Cryptography, ITC8240 Assignment #2

Oskar Pihlak

TalTech — November 18, 2021

Introduction

This is the Assignment #2 submission for the Cryptography course, written in LaTeX.

1 2.1 Task 1: Key establishment

There are three secret agents Alex, Bob and Connie. They want to generate a common secret key so they can exchange secret messages. Design an extension of the Diffie-Hellman protocol that helps them to generate the key.

To recap - the Diffie-Hellmann family of algorithms work in a cyclic group with a generator g.
Every member in the party wishes to keep their privatly generated key private, meaning each exponentiation will be done in a different participator, meaning there will be intermediary steps which the parties have to send between each other before the key is established.
The protocol could be the following:
1. A, B, C generate private (secret) keys A_{sk}, B_{sk}, C_{sk}
2. A, B, C generate the public keys $A_{pk} = g^{A_{sk}}, B_{pk} = g^{B_{sk}}, C_{pk} = g^{C_{sk}}$
3. $A \xrightarrow{A_{pk}} B, B \xrightarrow{B_{pk}} C, C \xrightarrow{C_{pk}} A.$
4. Parties do exponentation.
5. $A \xrightarrow{C_{pk}^{A_{sk}}} B, B \xrightarrow{A_{pk}^{B_{sk}}} C, C \xrightarrow{B_{pk}^{C_{sk}}} A.$
4. Parties do exponentation.
5. $A \xrightarrow{B_{pk}^{C_{sk}^{A_{sk}}}} B, B \xrightarrow{C_{pk}^{A_{sk}^{B_{sk}}}} C, C \xrightarrow{A_{pk}^{B_{sk}^{C_{sk}}}} A.$

The three parties now know a common secret $B_{pk}^{C_{sk}^{A_{sk}}} = C_{pk}^{A_{sk}^{B_{sk}}} = A_{pk}^{B_{sk}^{C_{sk}}}$
Also seen on Figure 3.

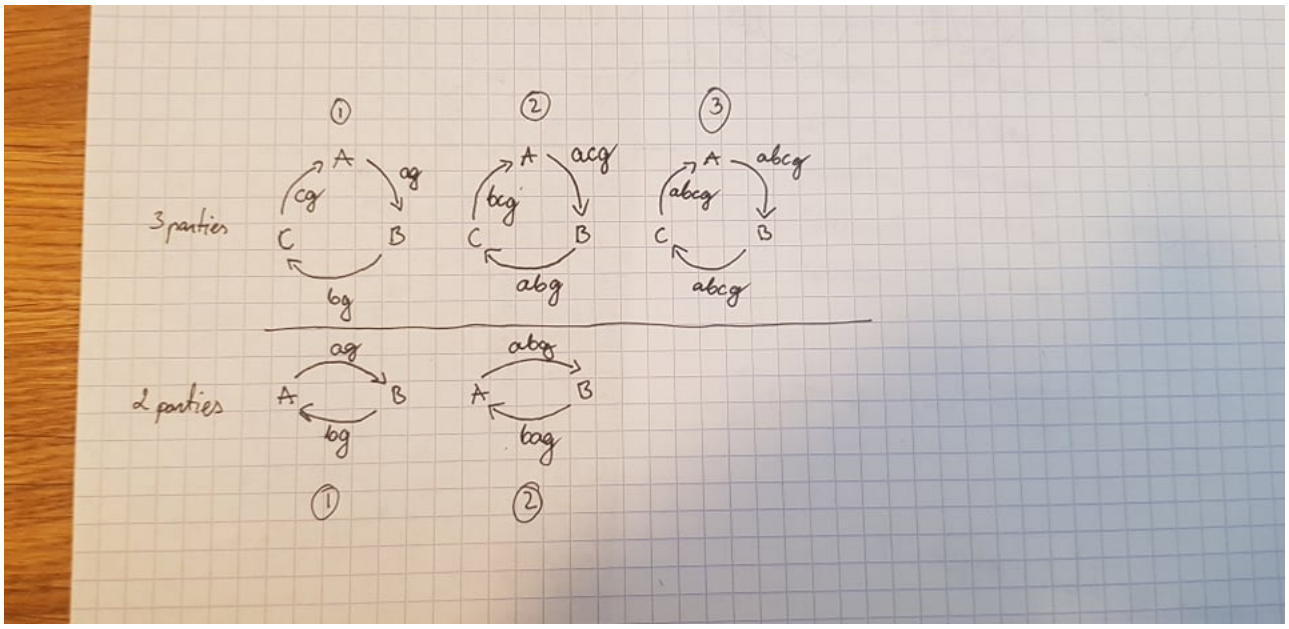

Figure 1: Diffie-Hellman key exchanges.

2 2.1 Task 2 - Block ciphers

Alice sends message m to Bob, encrypted with a block cipher. m is split into 6 blocks of equal length $m = m_0||m_1||m_2||m_3||m_4||m_5$ and encrypted using DES. In transmission one bit of the ciphertext c_2 changes its value.
Bob decrypts and gets message $m^{'} = m_0^{'}||m_1^{'}||m_2^{'}||m_3^{'}||m_4^{'}||m_5^{'}$.
Please, explain to Bob how many bits are expected to be wrong in each block $m_i^{'}$ if Alice used ECB or CBC mode.

