MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Differential Cryptanalysis – Part 2

Author: Nils Kopal, Christian Bender

January 2020

Introduction (1/2)

Differential cryptanalysis was publicly discovered by Eli Biham and Adi Shamir in the late 1980s. They published several papers about attacks on different block ciphers and hash functions. Differential cryptanalysis is said to be known previously to the NSA as well as to IBM already in the 1970s. The NSA decided not to publish their findings to have an advantage over other countries at that time.

NSA furthermore modified the DES cipher's S-boxes in its date of origin while not describing their reasons behind their changes. This lead to the suspicion that the NSA weakened the cipher to their advantage. Later it became clear that NSA in fact strengthened DES by making its S-boxes invulnerable to differential cryptanalysis.

Introduction (2/2)

Differential cryptanalysis is a chosen-plaintext attack on a block cipher revealing its secret round keys. Thus, the attacker is able to generate random plaintext pairs and to obtain the corresponding ciphertext pairs using the cipher as a white box, e.g. an encryption oracle.

The attacker chooses plaintext pairs having a specific bitwise difference. For that particular difference he previously computed a so-called characteristic. A characteristic is a "path through the cipher" based on input and output differences of each round.

Using the characteristics and the plaintext-ciphertext pairs, the attacker can draw conclusions and ultimately recover the round keys.

Challenge (1/5)

For this challenge, plaintext and ciphertext pairs were generated using the block cipher encryption algorithm “Mystery Cipher 1” (MC1). MC1 is a three-round toy cipher with a 64-bit key. The key is split into four round keys K_0, K_1, K_2 and K_3. To recover the four round keys you have to perform differential cryptanalysis on MC1.

The four round keys were also used to encrypt an image with the "FileEncrypter" program (FileEncrypter uses the MC1 algorithm). Having the round keys, you can call the command-line program "FileEncrypter" to actually decrypt the image and read the code word in there.

In contrast to part 1, in this challenge you need to implement filtering. Without a filter, the challenge can not be solved.

Challenge (2/5)

We provide the following documents, implementations, and data to solve the challenge:

1. Specification of Mystery Cipher 1 (pdf document)
2. Source code of the algorithm Mystery Cipher 1 and of FileEncrypter (both in .NET C#)
3. Pre-computed differentials for performing the attack (txt files)
4. Plaintext-ciphertext pairs having differences for each S-box (csv files)
5. Encrypted image containing the solution code (png file)
6. Tutorials about differential cryptanalysis in CrypTool 2

Challenge (3/5)

Further information about the documents and implementations:

- The specification contains test vectors which can be used for testing your implementation of the cipher.
- The source code contains methods to encrypt and decrypt plain- and ciphertext (little-endian numbers and binary data).
- The differential files contain the plaintext difference and the expected output difference with its probability.
- Pair files data is defined as the tuple $(\mathrm{P}, \mathrm{P}', \mathrm{C}, \mathrm{C}')$ where P and P' are two plaintexts having a specific difference and C and C' are their corresponding ciphertexts.
- Hint: You don't need to find characteristics and differentials on your own since we ship all the needed files.

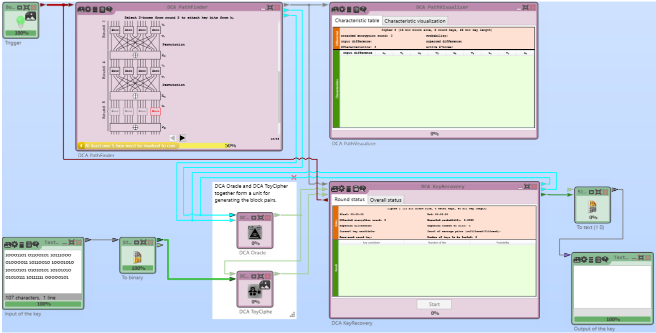
Challenge (4/5)

Some hints and ideas how to proceed:

- Read and understand the referenced papers [1], [2], and [3, pp. 109-126] about differential cryptanalysis.
- You can start your studies on differential cryptanalysis using the tutorials in CrypTool 2.
- Implement differential cryptanalysis based on the information you learned from the papers:
  1. Implement difference distribution table (DDT) of the S-box.
  2. Break round keys K_3 and K_2 using the differences and pair files.
  3. Break round keys K_1 and K_0 using the DDT.
- In the final step, use the found round keys to decrypt the image using our C# implementation (FileEncrypter).

Challenge (5/5)

CrypTool 2 (CT2) contains three diverse tutorials about differential cryptanalysis. The following screenshot shows the third tutorial (availably in the Nightly Build of CT2, downloadable from: `https://www.cryptool.org/en/ct2-downloads`).



DCA Oracle and DCA ToyCipher together form a unit for generating the block pairs.

Input of the key:

```
10001101 01100101 10111000
01000011 10110010 10001010
10010101 01010101 10101010
01010111 10111111 00000101
```

107 characters, 1 line

DCA PathFinder: Select S-boxes from round 5 to attack key bits from k_5

3 At least one S-box must be marked to con... 50%

DCA PathVisualizer – Characteristic table:

Cipher 3 (16 bit block size, 6 round keys, 96 bit key length)

Attacked encryption round: 0

Probability:

Input difference:

Expected difference:

#Characteristics: 0

Active S-boxes:

Input difference	u_1	v_1	u_2	v_2	u_3	v_3	u_4	v_4	u_5

DCA KeyRecovery – Round status:

Cipher 3 (16 bit block size, 6 round keys, 96 bit key length)

Start: 00:00:00

End: 00:00:00

Attacked encryption round: 0

Expected probability: 0.0000

Expected difference:

Expected number of hits: 0

Current key candidate:

Count of message pairs (unfiltered/filtered):

Recovered round key:

Number of keys to be tested: 0

key candidate	Number of hits	Probability

Literature

[1] Howard M Heys. "A Tutorial on Linear and Differential Cryptanalysis". In: *Cryptologia* 26.3 (2002), pp. 189–221.

[2] Lars R Knudsen and Matthew Robshaw. *The Block Cipher Companion*. Springer Science & Business Media, 2011.

[3] Christian Bender. *Master's thesis: Analyse symmetrischer Blockchiffren mittels differenzieller Kryptoanalyse in CrypTool 2*. 2019. URL: `https://www.cryptool.org/images/ctp/documents/MA_Bender.pdf`.