MATH 75: Cryptography **Spring 2022**

PSET 4 — April 29, 2022

Prof. Asher Auel ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***Cryptography*** by **Simon Rubinsen-Salzedo**

Problems

1. Let

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}.$$

For which n is the matrix A invertible over $\mathbb{Z}/n\mathbb{Z}$? Find its inverse if $n = 100$.

For the matrix A to be invertible over $\mathbb{Z}/n\mathbb{Z}$, it must be the case that $\det A \not\equiv 0 \pmod{n}$, i.e. $\det A$ and n are coprime.

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{vmatrix} = 1 \cdot 2 - 2(-2) + 3(-3) = 2 + 4 - 9 = -3$$

Thus, A is not invertible in any group $\mathbb{Z}/n\mathbb{Z}$ where $3 \mid n$.
A^{-1} in $\mathbb{Z}/100\mathbb{Z}$, via row-reduction:

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 10 & 0 & 0 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -11 & -7 & 0 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 4/3 & 1/3 & 0 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 2 & 0 & -2 & 6 & -3 \\ 0 & 1 & 0 & -2/3 & 11/3 & -2 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -2/3 & -4/3 & 1 \\ 0 & 1 & 0 & -2/3 & 11/3 & -2 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}\right]$$

$$\begin{aligned}
\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{bmatrix}^{-1} &= \begin{bmatrix} -2/3 & -4/3 & 1 \\ -2/3 & 11/3 & -2 \\ 1 & -2 & 1 \end{bmatrix} \\
&\equiv \begin{bmatrix} -2 \cdot 3^{-1} & -4 \cdot 3^{-1} & 1 \\ -2 \cdot 3^{-1} & 11 \cdot 3^{-1} & -2 \\ 1 & -2 & 1 \end{bmatrix} \pmod{100} \\
&\equiv \begin{bmatrix} -2 \cdot 67 & -4 \cdot 67 & 1 \\ -2 \cdot 67 & 11 \cdot 67 & -2 \\ 1 & -2 & 1 \end{bmatrix} \pmod{100} \\
&\equiv \begin{bmatrix} 66 & 32 & 1 \\ 66 & 37 & 98 \\ 1 & 98 & 1 \end{bmatrix} \pmod{100}
\end{aligned}$$

Just to be sure...

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{bmatrix} \begin{bmatrix} 66 & 32 & 1 \\ 66 & 37 & 98 \\ 1 & 98 & 1 \end{bmatrix} = \begin{bmatrix} 201 & 400 & 200 \\ 600 & 901 & 500 \\ 1000 & 1500 & 801 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \pmod{100}$$

2. Alice uses the Hill cipher, encrypting the plaintext

Consistency is the last refuge of the unimaginative

to get the ciphertext

`voqimugocogmttfkxvlvdynhawugtfrsksoizgaanlygk`

to send to Bob using blocks of size $m = 3$ (and $n = 26$). Playing the role of Eve, hack Alice's encryption key $A \in M_3(\mathbb{Z}/26\mathbb{Z})$. The matrix key spells out a keyword: what is it?

After you find the key, notice that Alice has not followed the protocol correctly. Explain why, then find two plaintexts that encrypt to the same ciphertext using Alice's key.

Since we know the plaintext that was encrypted, we can use it (and the corresponding ciphertext) to pull out equations from the encryption and find the key.
Let $A = \left(\begin{smallmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{smallmatrix}\right)$ be the encryption matrix.
Then, we know that:

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \begin{bmatrix} c & t & a \\ o & e & t \\ n & n & i \end{bmatrix} \equiv \begin{bmatrix} v & g & a \\ o & o & n \\ c & c & l \end{bmatrix} \pmod{26}$$

We can now focus on the equations.

