finds a random number between 2 exponential 8 times and 2 exponential 9 times
● ord(char)	FInds the ASCII value of a character
● .join	Joins the characters

Vocabulary

- **Encryption** is the process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it.
- A **public key** can be given to any person with whom an individual wants to communicate, whereas a **private key** belongs to the individual it was created for and isn't shared.
- A **prime number** is a whole number greater than 1 whose only factors are 1 and itself..
- **Co-prime numbers** are pairs of numbers that do not have any common factor other than 1.
- **Exponents,** also known as powers, are values that show how many times to multiply a base number by itself.

Learning Objectives

Student/s should be able to:

- ***Explore*** how keys help to authorize the access to the data.
- ***Explain*** how to generate keys using different mathematical calculations.
- ***Explain*** how to encrypt and decrypt the data.

Activities

1. **Class Narrative:** *(2 mins)*
    - Brief the student/s that they ciphered text but it is still accessible to the unauthorized users and can be secured by encrypting and decrypting the data with keys.

2. **Concept Introduction Activity:** *(5 mins)*

    - Let the student/s play the explore-activity to observe.
    - Ask students to enter the transaction details and observe the output.
    - Introduce the values in the encrypted data as keys and show how encrypted data is decrypted.
    - Explain symmetric and asymmetric encryption decryption and its need.

3. **Activity 1: Create Prime Number Keys** *(10 min)*

    Teacher Activity: *(5 mins)*

    - Explain prime numbers and why we choose prime numbers to generate the keys.
    - Explain how to generate the prime number keys by finding the random number and checking if its prime.

    Student Activity: *(5 mins)*

    - Guide the student/s to generate the prime number keys.

4. **Activity 2: Generate the Public and Private Keys** *(20 min)*

    Teacher Activity: *(10 mins)*

    - Explain why complex calculations need to be performed for secure keys and introduce the RSA algorithm steps.
    - Demonstrate how to find exponential values, modulus to generate the private and public keys.

    Student Activity: *(10 mins)*

    - Guide the student/s to create the public and private keys.

5. **Activity 3: Encrypt and Decrypt the Data** *(10 mins)*

    Teacher Activity: *(5 mins)*

    - Explain the encryption technique by finding the ASCII value for each character, calculating the exponential value and performing modulo operation to achieve the ciphered text with values.
    - Demonstrate encryption using keys.

    Student Activity: *(5 mins)*

    - Guide the students to decrypt the data by finding the ASCII value for each character, calculating the exponential value and performing modulo operation to achieve the deciphered text.

6. **Introduce the Post class project:** *(2 min)*
    - Encrypt the password once entered and decrypt the password while logging in.

7. **Test and Summarize the class learnings:** *(5 mins)*
    - Check for understanding through quizzes and summarize learning after respective activities.
    - Summarize the overall class learning towards the end of the class.
8. **Additional activities:**
    - Encourage the student/s to debug the `isPrime()` function to find the prime numbers as a key.
    - Encourage the student/s to find the prime number keys within a specified range.

9. **State the Next Class Objective:** *(1 min)*
    - In the next class, student/s will learn to generate a hash to authenticate the blocks connected in a blockchain.

U.S. Standards:

CSTA: 2-AP-11, 2-AP-12, 2-AP-13, 2-AP-14, 2-AP-19

Links Table		
Activity	**Activity Name**	**Link**
Class Presentation	Asymmetric Encryption and Decryption	https://s3-whjr-curriculum-uploads.whjr.online/d9e2d6f1-95c7-4f30-89b7-5de58eb76d1e.html
Explore Activity	Asymmetric Encryption and Decryption	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS-BP
Teacher Activity 1	Create Prime Number Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-TAS-BP
Teacher Reference: Teacher Activity 1 Solution	Create Prime Number Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-TAS
Student Activity 1	Create Prime Number Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS-BP
Teacher Reference: Student Activity 1 Solution	Create Prime Number Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS
Teacher Activity 2	Generate the Public and Private	https://github.com/Tynker-Blockchai

	Keys	n/TNK-M11-C83-TAS-BP
Teacher Reference: Teacher Activity 2 Solution	Generate the Public and Private Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-TAS
Student Activity 2	Generate the Public and Private Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS-BP
Teacher Reference: Student Activity 2 Solution	Generate the Public and Private Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS
Teacher Activity 3	Encrypt and Decrypt the Data	https://github.com/Tynker-Blockchain/TNK-M11-C83-TAS-BP
Teacher Reference: Teacher Activity 3 Solution	Encrypt and Decrypt the Data	https://github.com/Tynker-Blockchain/TNK-M11-C83-TAS
Student Activity 3	Encrypt and Decrypt the Data	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS-BP
Teacher Reference: Student Activity 3 Solution	Encrypt and Decrypt the Data	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS
Student's Additional Activity 1	Debug the Function	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS-BP
Teacher Reference: Student's Additional Activity 1 Solution	Debug the Function	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS
Student's Additional Activity 2	Create Prime Number Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS-BP
Teacher Reference: Student's Additional Activity 2 Solution	Create Prime Number Keys	https://github.com/Tynker-Blockchain/TNK-M11-C83-SAS
Post Class Project	Encrypt and Decrypt the Password	https://github.com/Tynker-Blockchain/TNK-M11-C83-PCP-BP
Teacher Reference: Post Class Project Solution	Encrypt and Decrypt the Password	https://github.com/Tynker-Blockchain/TNK-M11-C83-PCP