Introduction To Cryptography
Lesson Plan: Class 08 / IP / 01

Overall goal of the lesson: Children will learn the concept of encryption and decryption.
Prior knowledge required: 08-IP-01A Modulo arithmetic
MODULE 1:
Module time: 35 X 1 minutes
Goal: To understand the concept of basic cryptography. Understand Caesar Cipher, use it to encrypt and decrypt a message and to use modulo arithmetic to generalize this approach
Description: Children will learn understand the concept of cryptography, apply the concept of modulo arithmetic and implement the same
Material required:
Physical:

1. One copy of the worksheet per child.
2. Writing material to solve the worksheet: pencil and eraser.

Electronic:
PPT Presentation
Procedure Summary:

1. Run through the presentation
2. Do all the activities that are in the presentation
3. Distribute the worksheets
4. Let children try to solve them in class and help them with the answers

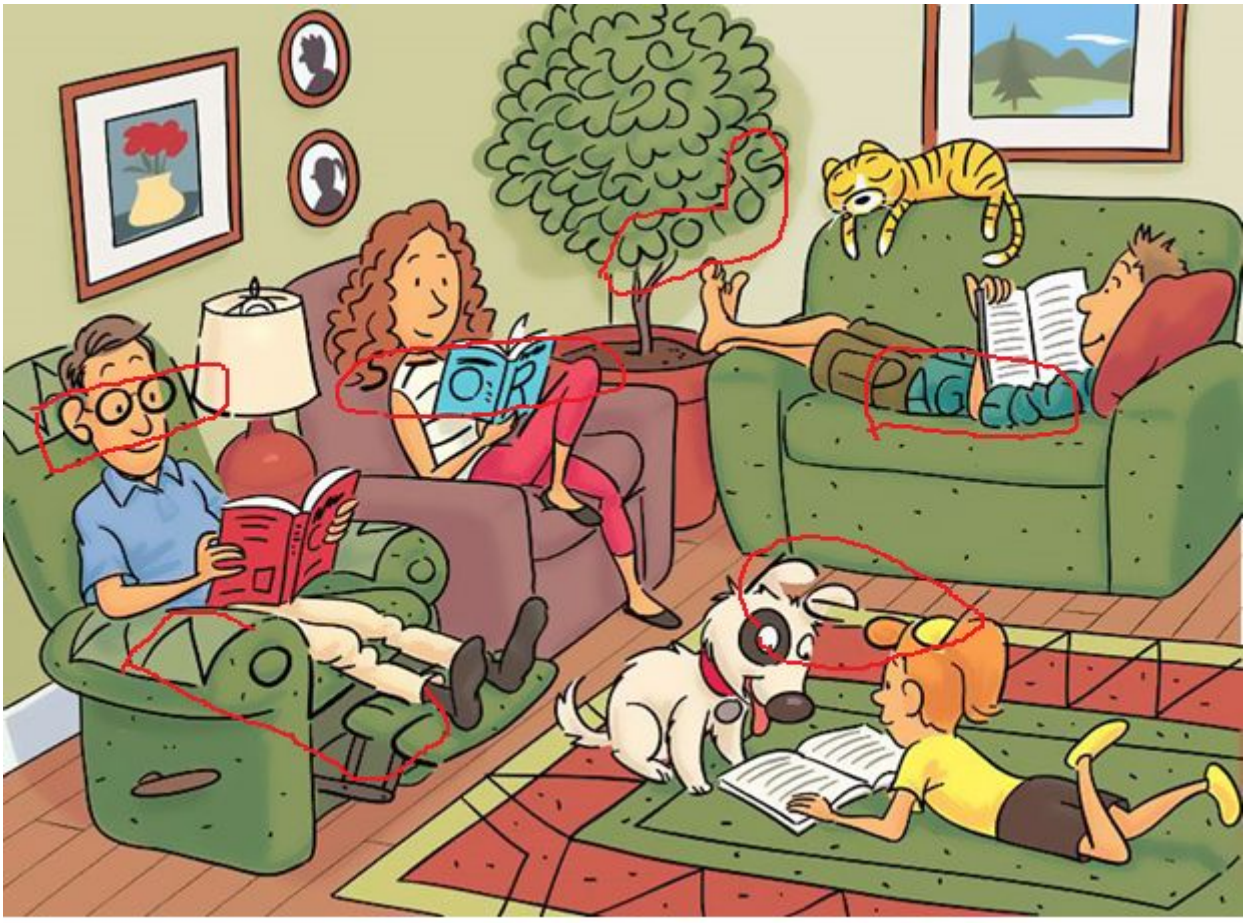
Procedure Details:

1. Slide 3:
   Ask the children what methods they adopt to discuss secrets. Children will normally think of how they communicate using chits in class, using sign language etc.
   Sending chits from the last bench to the first bench without anyone opening the chit !