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \begin{bmatrix} c & t & a \\ o & e & t \\ n & n & i \end{bmatrix} \equiv \begin{bmatrix} v & g & a \\ o & o & n \\ c & c & l \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \begin{bmatrix} 2 & 19 & 0 \\ 14 & 4 & 19 \\ 13 & 13 & 8 \end{bmatrix} \equiv \begin{bmatrix} 21 & 6 & 0 \\ 14 & 14 & 13 \\ 16 & 2 & 11 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \equiv \begin{bmatrix} 21 & 6 & 0 \\ 14 & 14 & 13 \\ 16 & 2 & 11 \end{bmatrix} \begin{bmatrix} 2 & 19 & 0 \\ 14 & 4 & 19 \\ 13 & 13 & 8 \end{bmatrix}^{-1} \pmod{26}$$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \equiv \begin{bmatrix} 21 & 6 & 0 \\ 14 & 14 & 13 \\ 16 & 2 & 11 \end{bmatrix} \begin{bmatrix} 15 & 10 & 25 \\ 19 & 14 & 22 \\ 0 & 13 & 18 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \equiv \begin{bmatrix} 13 & 8 & 7 \\ 8 & 11 & 8 \\ 18 & 19 & 18 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \equiv \begin{bmatrix} N & I & H \\ I & L & I \\ S & T & S \end{bmatrix}$$

The matrix key spells out the word `NIHILISTS`.

Alice's encryption matrix is faulty because its determinant, 16, is not coprime with 26. This means the matrix is not invertible since it is not injective—for example, it maps both "" and "" to "". Bob needs to be able to find the inverse in order to decrypt the message.

3. The Hill cipher succumbs to a known plaintext attack if sufficiently many plaintext-ciphertext pairs are known. It is even easier to break the cipher if Eve can trick Alice into encrypting a chosen plaintext, a *chosen plaintext attack*. Describe such an attack.

Although the Hill cipher generates somewhat "contextualized" ciphertext by having each letter's encryption depend on a number of letters surrounding it, the ciphertext it generates, when broken down into appropriate block sizes, is always the same linear combination of the corresponding plaintext blocks.
This is the weakness in the system—if enough plaintext and corresponding ciphertext is known, then attackers (Eve, in this case) can compute the

The Hill cipher produces the same linear combinations of the letter vectors it receives. While this is helpful in avoiding single-letter encryption and ensuring that a letter's encryption is, to an extent, also dependent on its surrounding letters, it is also a weakness — suppose a set of vectors and the corresponding set of ciphertexts is known, then Eve can easily solve solve a linear system of equations to find the key.
A chosen plaintext attack is a situation where an attacker (Eve, in this case) tries to get the encryptor (Alice) to encrypt a specific word or words. Using the original and encrypted forms of the words, Eve can generate the systems of equations she needs to figure out the encryption matrix, henceforth breaking Alice's encryption.

4. Let $n \in \mathbb{Z}_{>0}$. We consider the row-reduction algorithm over $\mathbb{Z}/p\mathbb{Z}$ where p is prime. Recall that every nonzero element in $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse, so that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a *field* and all the methods of linear algebra apply.

Find an explicit polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 such that no more than $f(n)$ operations in $\mathbb{F}_p$ are required by the row-reduction algorithm for computing the determinant of a matrix in $M_n(\mathbb{F}_p)$. How many of these operations are inversions of nonzero scalars?

Suppose we have an n by n matrix A in $M_n(\mathbb{F}_p)$.
We can find the determinant of A by row-reducing A into a triangular matrix then finding the product of the pivot-position elements.
We first remove the lower non-diagonal elements in the first column, then the second, and so on up to the $n-1$th column. The n'th column's diagonal element, being in the last row in the matrix, has no rows below it.
This step involves:

- Finding the inverse of the diagonal element. This is a total of $n-1$ inversions (1 per column, over the $n-1$ columns).
- Adding a multiple of the row to *all the rows below the current element that have a non-zero element in the column of interest*, such that we cancel out the nonzero value. This involves a multiplication and an addition.

This is a total of $n-1$ inversions $+\sum_{i=1}^{n-1} i$ row additions, which add up to
$n-1$ **inversions** $+2 \cdot \frac{n(n-1)}{2} = n(n-1)$ **row multiplications and additions**.
However, each row multiplication or addition requires doing the operation on each of the n elements of the row.
Thus, the total comes to $n - 1 + n(n-1) \cdot n = \frac{n^3-n^2}{2} + n - 1$.
Finally, we need to multipy the n diagonal elements to find the determinant, making a total of
$n^3 - n^2 + 2n - 1$ integer operations.
Of these operations, $n-1$ are inversions of nonzero scalars, and $n^3 - n^2 + n$ are integer additions and multiplications.

