Academic Year: Winter Semester 2021/22

6090: Security of Computer and Embedded Systems

Problem Sheet 6

Cryptographic Foundations Part 1

In this problem sheet, we will deepen our knowledge of symmetric cryptographic schemes. In particular, we will have a closer look on the cryptanalysis of simple encryption schemes and develop a better understanding of DES.

1. Cryptographic Concepts

This section contains a couple of multiple choice questions covering the basic concepts of cryptography. You might want to review the lecture slides and read Section 5.1 and Section 5.2 of Anderson [1] before working on these questions.

Exercise 1: *Cryptographic Concepts*

1. What is a cipher?
   - ☐ An algorithm performing encryption/decryption
   - ☐ An encrypted message
   - ☐ A method for breaking encrypted messages
   - ☐ An unencrypted message
2. The process of discovering a plaintext of a key is known as
   - ☐ Cryptography
   - ☐ Cryptanalysis
   - ☐ Steganography
   - ☐ Cryptoprocessing
3. The unencrypted message is called
   - ☐ Plaintext
   - ☐ Cleartext
   - ☐ Chiffre
   - ☐ Ciphertext
4. The order of letters in a message is rearranged by
   - ☐ Substitution cipher
   - ☐ Asymmetric cipher
   - ☐ Transpositional cipher
   - ☐ Symmetric cipher
5. Encryption protects against
   - ☐ Attacks
   - ☐ Loss of Data
   - ☐ Unavailability
   - ☐ None of the mentioned

2. Symmetric Encryption

In the following, we will deepen our knowledge of symmetric encryption schemes.

Exercise 2: *Cryptanalysis*

In this exercise, we will have a closer look on substitution and transposition ciphers. Thus, you might want to read Chapter 7 of Menezes et al. [2] before you start with the cryptanalysis in the following exercise.

The following cipher text is encrypted using a substitution cipher that leaves white spaces intact (e.g., the plain text starts with a word of length eight):

6G6CJ@?6 92D E96 C:89E E@ C6DA64E 7@C 9:D AC:G2E6 2?5 72>:=J =:76 9:D 9@>6 2?5 9:D 4@CC6DA@?56?46

Moreover, we assume the following relative letter frequency in the English language:[1]

Frequency	12.70	9.06	8.17	7.51	6.97	6.75	6.33	6.09	5.99	4.25	4.03	2.78	2.76
Letter	E	H	I	R	S	O	A	N	T	D	C	P	F
Frequency	2.41	2.36	2.23	2.02	1.97	1.93	1.49	0.98	0.77	0.15	0.15	0.10	0.07
Letter	V	M	L	Y	G	U	B	W	K	J	X	Q	Z

Apply a frequency analysis to obtain the plain text.

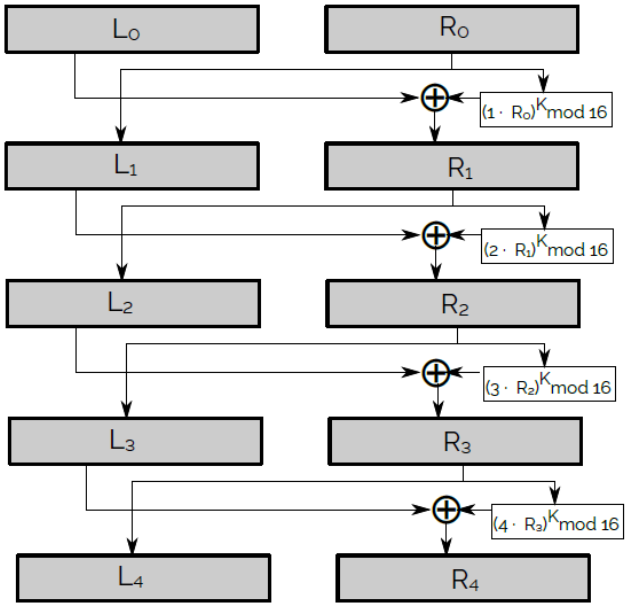
[1] The table is based on artificial data, as our example is only a very small cipher text. A table based on real data is, e.g., available at http://en.algoritmy.net/article/40379/Letter-frequency-Englis

Exercise 3: *DES*

In this exercise, we will deepen our understanding of the Data Encryption Standard (DES). A brief overview of DES is given in Chapter 7 of Schneier [3]; more details are provided in Chapter 7.4 of Menezes et al. [2].

In this exercise, we use simplified version of DES. 5 shows the structure of this DES-like encryption scheme. Our DES-like encryption scheme does not use an initial permutation and is based on

- A block length of 8
- Four rounds
- $f_i(x, K) = (i \cdot x)^K \bmod 16$ (for $i = 1, \ldots, 4$)



Encrypt $\mathtt{00011001}_2$ using they key $K = \mathtt{0101}_2$ $(= \mathtt{5}_{10})$

References

1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2001. The complete book is available at: http://www.cl.cam.ac.uk/~rja14/book.html
2. Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001. The complete book is available at: http://cacr.uwaterloo.ca/hac/
3. Bruce Schneier. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.