Electronic codebook (ECB) cipher mode.
Since in ECB the only method used is confusion, then other blocks would not be affected by the single bit change inside the message m.

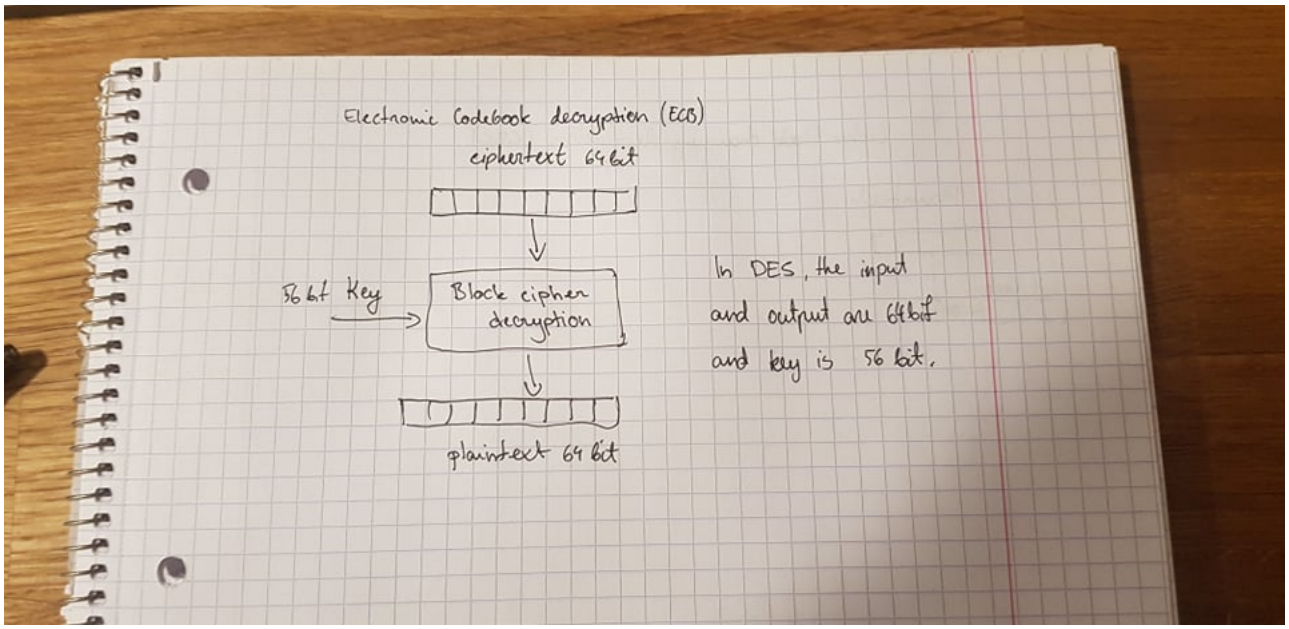

Figure 2: ECB decrypt

Hence only a single bit will be incorrect in the final message. The incorrect bit will occur in a single decryption block.

Cipher block chaining (CBC) cipher mode.
In CBC both diffusion and confusion are used. Meaning an incorrect bit will cause a cascade of incorrect bits on the condition that the invalid bit is not in the final decryption block which would mean that bit would be the only invalid bit. The closer the invalid bit is to the starting block the more bits are influenced. If the invalid bit is in the first block. Then in our example a single bit in every block would be incorrect, meaning there could be 1 - 6 invalid bits in a 6 block CBC cipher.