5. Decrypt the message

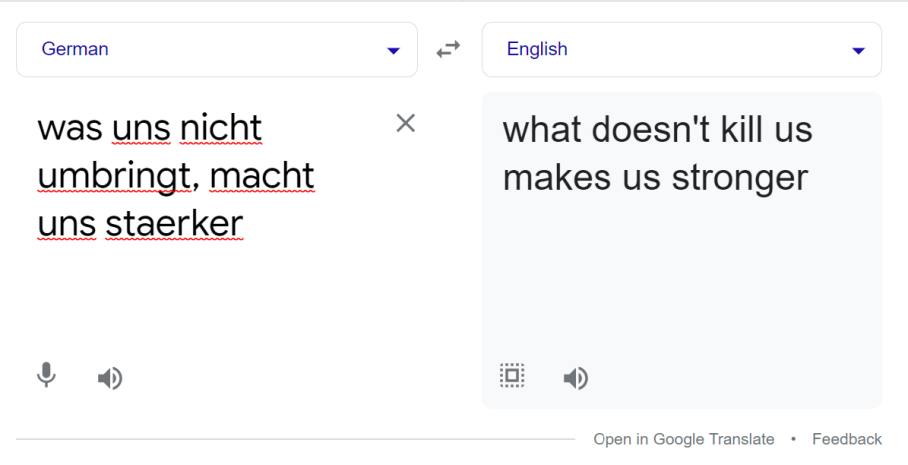
`CLV SSH = MMBVC RDMVE PFZII EAVYS XFTHS FNMOB RRPDH VBSQH`

with the following Enigma settings:

```
Walzenlage (Rotors): I V III
Ringstellung (Ring setting): 13 06 24
Steckerverbindungen (Plug connections): AU PB EF IQ RH ZL DT MS CG KN
Kenngruppen: KIJ TFR BVC ZAE
```

[Hint: The message is in German!]

First, after plugging in the rotor and ring settings, I used the first 3 letters of the key (`CLV`) as the rotor starting positions to decrypt the second part of the key (`SSH`) to get `PJR`.
Using `PJR` as the new starting position for the rotors, I decrypted the message
`RDMVE PFZII EAVYS XFTHS FNMOB RRPDH VBSQH` (skipping the key identification group, `MMBVC`)
to get `wasun snich tumbr ingtm achtu nssta erker`
I plugged this into Google translate and, after a little trial-and-error with spacings, got out the message
`what doesn't kill us makes us stronger`



6.

Read Section 15.1 (pages 368–376) of*The Pleasures of Counting* by Koerner (posted on Canvas) and do Exercises 15.1.1–15.1.3.

Exercise 15.1.1 *Suppose that the encipherment of* THEGENERALHE *is*

ALAPHQNSNTTL

but the trial alphabets are as in Table 15.1. (For convenience we give the appropriate alphabets in Table 15.2.) Draw a menu and carry out a few stages of the appropriate deductions.

In Chapter 13 of [94], Derek Taunt discusses the work involved in setting up a menu. We can well believe that 'Much skill, ingenuity, and judgement could be expended on the composition of good menus from otherwise intractable material.' The construction of the prototype

Table 15.2. *A possible Enigma encipherment?*

	In	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Out
1	T	JFQXHBSEKAIYZTVUCWGNPORDLM	A
2	H	PNSKUZOWVLDJRBGATMCQEIHYXF	L
3	E	KDPBIQTMEOANHLJCFTGRXZYUWV	A
4	G	XODCHZLEPYUGQWBIMVTSKRNAJF	P
5	E	OFYEDBZXLWQINMASKVPUTRJHCG	H
6	N	VWPTMXKUOLGJEZICRQYDKABFSN	Q
7	E	DRTAGUEMZKJXIVYWSBQCFNPLOI	N
8	R	VZEJCQUNLDYIRHWXFNTSGAOPKB	S
9	A	HXIZGPEACYOVSTKFWUMNRLQBJD	N
10	L	HVXMZIKAFSGWDQURNPJYOBLCTE	T
11	H	OWMPYLTZKXIGCUADRQVFNSBJEH	T
12	E	RUZLJYITFEMDKXQROAPHBWVNFC	L