2. Slide 4:
   Explain the definition of the word secret. Ask them to discuss a few examples which were maintained as top secrets. Some students may have the habit of writing a diary. Ask them if they allow anyone to read their diary. Why do they prefer to keep the contents of their diary a secret?
   Now you can quote a few real examples which children may be aware of
   The entire episode of demonetization was maintained a top secret by the government of India. Only two or three people knew about it.
   Another classical example was the Pokhran nuclear test on May 11th 1998. During this test, Dr Kalam was the mission director. He had to move the nuclear war heads to the test site and it should be moved without people knowing that it's a nuclear war head. Also developed countries like US or UK should not know about this test. The national intelligence agency admitted that they were aware of the nuclear test until it happened. They accepted a lapse of intelligence from their end.

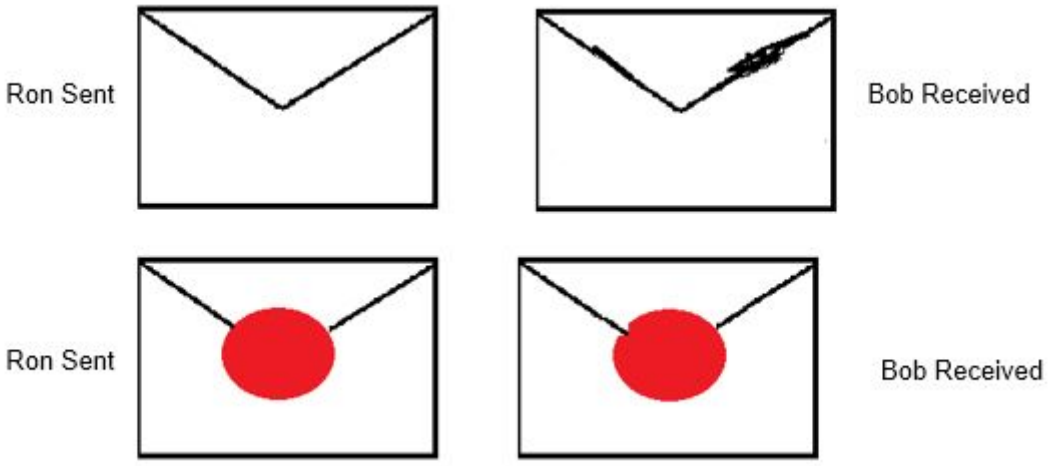
   Explain the students the importance of keeping somethings secret. If they had announced to the world that on May 11th a nuclear test is going to happen, will countries like US remain silent?

3. Slide 5
   Activity 01: The simplest way to communicate a secret message is to embed them in a picture. See if the students can identify all the 6 words. Note down the time they take to identify the same



   The hidden words are Novel, Story, Book, Pages, Words and Read

4. Slide 6, 7:
   Introduce two characters Ron and Bob. They are good friends and they always share secrets.
   Ask the students different ways in which they can share secret information.
   Tell them that one way is to put the secret message in an envelope and send it by post. Here we are trying to explain the concept that a message can be read by an unintended person. In our example we will say that the postman reads all the messages that are sent by Ron to Bob. If this happens, then Mike the postman can not only read the message but also change the message before it reaches Bob
5. Slide 9, 10:
   In this slide we are trying to get different ideas from children to protect the message sent by Ron to Bob. Prompt the students so that they tell that the message can be locked, envelope can be sealed, or the message can be encrypted. Introduce them to the concept of encryption.
   Ask them to identify which of the messages appear to be tampered



Notice that in the first envelope seems to be tampered or it was opened by Mike. The second one seems to be secure

6. Slide 11-15: Introduce them to the word encryption, show them the encrypted message that Ron sent Bob and see if the students can attempt to decode it. Explain them the concept of decoding a message using brute force.

7. Slide 16: Discuss the advantages and disadvantages of brute force. It takes lot of time to decrypt a small message. Explain the time taken to decrypt passwords using brute force. Brute force although a good technique cannot be used to identify long messages.

