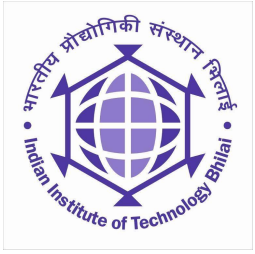

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Indian Institute of Technology Bhilai
CS553/CSL505 – CRYPTOGRAPHY
Semester: 2024-M
Scope: Block Ciphers, Differential/Linear/Automated Cryptanalysis

Assignment 3
September 14, 2024

- Instructions
  - LaTeX based answers are preferred
  - "Readme" file for your code (if applicable)
  - Submissions in a zip file named as `<group-name>_<assignment_no>`
  - Some problems are to be submitted in the notebook.

1 Capture The Flag

1. Demonstrate how you solved the CTF that lead you to this Assignment? If your group is among the first three teams then, you will receive bonus points. However, every group must justify how they got hold of this `pdf` file.

   ***Note**: If you are unable to justify this then the rest of the solutions will not be accepted.*

2 Block Ciphers

2. Search for five Fiestal & five SPN block ciphers with following details [**Notebook**]
   - Name
   - Block-length
   - Supported Key-sizes
   - Any other additional info (in one line only)
3. Random Sbox
   - Generate a 4-bit random Sbox in your favourite programming language
   - State it in the main assignment and **also** document in the **notebook**.
   - Submit the code file separately with comments briefly stating your approach
   - Follow file naming convention
   - It is expected that your Sbox-es will be unique

4. Use the random Sbox you generated for the following

   - Write a code to generate its DDT-LAT in your favorite programming language.
   - Submit code in a separate file and show the DDT-LAT in answer script
   - What is the maximum differential probability of your Sbox? Mention the transition(s) that lead to that.
   - What is the maximum bias your Sbox? Mention the input-output mask(s) that lead to that.
   - Now use Sage to generate the DDT-LAT for your Sbox.
   - What is the meaning of component function of an Sbox?
   - Enumerate the component functions of your Sbox using Sage.
   - How would you represent your Sbox as a Boolean function using the component functions? [Hint: There will be four functions each representing one output bit]
   - Ref: http://match.stanford.edu/reference/cryptography/sage/crypto/sbox.html

3 Block Cipher Cryptanalysis

5. Recall the experiments from Chapter 6 of the *"The Block Cipher Companion Book"* discussed in class.

   - Implement Sypher004[1]
   - Use random keys using `openssl rand`
     - (Six 16-bits keys $\rightarrow k_0, \cdots, k_5$)
   - Verify the following experiments from the book using your implementation of Sypher004.
   - Use 6 sets of randomly generated keys.
   - Submit the well commented code so that your results can be verified.
   - Also document (preferably in a table) the randomly generated keys used here.
   - Write paragraphs for each one to describe your observations referring to the figures below.

> Consider CipherFour with five rounds using randomly chosen subkeys $k_0 = \texttt{5b92}$, $k_1 = \texttt{064b}$, $k_2 = \texttt{1e03}$, $k_3 = \texttt{a55f}$, $k_4 = \texttt{ecbd}$, and $k_5 = \texttt{7ca5}$. An exhaustive search over all 2^{16} pairs of messages with difference $(0,0,2,0)$ reveals that $1,300$ pairs follow the four-round characteristic and the difference in the ciphertexts after each round of encryption is $(0,0,2,0)$. For this specific key, this yields a probability of approximately 0.02. For five other randomly chosen subkey sets, the number of such pairs were $1,312$, $1,290$, $1,328$, $1,318$, and $1,228$ providing an average of $1,296$. Thus, for all six sets of keys, the probability of the four-round characteristic was approximately 0.02. Our expected value was $(\frac{6}{16})^4 \simeq 0.02$.
>
> **Fig. 6.7** Experimental confirmation of the four-round characteristic for CipherFour.

[1] Follow the description in *The Block Cipher Companion*

Consider five rounds of CIPHERFOUR using the same subkeys as Fig. 6.7. Consider all 2^{16} pairs of messages with difference $(0,0,2,0)$. An exhaustive search reveals that $7,216$ of these pairs would not be discarded in a filtering process. For the five other sets of subkeys from Example 6.7, the number of pairs not filtered were $7,842$, $6,638$, $7,292$, $7,478$, and $7,856$ providing an overall average of $7,387$. It may be helpful to compare this to the figure derived in Fig. 6.8. There we had that, on average, $5,310$ pairs satisfied our target differential. Thus we might expect $\frac{5310}{7387} \simeq 70\%$ of filtered pairs to be useful in our attack whereas only $\frac{5310}{65536} \simeq 8\%$ would have been useful without filtering.

Fig. 6.9 Experimental confirmation of the process of filtering for CIPHERFOUR.

Consider five rounds of CIPHERFOUR using the subkeys of Example 6.7. Consider all 2^{16} message pairs with difference $(0,0,2,0)$. An exhaustive search reveals that $5,080$ pairs give a difference $(0,0,2,0)$ after four rounds of encryption. For this specific key, this yields a probability for the differential $(0,0,2,0) \to ? \to ? \to ? \to (0,0,2,0)$ of approximately 0.078. For five other randomly chosen sets of subkeys (the same as those used in Example 6.7) the number of pairs were $5,760$, $4,640$, $5,060$, $5,542$, and $5,776$ respectively. This provides an average of $5,310$ corresponding to an average probability for the four-round differential of 0.081.

Fig. 6.8 Experimental confirmation of the four-round differential for CIPHERFOUR.

6. Describe a differential attack, analogous to the one described in class for Sypher004, that will find eight subkey bits in the last round. What is the probability of the differential characteristic you devised.

   [Hint]: Your differential characteristic must involve two Sbox-es in the 4th round.

4 Make Thy Sypher004

7. Make your own version of Sypher004

   - Substitution-Layer: Use the Sbox you generated earlier.
   - Permutation-Layer: Generate a random permutation layer.
   - Key-Addition-Layer remains same.
   - Draw the picture of two rounds of *your* Sypher004 in the **notebook**.

5 Automated Cryptanalysis (MILP)

8. Create an example as shown in class to demonstrate your understanding of an optimization problem.
   - State the objective function.
   - State the constraints and justify them.
   - State the restrictions on the variables.
   - Generate the `.lp` file using the syntax shown in the sample file used in class.
   - Solve it using `Gurobi` solver.
9. You know that the best 4-round differential characteristic for Sypher004 has 4 active Sbox-es. This can also be verified using `Gurobi`. What constraint should you add to your set of constraints for Gurobi so that it reports more that 4 active Sbox-es in its solution? Verify this and submit your `.lp` and `.sol` files.
10. Find the best 4-round trail for *your* Sypher004 using `Gurobi`. Concentrate on how the constraints for different rounds are to be generated taking care of your permutation layer. Submit your `.lp` and `.sol` files.

Recall: We are not taking the properties of the Sbox into consideration in the current MILP model.
