Applied Cryptography: Homework 4

(Deadline: 10:00am, 2020/10/10)

Justify your answers with calculations, proofs, and programs.

1. (10 points, question 4.3, page 132 of the textbook)

   Let $DES(x, K)$ represent the encryption of plaintext x with key K using the *DES* cryptosystem. Suppose $y = DES(x, K)$ and $y' = DES(c(x), c(K))$, where $c(\cdot)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$ (i.e., if we complement the plaintext and the key, then the ciphertext is also complemented). Note that this can be proved using only the "high-level" description of *DES*-the actual structure of S-boxes and other components of the system are irrelevant.

2. (20 points, question 4.4 + question 4.5, page 132 of the textbook)

   (a) Suppose that we have the following 128-bit *AES* key, given in hexadecimal notation:

   `2B7E151628AED2A6ABF7158809CF4F3C`

   Construct the complete key schedule arising from this key.

   (b) Compute the encryption of the following plaintext (given in hexadecimal notation) using the 10-round *AES*:

   `3243F6A8885A308D313198A2E0370734`

   Use the 128-bit key from the previous exercise.

3. (30 points, question 4.15, page 134 of the textbook)

   Suppose that the S-box of Example 4.1 is replaced by the S-box defined by the following substitution $\pi_{S'}$:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_{S'}(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

   (a) Compute the linear approximation table for this S-box.

   (b) Find a linear approximation using three active S-boxes, and use the piling-up lemma to estimate the bias of the random variable $\mathbf{X}_{16} \oplus \mathbf{U}_1^4 \oplus \mathbf{U}_9^4$.

   (c) Describe a linear attack, analogous to Algorithm 4.2, that will find eight subkey bits in the last round.

   (d) Implement your attack and test it to see how many plaintexts are required in order for the algorithm to find the correct subkey bits (approximately $1000-1500$ plaintexts should suffice; this attack is more efficient than Algorithm 4.2 because the bias is larger by a factor of 2, which means that the number of plaintexts can be reduced by a factor of about 4).

4. (30 points, question 4.16, page 135 of the textbook)

   Suppose that the S-box of Example 4.1 is replaced by the S-box defined by the following substitution $\pi_{S''}$:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_{S''}(z)$	E	2	1	3	D	9	0	6	F	4	5	A	8	C	7	B

.

(a) Compute the table of values N_D (as defined in Definition 4.3) for this S-box.

(b) Find a differential trail using four active S-boxes, namely, S_1^1, S_4^1, S_4^2, and S_4^3, that has propagation ratio 27/2048.

(c) Describe a differential attack, analogous to Algorithm 4.3, that will find eight subkey bits in the last round.

(d) Implement your attack and test it to see how many plaintexts are required in order for the algorithm to find the correct subkey bits (approximately $100-200$ plaintexts should suffice; this attack is not as efficient as Algorithm 4.3 because the propagation ratio is smaller by a factor of 2).