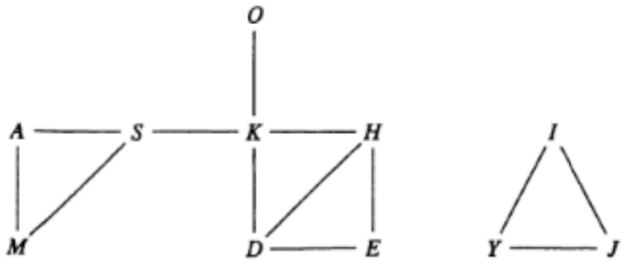


Figure 15.2: A good menu.

bombes must have been accompanied by many hand trials, much discussion of more or less plausible mathematical models and a great deal of nail-biting.

So far we have dealt with what will happen if our rotors and their positions do not correspond to those in the original Enigma. What will happen if they do? Table 15.3 shows an encipherment (for some unrevealed plugboard setting) corresponding to the 12 substitution codes shown.

Exercise 15.1.2 *Suppose we are in the situation given by Table 15.3. Draw the menu and carry out completely all the appropriate deductions which can be made starting from* E ↔ L.

I believe that the reader who carries out Exercise 15.1.2 will obtain the statements E ↔ L, N ↔ N, I ↔ I, Z ↔ B, D ↔ A, H ↔ Y, G ↔ C, X ↔ F, T ↔ Q and no more. This suggests that (as, in fact, is the case) we have the correct alphabets (and so the correct rotors in the correct positions) and the correct steckering E ↔ L. What will happen if we test another steckering, say E ↔ E?

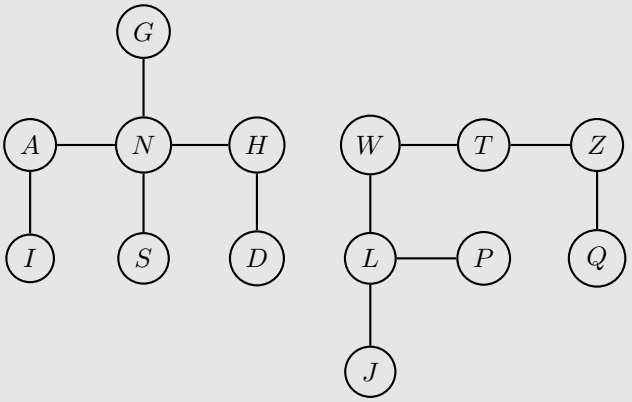
Exercise 15.1.3 *Suppose we are in the situation given by Table 15.3 (and for which you drew the menu in Exercise 15.1.2). Carry out the first few stages of deductions starting from* E ↔ E.

Once again we expect an avalanche of statements to follow from the false assumption E ↔ E. However, *there is one statement about the steckering of* E *that cannot form part of the avalanche.* We have already seen that every statement in the avalanche is deducible from every other.

Table 15.3. *A correct Enigma encipherment.*

	In	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Out
1	T	JFQXHBSEKAIYZTVUCWGNPORDLM	G
2	H	PNSKUZOWVLDJRBGATMCQEIHYXF	F
3	E	KDPBIQTMEOANHLJCFTGRIZYUWV	N
4	G	XODCHZLEPYUGQWBIMVTSKRNAJF	A
5	E	OFYEDBZXLWQINMASKVPUTRJHCG	I
6	N	VWPTMIXUOLGJEZICRQYDKABFSN	B
7	E	DRTAGUEMZKJXIVYWSBQCFNPLOI	F
8	R	VZEJCQUNLDYIRHWIFNTSGAOPKB	J
9	A	HXIZGPEACYOVSTKFWUMNRLQBJD	B
10	L	HVIMZIKAFSGWDQURNPJYOBLCTE	B
11	H	OWMPYLTZXIGCUADRQVFNSBJEH	L
12	E	RUZLJYITFEMDKIQROAPHBWVNFC	A

(a) 15.11



(b) 15.12
(c) 15.13