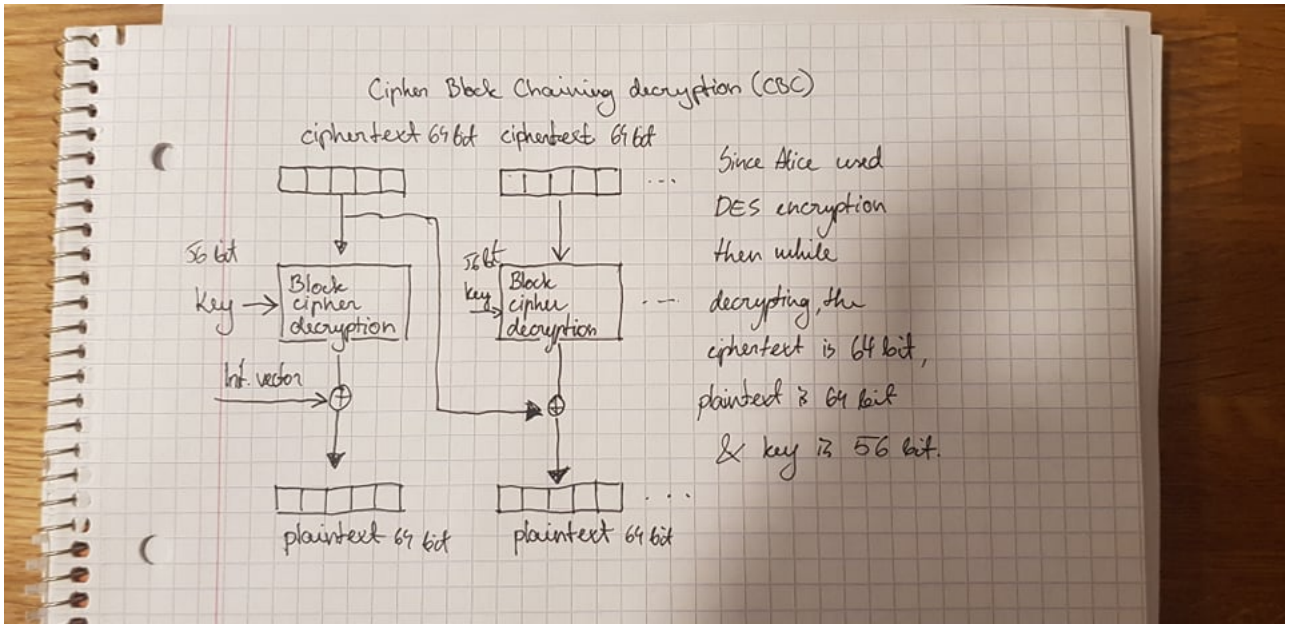

Figure 3: CBC decrypt.

3 2.3 Task 3 - Security definitions and proofs

Show that OTP (one time pad) in CBC mode does not satisfy the security definition, by describing an attack. We send $m_1 and m_2$ to the Challenger and get back c. The adversary would take c and check if conducting modulo arithmetic with the sent messages and recieved IV gives us back the recieved c or not. $c_2 = m_{0_0} \oplus m_{0_1} \oplus IV$ or $c_2 = m_{1_0} \oplus m_{1_1} \oplus IV$ which ever matches c. So it seems this advesary has an non-neglible advantage.

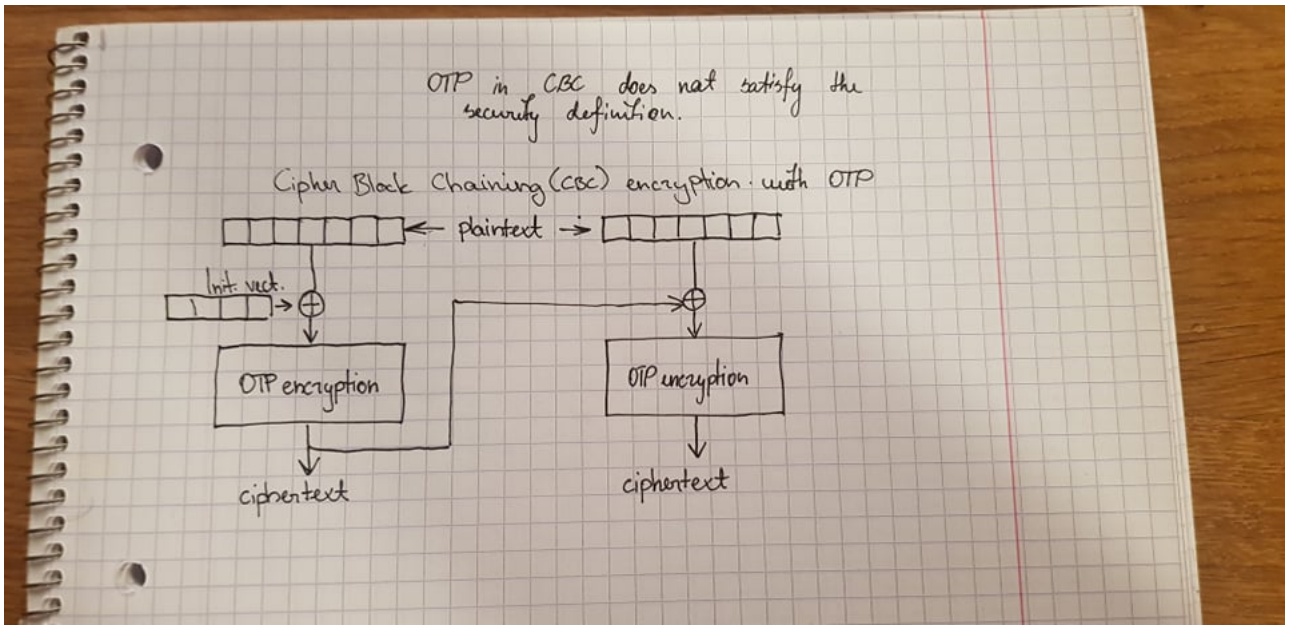

Figure 4: CBC encrypt mode with OTP.

4 2.4 Task 4 O-notation

Show that

$$O(n^3) = 11n^3 + 4n^2 + 9n - 36$$
$$11n^3 + 4n^2 + 9n - 36 \leq c \cdot n^3$$
$$c = 12$$
$$n^3 - 4n^2 - 9n + 36 \geq 0$$

Show that

$$O(n^4) = 5n^4 - 4n^2 - 4$$
$$5n^4 - 4n^2 - 4 \leq c \cdot n^4$$
$$c = 6$$
$$n^4 + 4n^2 + 4 \geq 0$$