SSGMCE	SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG.	LABORATORY MANUAL
	PRACTICAL EXPERIMENT INSTRUCTION SHEET	
	EXPERIMENT TITLE : To simulate a password guessing attack (brute force/dictionary) using tools (like John the Ripper), and demonstrate the importance of strong passwords.	

EXPERIMENT NO.: **SSGMCE/WI/IT/01/5IT08/3**	ISSUE NO. : 00	ISSUE DATE : 08.07.2025
REV. DATE :	REV. NO. :	DEPTT. : INFORMATION TECHNOLOGY
LABORATORY : Information Security System (5IT08)	SEMESTER : V	PAGE: 1 OF 4

1.0) AIM: To simulate a password guessing attack (brute force/dictionary) using tools like John the Ripper or Cain & Abel, and demonstrate the importance of strong passwords.

2.0) SCOPE:

- To understand the concept of brute force and dictionary attacks.
- To learn how attackers attempt to crack weak passwords.
- To highlight the necessity of strong password policies for cyber security.

3.0) FACILITIES/ APPARATUS:

- **Windows**: John the Ripper (open-source password cracker)
- **7-Zip** (to create password-protected files)

4.0) THEORY:

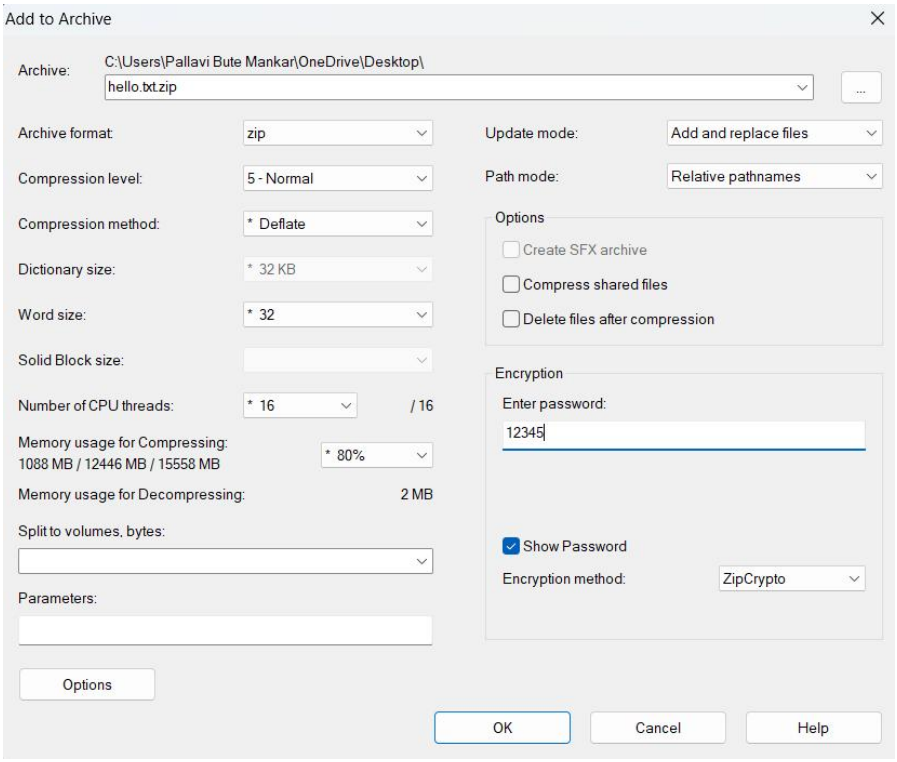
- **Brute Force Attack**: Trying all possible combinations of characters until the correct password is found.
- **Dictionary Attack**: Using a predefined list of common passwords (dictionary) to guess the correct one.
- These attacks are effective against weak passwords like *1234*, *password*, *admin*, etc.

5.0) STEPS:

Step A: Creating a Password-Protected File

SSGMCE	SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG.	LABORATORY MANUAL
	PRACTICAL EXPERIMENT INSTRUCTION SHEET	
	EXPERIMENT TITLE : To simulate a password guessing attack (brute force/dictionary) using tools (like John the Ripper), and demonstrate the importance of strong passwords.	
EXPERIMENT NO.: **SSGMCE/WI/IT/01/5IT08/3**	ISSUE NO. : 00	ISSUE DATE : 08.07.2025
REV. DATE :	REV. NO. :	DEPTT. : INFORMATION TECHNOLOGY
LABORATORY : Information Security System (5IT08)	SEMESTER : V	PAGE: 2 OF 4

1. Create a text file secret.txt with some content.
2. Right-click → 7-Zip → Add to archive.
3. Set Archive format = zip.
4. Enter a weak password (e.g., 1234).
5. Choose Encryption method = ziptocrypto → Click OK.
6. File secret.zip will be created.



Step B: Extracting Hash Using John the Ripper

Open Command Prompt and go to John's run directory.

cd path\to\john\run

Run the command:

PREPARED BY: PROF.MS.P.P BUTE	APPROVED BY: (H.O.D.)

zip2john "C:\path\to\secret.zip" > hash.txt

The password hash will be saved in hash.txt.

Step C: Cracking the Password

Run John the Ripper with the hash file:

john hash.txt

Observe how John tries possible passwords.

Once the password is cracked, it will display the result (e.g., 1234).

Output

```
C:\Users\Pallavi Bute Mankar\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>zip2john "C:\Users\Pallavi
Bute Mankar\OneDrive\Desktop\hello.txt.zip" >hash.txt
ver 2.0 hello.txt.zip/hello.txt.txt PKZIP Encr: cmplen=33, decmplen=75, crc=ECA0E2D

C:\Users\Pallavi Bute Mankar\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 16 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 13 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:password.lst, rules:Wordlist
123456          (hello.txt.zip/hello.txt.txt)
1g 0:00:00:01 DONE 2/3 (2025-09-24 02:50) 0.9451g/s 48321p/s 48321c/s 48321C/s 123456..skyline!
Use the "--show" option to display all of the cracked passwords reliably
```

We observe that weak passwords (like 1234, qwerty, admin) are cracked quickly.

Strong passwords (long + mix of characters) take much more time or may not crack within the lab

duration.

6.0) RESULT

In this practical we obverse brute force/dictionary attacks are simulated.

Importance of strong, complex passwords (12+ chars, mix of letters, numbers, symbols) and cyber security practices in daily life.