# National University

of Computer & Emerging Sciences-Lahore

| | |
|---|---|
| Course – Section | Information Security (CS3002 - Fall 2024) – (BDS-7A, BDS-7B, BSE-7A) |
| Assignment Number | 02 |
| Total Marks | 80 Marks |
| Date Assigned | September 18, 2024 |
| Due Date | September 26, 2024 |
| Submission | Submit hand-written hardcopy in class (BSE-7A) ~ 08.30am<br>Submit hand-written hardcopy in instructor office (BDS-7A/7B) ~ 10.30am |
| Author | Muhammad Mobeen (l247715@lhr.nu.edu.pk) |
| Approved By | Dr. Syed M. Irteza (m.irteza@nu.edu.pk) |
| Submission Guidelines | - ***Write your name, section and roll number clearly at the top of your assignment, and staple your assignment properly.***<br>- *Assignments must be received before the deadline. Submissions after the deadline will face a 25% grade penalty (within 1 day) or a 50% grade penalty (within 2 days).*<br>- *Plagiarism cases will be dealt with strictly.*<br>- *Read questions and marks distribution carefully and write precise answers, avoiding wordy stories.*<br>- *Make assumptions where needed but state them clearly in your answer.* |

**Q1. Explain how** **[10+10 = 20 Marks]**

**(i) AES is different from DES.**

**(ii) The different steps that take place in each round of AES.**

**Q2. RSA.** **[20 Marks]**

**Using RSA, encrypt the message M = 3, assuming the two primes chosen to generate the keys are p = 19 and q = 13. You should choose a value of e where (e < 10). Show your calculations and assumptions.**

**Q3. DES.** **[40 Marks]**

**By using the DES algorithm, perform encryption on the plaintext given below. ONLY UP TILL ROUND 1.**

**PT = John Wick!** **(Space and exclamation mark are also included in the PT)**

**Key**:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |

## Helping Material:

**Table 6.3** *S-box 1*

| | *0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* | *12* | *13* | *14* | *15* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *0* | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| *1* | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 10 | 03 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| *2* | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| *3* | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

**Table 6.4** *S-box 2*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 15 | 01 | 08 | 14 | 06 | 11 | 03 | 04 | 09 | 07 | 02 | 13 | 12 | 00 | 05 | 10 |
| *1* | 03 | 13 | 04 | 07 | 15 | 02 | 08 | 14 | 12 | 00 | 01 | 10 | 06 | 09 | 11 | 05 |
| *2* | 00 | 14 | 07 | 11 | 10 | 04 | 13 | 01 | 05 | 08 | 12 | 06 | 09 | 03 | 02 | 15 |
| *3* | 13 | 08 | 10 | 01 | 03 | 15 | 04 | 02 | 11 | 06 | 07 | 12 | 00 | 05 | 14 | 09 |

**Table 6.5** *S-box 3*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 10 | 00 | 09 | 14 | 06 | 03 | 15 | 05 | 01 | 13 | 12 | 07 | 11 | 04 | 02 | 08 |
| *1* | 13 | 07 | 00 | 09 | 03 | 04 | 06 | 10 | 02 | 08 | 05 | 14 | 12 | 11 | 15 | 01 |
| *2* | 13 | 06 | 04 | 09 | 08 | 15 | 03 | 00 | 11 | 01 | 02 | 12 | 05 | 10 | 14 | 07 |
| *3* | 01 | 10 | 13 | 00 | 06 | 09 | 08 | 07 | 04 | 15 | 14 | 03 | 11 | 05 | 02 | 12 |

**Table 6.6** *S-box 4*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 07 | 13 | 14 | 03 | 00 | 6 | 09 | 10 | 1 | 02 | 08 | 05 | 11 | 12 | 04 | 15 |
| *1* | 13 | 08 | 11 | 05 | 06 | 15 | 00 | 03 | 04 | 07 | 02 | 12 | 01 | 10 | 14 | 09 |
| *2* | 10 | 06 | 09 | 00 | 12 | 11 | 07 | 13 | 15 | 01 | 03 | 14 | 05 | 02 | 08 | 04 |
| *3* | 03 | 15 | 00 | 06 | 10 | 01 | 13 | 08 | 09 | 04 | 05 | 11 | 12 | 07 | 02 | 14 |

