ECE 5960/6960-010: Hardware Cryptography and Security

Prepared by *Priyank Kalla*
Spring 2024, Homework # 1
Due Date: Sunday Feb 4, 2024.

- As you work through the HWs and projects in the course, you will find the need to typeset your math formulas, algorithm pseudocode, figures, graphs, etc. I strongly recommend using LaTeX for this purpose.

  For your benefit, a LaTeX tarball is also uploaded on the class website, under the 'CAD tools Software and Benchmarks' section. If you aren't a LaTeX expert, you can now get started with using LaTeX for typesetting technical documents and manuscripts. I hope you will be brave enough to typeset this HW and subsequent HWs also in LaTeX ☺. Download the tarball, and go through the file latex-for-class.pdf. It is self-explanatory.
- For all computations, you are encouraged to use the SINGULAR computer algebra tool. Info is provided on the class website. Singular is installed on the CADE lab machines under `'/usr/local/bin/Singular'`. Notice that the 'S' in Singular is upper-case. Feel free to download the latest version on your own personal computers for use.
- *Read Singular's manual.* In the manual, you only need to glance through the following sections for now:
  1) Section 2 on Introduction, of course: particularly 2.3.1, 2.3.2, 2.3.3.
  2) Section 3.1 (usage), 3.3 (rings and orderings), 3.7 and Section D.3 for the linear algebra libraries. You are free to use any available library in Singular, particularly "linalg.lib" and "matrix.lib".
  3) Just be careful, there are limited algorithms available for computations $\pmod n$, i.e. in $\mathbb{Z}_n, n \neq p$.
- On a unix terminal, the way to load a singular script file is as follows:

```
prompt>> Singular
                     SINGULAR                                 /
 A Computer Algebra System for Polynomial Computations   /   version 3-1-1
                                                       0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann        \   Feb 2010
FB Mathematik der Universitaet, D-67653 Kaiserslautern    \
> < "matrices.sing";
```

Now, let's get to the assignment:

1) (20 points) Briefly describe the *Extended Euclidean algorithm*, provide a pseudocode, and demonstrate it's application for the computation of modular multiplicative inverses in $\mathbb{Z}_n$.
   a) Implement the extended Euclidean algorithm in Singular, preferably as a procedure in Singular. [Note: Singular already provides a library function gcd(), so you may wish to name your procedure as `my_gcd()` to avoid conflict.]
   b) Using your procedures, compute the gcd over integers: $\mathrm{GCD}(200, 180, 450, 610)$.
   c) Using your `my_gcd()` procedure, identify whether the integers 38 and 7 have multiplicative inverses in $\mathbb{Z}_{180}$. If so, compute their inverses.

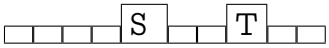
2) (15 points) In class, we have studied how to solve linear Diophantine equations (LDEs), as well as linear congruences (LCs) in 1 variable $\pmod m$. The procedures are given in the lecture slides. In this question, you will investigate how LDEs and LCs are related to each other.
   a) Solve the LC $4x \equiv 4 \pmod 6$. How many solutions does the congruence have? Enumerate the solutions $\pmod 6$.
   b) LDEs and LCs can be transformed into one another. You are now asked to transform this LC into an equivalent LDE, and solve the corresponding LDE, using the LDE solving procedure given in the slides. [*Hint:* To transform an LC into an LDE, observe that $a \equiv b \pmod c$ means that $c \mid (a - b)$.]

3) (20 points) Alice and Bob agree to exchange messages using an affine cipher (k_1, k_2) where k_1 is the multiplicative key and k_2 the additive key. Alice is going on a vacation, and wants Bob to join her. When Bob asks her about the destination, Alice sends to Bob the following

10-character ciphertext codeword:

H W X U E Y W T K U (ignore the spaces)

Moreover, Alice also tells Bob that the 5^{th} plaintext character is S and the 8^{th} character is T. In other words, the plaintext is like:



Where should Bob join her for vacation?

Of course, for integer values of the characters, we always use Fig. 1.

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fig. 1: Integer value of characters in $\mathbb{Z}_{26}$

4) (45 points) [*Hill ciphers: Can matrices that do not have inverses help obfuscate the key? Or is it necessary for key matrices to be unique? This HW problem should help you understand this concept, as well as demonstrate the application of solving linear congruences when matrices do not have inverses. Please solve this question very carefully. This may be non-trivial.*]

Consider a (hypothetical) Hill cipher where, instead of the 26 letters of the English language alphabet, only 8 letters are used. Thus, all computations are performed $\pmod 8$. Recall that encipherment with Hill ciphers comprises of a $m \times m$ key matrix $\mathbf{K}$, such that encryption $\mathbf{C} = \mathbf{P} * \mathbf{K}$, and decryption $\mathbf{P} = \mathbf{C} * \mathbf{K}^{-1}$.

Alice wants to generate a key matrix $\mathbf{K} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$ so as to encrypt a plaintext matrix $\mathbf{P} = \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}$ to obtain the ciphertext matrix $\mathbf{C} = \begin{pmatrix} 4 & 5 \\ 0 & 7 \end{pmatrix}$. Also, $\mathbf{K}$ should be such that Bob should be able to decrypt Alice's message. Answer the following:

a) Set up the problem as a system of linear congruences to solve so as to identify a key matrix $\mathbf{K}$. Your matrix $\mathbf{K}$ should work for both encryption and decryption: i.e. $\mathbf{C} = \mathbf{P} \cdot \mathbf{K} \pmod 8$ as well as $\mathbf{P} = \mathbf{C} \cdot \mathbf{K}^{-1} \pmod 8$.

b) Is the given matrix $\mathbf{P}$ invertible? Is the given matrix $\mathbf{C}$ invertible? In other words, can we compute the key as $\mathbf{C} \cdot \mathbf{P}^{-1} = \mathbf{K}$?

c) Does there exist a unique (one and only one) key matrix $\mathbf{K}$ that satisfies these constraints? If not, how many distinct matrices $\mathbf{K}$ can be used for this cipher?

d) Based on the above analysis, explain whether the above system is secure to a known-plaintext or a chosen-plaintext attack? [Note: A known-plaintext attack is one where some $(\mathbf{P}, \mathbf{C})$ pairs are known to Eve. A chosen-plaintext attack is similar to the known-plaintext one, except that the $(\mathbf{P}, \mathbf{C})$ pairs are chosen by the attacker herself.]