Understanding Cryptography

Homework No.2 **Due Date: 1400.01.10**

HAPPY NEW YEAR!

Chapter 3

1. DES has weak and semi-weak keys.

- *Weak key: A DES key k is called a weak key if encryption and decryption are same.*

$$E_k(E_k(x)) = x$$

1.1.Describe the relationship of the sub-keys in encryption and decryption algorithm for that this equation is fulfilled.

1.2.DES has four weak keys (64- bit). What are they?

1.3.What is the likelihood that a randomly selected key is weak?

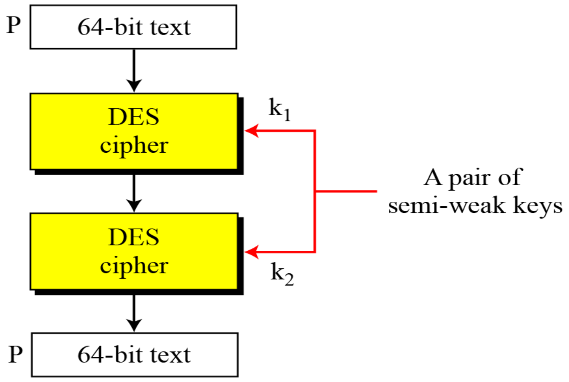
1.4. Explain where weak keys should not be used?

- *Semi-weak key: They have the property that* $E_{k1}\left(E_{k2}(x)\right) = x$

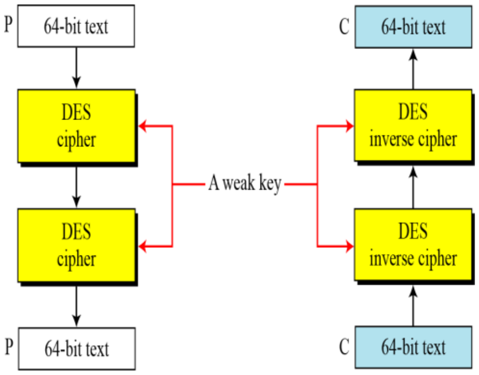
1.5.How many pairs of Semi-weak keys are there in DES?

1.6.Semi-weak keys only produce two different subkeys. How many times is each sub-key used in the algorithm?

1.7.What is the probability of randomly selecting a weak, a semi-weak, or a possible weak key? Is this probability possible?



A pair of semi-weak keys in encryption and decryption



Double encryption and decryption with a weak key

2.

2.1. What is the most important property of S-boxes which makes DES secure?

2.2. Compute $S_i(x_1) \oplus S_i(x_2)$ *and* $S_i(x_1 \oplus x_2)$*. Suppose that* $x_1 = 101010$ *and* $x_2 = 010101$.

2.3. The following table shows the permutation for S-box. Suppose The input to S-box is 100011. What is the output?

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

3. *We know Two desired properties of a block cipher are the* ***Avalanche effect*** *and the* ***Completeness effect.***

- ***Avalanche effect:*** *we encrypt two plaintext blocks (with the same key) that differ only in one bit and observe the differences in the number of bits in each round.*
- ***Completeness effect:*** *Completeness effect means that each bit of the cipher text needs to depend on many bits on the plaintext.*

To check the avalanche effect in DES, we apply an input word that has a ''1'' at bit position 57 and all other bits as well as the key are zero.

3.1. How many S-boxes get different inputs compared to the case when an all-zero plaintext is provided?
3.2. What is the output after the first round?
3.3. What is the minimum number of output bits of the S-boxes that will change according to the S-box design criteria?
3.4. How many output bit after the first round have actually changed compared to the case when the plaintext is all zero?

Chapter 4

4. *In the following, we check the diffusion properties of AES after a single round.*

Let $W = (w_0, w_1, w_2, w_3) = (0x01000000, 0x00000000, 0x00000000\ 0x00000000)$ *be the input in 32-bit chunks to a 128-bit AES. The sub-keys for the computation of the result of the first round of AES are* $W_0, \ldots, W_7$ *with 32 bits each are given by:*
$W_0 = (0x2B7E1516)$, $W_1 = (0x28AED2A6)$,
$W_2 = (0xABF71588)$, $W_3 = (0x09CF4F3C)$,
$W_4 = (0xA0FAFE17)$, $W_5 = (0x88542CB1)$,
$W_6 = (0x23A33939)$, $W_7 = (0x2A6C7605)$.

4.1. *Compute the output of the first round of AES to the input* W *and the sub-keys* $W_0, \ldots, W_7$.

4.2. *Compute the output of the first round of AES for the case that all input bits are zero.*

4.3. *How many output bits have changed? Remark that we only consider a single round and after every further round, more output bits will be affected (avalanche effect).*

***5**. Find all irreducible polynomials of degree 4 over GF (2).*

***6.** Generate the multiplication table (8×8) for the extension field $GF(2^3)$ for below irreducible polynomial manually.*

$$P(x) = x^3 + x + 1$$

Chapter 3 & 4

***7.** Search about one of the below topics of your choice and write a text with at least 500 words about this topic. Use this text to answer the following questions.*

- *Differences between stream and block ciphers*
- *RC2 block cipher*
- *Dictionary attack*

Note: Answer the below questions making use of CrypTool and your text about one of the above topics; use the ECB mode for all the exercises related to DES algorithm.

Encryption/Decryption

***7.1.** Answer the following questions about weak and semi-weak keys of DES algorithm as explained in exercise 1;*

i. *Encrypt your text twice, with DES algorithm using one of the weak keys for both rounds.*
ii. *Again, encrypt the text twice, using a DES semi-weak key pair.*

***7.2.** A more secure alternative to DES is Triple DES, answer the following questions surrounding this algorithm;*

i. *Why is it more secure compared to DES?*
ii. *When implementing a brute-force attack, how large is its keyspace? Why isn't it larger?*
iii. *Compare its two versions with each other. (refer to your textbook)*
iv. *Encrypt your text using the CrypTool Triple DES encryption scheme with your desired key.*
v. *Knowing that CrypTool uses the second version of 3DES and encrypts the text with k1=k3 (it uses the key of the first encryption round for both the first and the third rounds), Encrypt the same text 3 times using the simple DES algorithm, with k1 = the first half of your key in the previous part, and k2 = its second half.*

***7.3.** Another secure approach compared to DES is DESX, which makes use of key whitening, answer the following questions about this method.*

i. *Encrypt your text using the CrypTool DESX algorithm with your desired key. (hint: this algorithm is found on Further algorithms menu)*
ii. *Again, encrypt the text making use of simple DES and classic XOR algorithms, with k = the first 8 bytes of your previous key, k1 = its second and k2 = its third 8 bytes.*

***7.4.** Encrypt your text using the AES algorithm and your desired key.*

Analysis

***7.5.** Answer the below parts using CrypTool analysis tool for AES;*

i. *Try to find the plain text utilizing the ciphertext in exercise 8.4 without entering any parts of the key. According to the analysis time shown in standard form, calculate how long it takes the software to verify a key, and provide the answer in microseconds.*

ii. *Now, enter 14 bytes of your key and see the ultimate results. How is the entropy related to the correct decryption of your ciphertext?*

Deliverables

Put the answer to each of the questions in your answer sheet. For CrypTool exercises, put the output files generated in every step in your answer file, as well.