**Table 6.7** *S-box 5*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 02 | 12 | 04 | 01 | 07 | 10 | 11 | 06 | 08 | 05 | 03 | 15 | 13 | 00 | 14 | 09 |
| *1* | 14 | 11 | 02 | 12 | 04 | 07 | 13 | 01 | 05 | 00 | 15 | 10 | 03 | 09 | 08 | 06 |
| *2* | 04 | 02 | 01 | 11 | 10 | 13 | 07 | 08 | 15 | 09 | 12 | 05 | 06 | 03 | 00 | 14 |
| *3* | 11 | 08 | 12 | 07 | 01 | 14 | 02 | 13 | 06 | 15 | 00 | 09 | 10 | 04 | 05 | 03 |

**Table 6.8** *S-box 6*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 12 | 01 | 10 | 15 | 09 | 02 | 06 | 08 | 00 | 13 | 03 | 04 | 14 | 07 | 05 | 11 |
| *1* | 10 | 15 | 04 | 02 | 07 | 12 | 09 | 05 | 06 | 01 | 13 | 14 | 00 | 11 | 03 | 08 |
| *2* | 09 | 14 | 15 | 05 | 02 | 08 | 12 | 03 | 07 | 00 | 04 | 10 | 01 | 13 | 11 | 06 |
| *3* | 04 | 03 | 02 | 12 | 09 | 05 | 15 | 10 | 11 | 14 | 01 | 07 | 10 | 00 | 08 | 13 |

**Table 6.9** *S-box 7*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 4 | 11 | 2 | 14 | 15 | 00 | 08 | 13 | 03 | 12 | 09 | 07 | 05 | 10 | 06 | 01 |
| *1* | 13 | 00 | 11 | 07 | 04 | 09 | 01 | 10 | 14 | 03 | 05 | 12 | 02 | 15 | 08 | 06 |
| *2* | 01 | 04 | 11 | 13 | 12 | 03 | 07 | 14 | 10 | 15 | 06 | 08 | 00 | 05 | 09 | 02 |
| *3* | 06 | 11 | 13 | 08 | 01 | 04 | 10 | 07 | 09 | 05 | 00 | 15 | 14 | 02 | 03 | 12 |

**Table 6.10** *S-box 8*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 13 | 02 | 08 | 04 | 06 | 15 | 11 | 01 | 10 | 09 | 03 | 14 | 05 | 00 | 12 | 07 |
| *1* | 01 | 15 | 13 | 08 | 10 | 03 | 07 | 04 | 12 | 05 | 06 | 11 | 10 | 14 | 09 | 02 |
| *2* | 07 | 11 | 04 | 01 | 09 | 12 | 14 | 02 | 00 | 06 | 10 | 10 | 15 | 03 | 05 | 08 |
| *3* | 02 | 01 | 14 | 07 | 04 | 10 | 8 | 13 | 15 | 12 | 09 | 09 | 03 | 05 | 06 | 11 |

| *Initial Permutation* | *Final Permutation* |
|---|---|
| 58 50 42 34 26 18 10 02 | 40 08 48 16 56 24 64 32 |
| 60 52 44 36 28 20 12 04 | 39 07 47 15 55 23 63 31 |
| 62 54 46 38 30 22 14 06 | 38 06 46 14 54 22 62 30 |
| 64 56 48 40 32 24 16 08 | 37 05 45 13 53 21 61 29 |
| 57 49 41 33 25 17 09 01 | 36 04 44 12 52 20 60 28 |
| 59 51 43 35 27 19 11 03 | 35 03 43 11 51 19 59 27 |
| 61 53 45 37 29 21 13 05 | 34 02 42 10 50 18 58 26 |
| 63 55 47 39 31 23 15 07 | 33 01 41 09 49 17 57 25 |

**This Table is also called $IP^{-1}$**

**Table 6.2** *Expansion D-box table*

| | | | | | |
|---|---|---|---|---|---|
| 32 | 01 | 02 | 03 | 04 | 05 |
| 04 | 05 | 06 | 07 | 08 | 09 |
| 08 | 09 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 31 | 31 | 32 | 01 |

**PC-1**

| | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

**PC-2**

| | | | | | |
|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |

**Table 6.11** *Straight permutation table*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 07 | 20 | 21 | 29 | 12 | 28 | 17 |
| 01 | 15 | 23 | 26 | 05 | 18 | 31 | 10 |
| 02 | 08 | 24 | 14 | 32 | 27 | 03 | 09 |
| 19 | 13 | 30 | 06 | 22 | 11 | 04 | 25 |