Proposal for Master's Degree Project

Title: Implementing and Evaluating Nonsingular Matrices Generators for the Hill Cipher

Advisor and Contact
Pedro R. M. Inácio (inacio@di.ubi.pt), Ph.D.
Aleksandra Mileva (aleksandra.mileva@ugd.edu.mk), Ph.D. (co-advisor from Goce Delcev University)

Summary / Scope

The Hill Cipher is one of the most well known classical ciphers. Thought it is not really used in practice, it exhibits interesting properties of a symmetric key cipher, namely in terms of diffusion. Obviously, using the same key matrix to encrypt more than one block makes this cipher susceptible to the ciphertext only attack. Enhancing the cipher with a method to generate different key matrices for each block would solve that weakness, though the way matrices are generated needs to be carefully considered.

This master's project touches areas such as Information Security, Linear Algebra and Programming. It is focused on studying methods for generating nonsingular matrices and their applicability to cryptographic purposes. It will involve the implementation of at least two of those methods: one known from the literature and another one devised within the scope of this work. The evaluation will be mostly focused on assessing randomness of the matrices and ciphertexts produced, validating them resorting to well-known batteries of tests for randomness (e.g., [1]). Apart from the evaluation of both methods, the project should output the implementations of the methods in C programming language, as well as an implementation of the Hill cipher using the best of the methods. The main research challenge consists in evaluating the generators, even if for a number of particular small sized matrices (e.g., 3x3 or 4x4). The implementation should nonetheless be oriented towards 32x32 or 64x64 bit matrices.

During this master's project, the student will have the chance to engage in discussions with other people involved in the area of information security, as well as the opportunity to improve his or her knowledge in several computer science fields, namely maths and programming.

Objectives
As hinted in the previous discussion, this master's project has three main objectives:

1. Study means to generate nonsingular matrices;
2. Implement and evaluate the nonsingular matrices generators for the pur-

poses of cryptography;

3. Implement a modified Hill Cipher integrating the best method, optimized for computer words and with side-channel attacks in mind.

Tasks

In order to achieve its objectives, the following tasks are proposed as an initial work plan for this master's project:

Task 1 Getting acquainted with the context of the problem at hands and with the objectives of the project, as well as with the technologies involved. Revision of the specialized literature and related works (2 months);

Task 2 Identify methods for generating nonsingular matrices and implement them (2 months);

Task 3 Describe the randomness of the matrices produced, as well as of the ciphertexts (vectors) that may be obtained from multiplying them by (vector) patterns (1 month);

Task 4 Use batteries of tests to evaluate the randomness of the matrices and outputs produced by multiplying them by (vector) patterns (1 month);

Task 5 Implementation of an Hill cipher integrating the best method optimized to *computer words* and integrating side-channel attacks prevention (1 month);

Task 6 Writing of the master's dissertation, technical documentation and a conference paper (3 months, eventually distributed and interleaved with the time periods of other tasks).

Timetable

An approximate scheduling for the execution of the previously identified tasks is included below. The execution of a given task in a given month is marked with a cross (x).

Task \ Month	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
1	x	x									
2			x	x							
3					x						
4						x					
5							x				
6								x	x	x	

Expected Outcomes and Dissertation

The most visible outcome of this master's project are the implementation of the nonsingular matrices and of the modified Hill cipher Implementing them. The results from the evaluation of those methods are nonetheless the main outcomes of this work. This evaluation may be the subject of a scientific conference pa-

per. The final dissertation, entitled *"Implementing and Evaluating Nonsingular Matrices Generators for the Hill Cipher,"* may be written in English aiming for the international dissemination of this work.

References

[1] Pierre L'Ecuyer and Richard Simard. 2007. TestU01: A C library for empirical testing of random number generators. ACM Trans. Math. Softw. 33, 4, Article 22 (August 2007), 40 pages.