EE576 HW 2

Matt Ruffner

January 28, 2019

1

First, frequency analysis in CrypTool 2.1 was run on the encrypted file to find the two most used encrypted letters: G and O. These two letters were then exored with the encoded equivalent of an 'E', the most common letter in the English language. The result of these two ex-ors were the letters 'C' and 'K'. Two descriptions were then preformed on the encrypted data until the result was coherent. The key used for success full decryption was 'KC'. The resulting decoded text is included in the attached file `q1decoded.txt`

2

For this problem. The sample text included in `q2input.txt` was used. This was encoded with the Vigenere cipher three times, with the keys *fox*, *brownfox* and *quickbrownfox*. The first two were able to be successfully decrypted with the Vigenere breaker component of CrypTool, however the third key produced was not able to be successfully decrypted. The input file was then decreased in length by a factor of two. The results indicated that a shorter amount of encrypted text offered less clues as to the correct encryption key. A second halving of the input text yielded a wildly incorrect key that was also much shorter in length than previously.

3

To decrypt the input file, `AES-ciphertext.bin`, JCryptTool was used, with no padding in Electronic CodeBlock mode. The result of the decryption is included in `q3output.txt`.

4

The following tables depict the state bytes through one round of the AES encryption process. The final *MixColumns* step was calculated using the attached `mxmult.py` program.

00	01	02	03
04	05	06	07
08	09	0A	0A
0C	0D	0E	0F

Table 1: Original Contents

01	00	03	02
05	04	07	06
09	08	0B	0B
0D	0C	0F	0E

Table 2: After AddRoundKey

7C	63	7B	77
6B	F2	C5	6F
01	30	2B	2B
D7	FE	76	AB

Table 3: After SubBytes

7C	6B	01	D7
F2	30	FE	63
2B	76	7B	C5
AB	77	6F	2B

Table 4: After ShiftRows

AE	47	EC	69
B2	1E	E3	75
D9	D2	44	BF
FB	E9	58	75

Table 5: After MixColumns

5

The unmodified image is shown in Fig. 1. The image encrypted with AES in ECB mode is shown in Fig. 2. The image encoded with AES in CBC mode is shown in Fig. 3.

Figure 1: `apple.bmp`

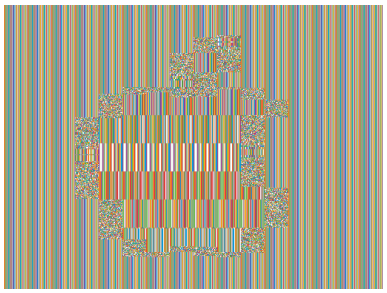

Figure 2: `appleecb.bmp`

Figure 3: `applecbc.bmp`

6

1 We know the random vector, v, since it is always the first 80 bits. With the addition of this information, all of v, c, and k are known. Thus, the the message can be decrypted by computing $\text{RC4}(v||k) \oplus c$.

2 By observing the random vector v across transmissions. The same v implies the same key stream was used to encrypt the messages.

3 The key stream varies with random 80 bit v since the key is fixed. Brute-force collision search is $O(2^{n/2})$, where n is the number of bits. Thus, after 2^40 transmissions the random v will probably be repeated.

4 This implies that the key should be changed before 2^{40} transmissions have occured.

Acknowledgements

This homework was completed in collaboration with Jordan Caudill.