Arizona State University

CSE 539 Applied Cryptography Project-2

CHIRAG BHANSALI (1215185491)
SHIVANK TIWARI (1217351382)

3. Perform the initial cryptanalysis. In the Project 2 Submission document, Describe the design of the (provided) algorithm used and how it works. Explain whether or not you think this encryption algorithm “cheats” (that is it is not a self-contained encryption algorithm) and why you think so.
On performing the initial cryptanalysis, we found that instead of encrypting the plaintext which it should be doing in the ideal scenario, it is instead doing MD5 operations on the key and for encrypting the plaintext to produce the ciphertext it is using the XOR operation between the plaintext and the key. It “cheats” (not a self-contained algorithm) since it is using the XOR operation for encryption and decryption, along with MD5 for the key.

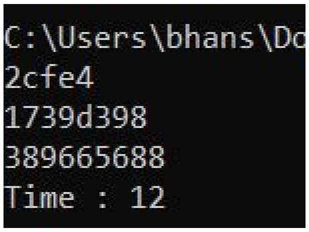
MD5 working: 4 rounds with 16 operations in each, totaling to 64 operations on the key.

For Encryption, the key is generated via the system entropy and then the key and the plaintext is XORed to give the Ciphertext.
For Decryption, the input key is used along with the ciphertext to get the plaintext via XOR operation.

4.Brute force the keys for the three files provided and find the keys used. You may modify the programs. Do not assume you know the plaintext, but assume you know what type of plaintext file it is. (Note: knowing the type of the file helps in brute-forcing.) Record the key for each file and what the file contains in the Project 2 Submission document. Also record the runtime of the brute force algorithm.

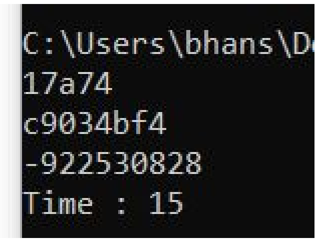
Txt file : 98d63c96
Data: The quick brown fox jumped over the lazy dog.
0123 456 789
Time: 70 seconds

Pdf : 1739d398
Data: Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
Time: 12 seconds



```
C:\Users\bhans\Do
2cfe4
1739d398
389665688
Time : 12
```

Png: c9034bf4
Data: Image of cat
Time: 15seconds



```
C:\Users\bhans\D
17a74
c9034bf4
-922530828
Time : 15
```

5. Find weakness(es) of the cipher design. Describe the weakness(es) and how they might have been avoided or could be fixed in the Project 2 Submission Document.
Weakness: The program uses the XOR function between the key and plaintext to calculate the ciphertext, instead of the MD5.
The weakness could have been removed if we could have done the MD5 operation on the plaintext, which we wouldn't even have needed the key, and the 32-bit hashes from the MD5 algorithm could have been the ciphertext (kinda unbreakable one).
Or, we could have used both the XOR and the MD5 algorithm, by first doing the XOR and then applying the MD5 algorithm on the XORed result, to get the ciphertext.

6. Use the weakness(es) in the cipher design to find keys faster. Describe how the weakness(es) can be used to find keys faster in the Project 2 Submission Document. Also, record the runtime of the faster algorithm.
Exploit weakness:
For exploiting the weakness, we XOR the header of the file with the first 4 characters of the ciphertext to get the plaintext.

Pdf: 0.1 seconds
Png: 0.08 seconds
Text file: 0.01 seconds