

Problem Set 5

Due 12/1/2005

Send to tmorgan@ccs.neu.edu, with CC to noubir@ccs.neu.edu

Problem 1 (20 points):

Textbook exercise 4.5, page 151.

Problem 2 (80 points):

This problem aims at cracking Comp-128 one of the implementations of the GSM A3/A8 algorithm.

GSM is a standard for cellular phones (<http://www.gsmworld.com/index.shtml>). In the US it is used by operators such as tmobile and cingular. Authentication of subscribers relies on a SIM card (Subscriber Identity Module) which is essentially a smart card with a secret key and two cryptographic algorithms (A3, A8). These algorithms are used for authenticating the subscribers and establishing a secret key for encrypting the traffic. The SIM card is tamperproof (i.e., you cannot read the secret key inside), but you can query it.

For more information on GSM security, read sections 3.1 & 3.2 of "GSM Interception" by Lauri Pesonen (<http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html>).

Problem Statement:

Assume that you have access to a SIM card that implements COMP128. You can only make the following call:

```
void SIMcard(Byte rand[16],Byte simoutput[12]);
```

Given an input `rand` computes `simoutput` (See link to `a3a8.c` for an implementation of COM128:

<http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F05/PS5/a3a8.c>

Your task is to find the secret key inside the SIM card. Analyze Comp-128 algorithm, and write a program to find the key in the SIM card. Document your approach/strategy. Demonstrate that you are able to recover a key.

Hints: There's a narrow "pipe" inside COMP128. Bytes `i,i+8,i+16,i+24` at the output of the second level depend only on bytes `i,i+8,i+16,i+24` of the input to COMP128. Since the second level has only 7 valid bits for each byte, by using differential technique you will be able to compute the secret key inside the chip.)

Bonus Points: SIM.h and SIM.o (compiled for CCIS Unix System) are given to you to emulate the SIM card. Find the secret key in SIM.o. Remember the result should be reproducible.

<http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F05/PS5/SIM.h>

<http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F05/PS5/SIM.o>

Note: Since the first attack against COMP-128 was discovered, most operators have moved to more secure versions such as COMP128-2, COMP128-3.

Additional links:

<http://calliope.uwaterloo.ca/~ssjsin/COMP128.pdf>

<http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F05/PS5/GSM-Cloning-WangKleiner.ppt>

<http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F05/PS5/COMP128-WangKleiner-Report.doc>