8. Slide 17: now we should explain the cipher technique and the ways in which we should decrypt the message. As the children to write down letters from A to Z in row 2 and the same alphabets shifted by 2 characters in row 1. Take the first two letters JK
   For the letter J find the corresponding letter in row 2
   do the same for the remaining letters you should get the message
   Hi let us meet at two

9. Slide 19: Ask the students to prepare a reply with the words Yes or No
   Yes would be AGU and No would be PQ

10. Slide 20 to 26 explain the same using modulo arithmetic.
    When we are encrypting a message, we are shifting the letter by the number specified in the Key so the general formula for encryption will be En = (Character position + Key) Mod 26
    We use mod 26 because we have 26 letters in English.
    In order to encrypt a message, students should know the position of each character. This can be found by writing down the alphabets in row 1 and the numbers from 1 to 26 in row 2.
    To Encrypt the letters Hi, they should first take the letter H, its position is 8 to find out the letter that will appear in the encrypted message, take the character position and add the key to it i.e 8 + 2
    Find mod 26 of this sum to get the encrypted character

Plain text	Character position	y	Modulus	Encrypted character
H	8	2	(8+2)MOD 26 = 10 MOD 26 = 10	10 → J
I	9	2	(9+2)MOD 26 = 11 MOD 26 = 11	11 → K
L	12	2	(12+2)MOD 26 = 14 MOD 26 = 14	14 → N
E	5	2	(5+2)MOD 26 = 7 MOD 26 = 7	7 → G
T	20	2	(20+2)MOD 26 = 22MOD 26 = 22	22 → V
U	21	2	(21+2)MOD 26 = 23 MOD 26 = 23	23 → W
S	19	2	(19+2)MOD 26 = 21 MOD 26 = 21	21 → U
M	13	2	(13+2)MOD 26 = 15 MOD 26 = 15	15 →O
E	5	2	(5+2)MOD 26 = 7 MOD 26 = 7	7 → G

E	5	2	(5+2)MOD 26 = 7 MOD 26 = 7	7 → G
T	20	2	(20+2)MOD 26 = 22 MOD 26 = 22	22 → V
A	1	2	(1+2)MOD 26 = 3 MOD 26 = 3	3 → C
T	20	2	(20+2)MOD 26 = 22 MOD 26 = 22	22 → V
T	20	2	(20+2)MOD 26 = 22 MOD 26 = 22	22 → V
W	23	2	(23+2)MOD 26 = 25 MOD 26 = 25	25 → Y
O	15	2	(15+2)MOD 26 = 17 MOD 26 = 17	17 → Q

Encrypted message
J K NGV WU OGGV CV VYQ

Decryption is very similar to Encryption the formula will be
Dn = (Encrypted character position – key) Mod 26

Plain text	Character position	Key	Modulus	Encrypted character
J	10	2	(10 - 2)MOD 26 = 8 MOD 26 = 8	8 → H
K	11	2	(11 - 2)MOD 26 = 9 MOD 26 = 9	9 → I
N	14	2	(14 - 2)MOD 26 = 12 MOD 26 = 12	12 → L
G	7	2	(7 - 2)MOD 26 = 5 MOD 26 = 5	5 → E
V	22	2	(22 - 2)MOD 26 = 20MOD 26 = 20	20 → T
W	23	2	(23 - 2)MOD 26 = 21 MOD 26 = 21	21 → U
U	21	2	(21 - 2)MOD 26 = 19 MOD 26 = 19	19 → S
O	15	2	(15 - 2)MOD 26 = 13 MOD 26 = 13	13 →M
G	7	2	(7 - 2)MOD 26 = 5 MOD 26 = 5	5 → E
G	7	2	(7 - 2)MOD 26 = 5 MOD 26 = 5	5 → E
V	22	2	(22 - 2)MOD 26 = 20 MOD 26 = 20	20 → T
C	3	2	(3 - 2)MOD 26 = 1 MOD 26 = 1	1 → A
V	22	2	(22 - 2)MOD 26 = 20 MOD 26 = 20	20 → T
V	22	2	(22 - 2)MOD 26 = 20 MOD 26 = 20	20 → T
Y	25	2	(25 - 2)MOD 26 = 23 MOD 26 = 23	23 → W
Q	17	2	(17 - 2)MOD 26 = 15 MOD 26 = 15	15 → 0