ANJUMAN-I-ISLAM'S KALSEKAR TECHNICAL CAMPUS

School of Engineering & Technology

Affiliated to : University of Mumbai, Recognised by : DTE (Maharashtra) & Approved by : AICTE (New Delhi)

Course Code : CSL604 **Course Name : System Security Lab**

Class : TE-CO **Batch : Computer Engineering**

Roll no : 18CO63 **Name : SHAIKH TAUSEEF MUSHTAQUE ALI**

Experiment : 04

Aim : For varying message sizes, test integrity of message using MD-5, SHA-1, and analyse the performance of the two protocols. Use crypt APIs.

Output :

```
users@Tauseef:~$ touch experi3.txt

users@Tauseef:~$ echo "Tauseef" >> experi3.txt

users@Tauseef:~$ md5sum experi3.txt
d1e87d22dd21e5a63a7578e055e750f8  experi3.txt

users@Tauseef:~$ sha1sum experi3.txt
2dd4a57416b419a354798122e23e34282435dc43  experi3.txt

users@Tauseef:~$ md5sum experi3.txt > experi3.md5 && md5sum -c experi3.md5
experi3.txt: OK

users@Tauseef:~$ sha1sum experi3.txt > experi3.sha1 && sha1sum -c experi3.sha1
experi3.txt: OK

users@Tauseef:~$ echo "Pathan" >> experi3.txt

users@Tauseef:~$ md5sum -c experi3.md5
experi3.txt: FAILED
md5sum: WARNING: 1 computed checksum did NOT match

users@Tauseef:~$ sha1sum -c experi3.sha1
experi3.txt: FAILED
sha1sum: WARNING: 1 computed checksum did NOT match
```

Conclusion:

Tested message integrity using MD-5, SHA-1, and analyzed the performance of the two protocols using crypt APIs for varying message sizes.