AHSANULLAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Department of Computer Science and Engineering

Program: Bachelor of Science in Computer Science and Engineering

Course Code: CSE 4174
Course Title: Cyber Security Lab
Academic Semester: Spring 2023

Assignment Topic: DES Calculator

Submitted On: 14 January 2024

Submitted by

Name: Shamim Rahim Refat
Student ID: 20200104125
Lab Section: C1

Question: Observe the avalanche effect of DES using the DES Calculator.

Answer:
Given Text = Ansary's
Given Key = MDAnsary

Original Text “Ansary's” in Hexadecimal: 416E736172792773
Original Key “MDAnsary” in Hexadecimal: 4D44416E73617279

After changing 8th bit (1 -> A) in original text,
Altered Text: 416E736A72792773

After changing 4th bit (4 -> A) in original key,
Altered Key: 4D4A416E73617279

Avalanche Effect in DES due to Change in Plaintext:

Round		δ
	416e736172792773 416e736a72792773	3
1	00fe22d6d4e7eb73 00fe2aded6d1cfdb	12
2	d4e7eb73198c2a54 d6d1cfdb5eee56e5	26
3	198c2a542996ef92 5eee56e5555a7abb	32
4	2996ef92e7d178c0 555a7abb163da1d7	35
5	e7d178c09ca473af 163da1d78ba0242e	31

6	9ca473af5fc97a8f 8ba0242e2f9c9d2c	29
7	5fc97a8fdbf751c2 2f9c9d2c5b2c5cda	29
8	dbf751c2e8331275 5b2c5cdaa71f4bcc	29
9	e8331275246cc40b a71f4bcccb1c8461	32
10	246cc40b9620f930 cb1c846152cda85d	32
11	9620f930477b1b0b 52cda85d055e8bf0	31
12	477b1b0ba6432681 055e8bf0ed503508	27
13	a643268187074a67 ed503508829a628f	26
14	87074a679879335f 829a628ffb3c5ca3	32
15	9879335f9896bc76 fb3c5ca37980dc10	32
16	9896bc76209e07a9 7980dc10acc3eb26	31
IP^{-1}	05363e99ba4b02b9 941549cc8ac59c7c	31

The table above shows that, after just four rounds, 35 bits differ between the two blocks. On completion, the two ciphertexts differ in 31 bits positions.

Avalanche Effect in DES due to Change in Key:

Round		δ
	4d44416e73617279 4d4a416e73617279	3
1	00fe22d6d4e7eb73 00fe22d6def7eb53	4
2	d4e7eb73198c2a54 def7eb532db5bb8f	20
3	198c2a542996ef92 2db5bb8f26d66af9	29
4	2996ef92e7d178c0 26d66af920433a04	26
5	e7d178c09ca473af 20433a045e6a7ef9	28
6	9ca473af5fc97a8f 5e6a7ef9ca46eae9	30
7	5fc97a8fdbf751c2 ca46eae96caa6b3e	36
8	dbf751c2e8331275 6caa6b3ed773eada	39
9	e8331275246cc40b d773eadaed439792	35
10	246cc40b9620f930 ed439792ac1b795f	33
11	9620f930477b1b0b ac1b795f4fc29981	27
12	477b1b0ba6432681 4fc299818232e11c	27
13	a643268187074a67 8232e11cfc16e5ac	35
14	87074a679879335f fc16e5ac38621858	32

15	9879335f9896bc76 3862185843652bf9	35
16	9896bc76209e07a9 43652bf9d10f4ff3	36
IP^{-1}	05363e99ba4b02b9 ff9d341e432be743	36

The table above shows that, after just three rounds, 29 bits differ between the two blocks. On completion, the two ciphertexts differ in 36 bits positions.

The results show that about half of the bits in the ciphertext differ and that the avalanche effect is pronounced after just a few rounds due to change in text or key.