Second homework solution

Snetkov Nikita / B88482

March 2020

1 Problem 1: Security definitions

1.1 Task

Your task is to write a security definition in Python (or another language, but we provide a template in Python). The goal of this is to give you a better understanding what security definitions mean, besides just being formulas

1. Write the security definition for IND-OT-CPA as a Python program. (Recall, in IND-OT-CPA, the adversary is called twice, so you will need two functions $adv1$ and $adv2$. Also pay attention to the following: the adversary should not be allowed to output messages that are not in the message space.)

2. Write an adversary that breaks the encryption scheme enc defined in the source code below. (This adversary should have a success probability, as measured by $test_indotcpa$ of at least 0.95.

1.2 Solution

I decided to use Java language for this task. The main strategy of adversary is always send two messages - 0 and 1. When adversary needs to guess which message was encrypted - adversary send b=0 if ciphertext is 0; and 1 otherwise. This is strategy always works for encryption scheme enc, due to the fact formula $enc = key * message$ will always give zero if message is also equals to zero (it doesn't matter what key was generated).

The code listing provided here:

```
public class Lab2{
        public static long enc(long key, long message){
                return key*message;
        }

        public static long[] adv1(){
                long[] buff = new long[]{0,1};
                return buff;
        }

        public static int adv2(long cipher){
                if (cipher == 0){
                        return 0;
                }
                else{
                        return 1;
                }
        }

        public static boolean indotcpaGame(){
                long size = (long)Math.pow(2,32);
                int bit = (int)(Math.random()*2);
                long key = (int)(Math.random()*size);
```

```
                long message[] = new long[2];
                while(true){
                        message = adv1();
                        if (0>message[0] || message[0]>size ||
                        0>message[1] || message[1]>size){
                                System.out.println("Wrong size of messages");
                        }
                        else break;
                }
                long cipher = enc(key,message[bit]);
                int bit2 = adv2(cipher);
                if(bit2 == bit){
                        return true;
                }
                return false;
        }
        public static void test_indotcpa(){
                int numTrue = 0;
                int numTries = 10000000;
                for(int i=0; i<numTries; i++){
                        if (indotcpaGame()){
                                numTrue++;
                        }
                }
                float ratio = numTrue/numTries;
                System.out.println(ratio);
        }

        public static void main (String[] args) {
                test_indotcpa();
        }
}
```