Université Libre de Bruxelles
INFO-F-405 - Computer Security
Project: Meet-in-the-middle

Nikita Veshchikov

2015-2016

The purpose of this project is to better understand how a type of attacks called “Meet in the middle” works. We are going to use a toy example of a block cipher.

1 Meet in the middle

Meet in the middle (MitM) attack on block cipher is what is called a “known plaintext attack” i.e., the attacker was able to obtain several pairs of plaintext messages and their corresponding ciphertexts.

The main idea behind MitM attack is the memory-time trade-off. An attacker will take a known pair: a plaintext and a ciphertext. Then he will try to enumerate a part of a key in order to partially encrypt the plaintext (and store the results). Finally, the attacker would try to guess the remaining part of the key in order to partially decrypt the ciphertext and check if the obtained result matches one of the previously calculated partially encrypted plaintexts. One such match if found the whole key might be checked against a second known plaintext-ciphertext pair. See Figure 1 for a graphical representation of the idea behind MitM attack.

2 Project details

For this project we are going to use a block cipher called “Bad Block Cipher” (BBC). A `python` version of BBC is available on the UV. You will also be given a `csv` file that contains a list of plaintexts with their corresponding ciphertexts. Each message is encrypted with the same secret key that you will have to find. Plaintexts and ciphertexts in the file are represented in HEX format.

At the end of this project you should deliver a short report (maximum 6 pages excluding bibliographic references and appendixes). Your report should contain:

1. short description of your code (diagrams) and implementation choices,
2. a high level description of the BBC (diagrams and schemes that explain how it works),
3. a section where you describe difficulties that you met during this project (and solutions that you found),
4. a section that describe results of your project (the key that you found).

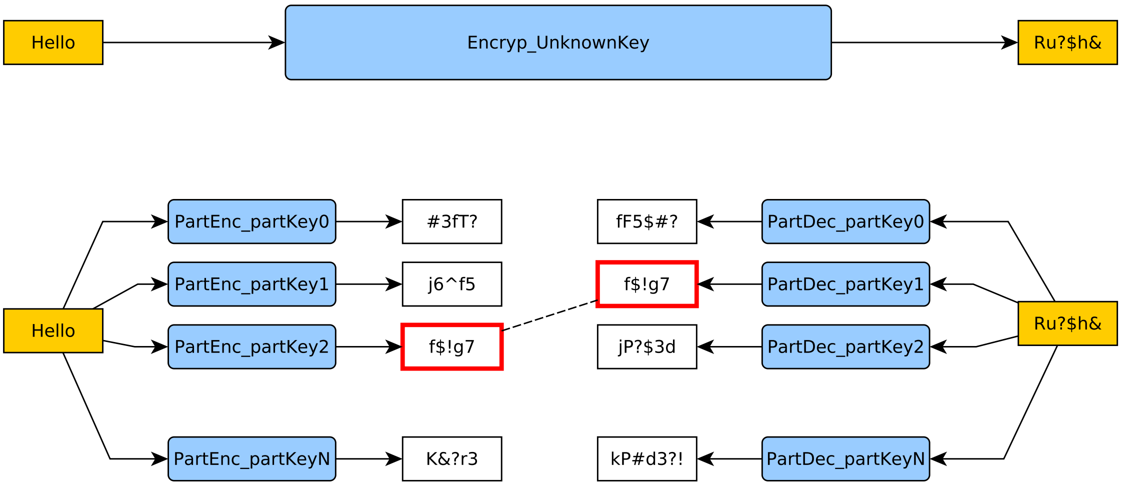

Figure 1: Meet in the middle attack on a block cipher. The full key is the combination of $partKey2$ (from the left part) and $partKey1$ (from the right part).

After the submission of the project you should also prepare a short (10 minutes) presentation that you should use for the defense of the project.

Each group will receive its own file with plaintexts and ciphertexts and you should use the file that was assigned to your group. However, you are allowed to break more than one key (break keys of other groups) and explain it in your report, in this case you will get some bonus points.

This project has to be done by groups of $5-6$ students. Each group should contain (if possible) at least one mathematician, at least one engineer and at least one computer scientist. A group must not consist of students that come from only one field (e.g. only engineers), there must be students of at least two different fields in each group (e.g. computer scientists and mathematicians).

The report should be submitted via UV before 23:55:00 on Monday, the 23rd of November.

You are allowed to use any programming language as well as any number of computers that are available to you.

Good luck!