Algebra for Cryptology

Arkadii Slinko

Department of Mathematics
The University of Auckland

Auckland, 6 April, 2013

What is cryptology?

Cryptology is about communication in the presence of adversaries or potential adversaries.

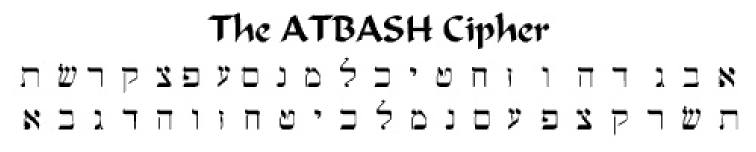
It addresses the following problems in particular:

- secrecy;
- privacy;
- authentication:
  - passwords;
  - digital signitures;
  - friend-or-foe identification
- digital money.

It is now an integral part of a modern society.

Cryptology in Aincient History 1

One of the oldest cyphers known is Atbash. It appears in the Hebrew Scriptures of the Bible. Any letter of the alphabet is replaced by the 'symmetric' letter.



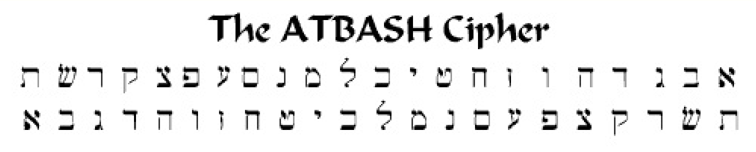
The ATBASH Cipher

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א

Cryptology in Aincient History 1

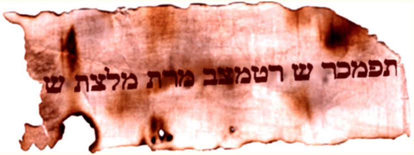
One of the oldest cyphers known is Atbash. It appears in the Hebrew Scriptures of the Bible. Any letter of the alphabet is replaced by the ‘symmetric’ letter.



The ATBASH Cipher

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

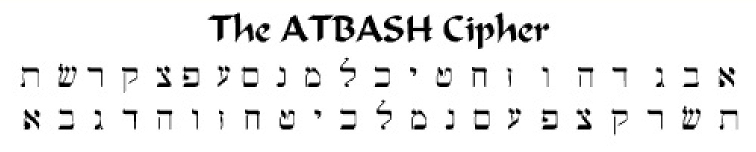
ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א



תפמכר ש רטמצב מרת מלצת ש

Cryptology in Aincient History 1

One of the oldest cyphers known is Atbash. It appears in the Hebrew Scriptures of the Bible. Any letter of the alphabet is replaced by the ‘symmetric’ letter.



The ATBASH Cipher

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

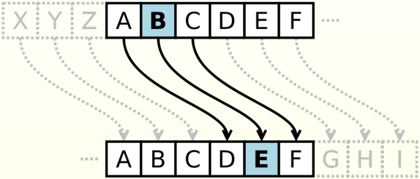
ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א

Example for Latin alphabet:

$$\text{MATH} \longrightarrow \text{NZGS}.$$

Cryptology in Aincient History 2

Caesar is also a very old cypher used by Gaius Julius Caesar (130 BC - 87 BC). Letters are simply replaced by letters three steps further down the alphabet.

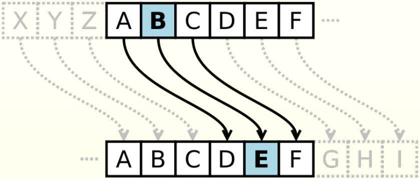


Example:

$$\text{MATH} \longrightarrow \text{PDWK}.$$

Cryptology in Aincient History 2

Caesar is also a very old cypher used by Gaius Julius Caesar (130 BC - 87 BC). Letters are simply replaced by letters three steps further down the alphabet.



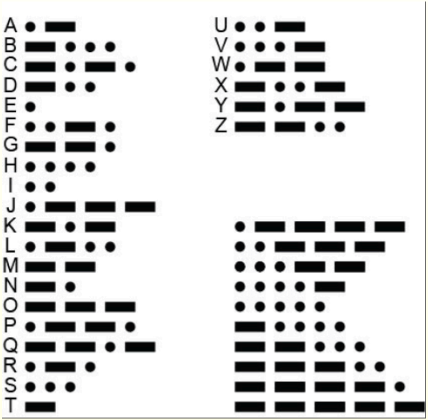
Example:

$$\text{MATH} \longrightarrow \text{PDWK}.$$

These two cyphers are examples of the so-called substitution methods.

One-time pad 1

The one-time pad is a nearly perfect cryptographic solution. It was invented in 1917 by Gilbert Vernam for use in telegraphy with International Morse Code.



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 ▬ ▬ • •

• ▬ ▬ ▬ ▬
• • ▬ ▬ ▬
• • • ▬ ▬
• • • • ▬
• • • • •
▬ • • • •
▬ ▬ • • •
▬ ▬ ▬ • •
▬ ▬ ▬ ▬ •
▬ ▬ ▬ ▬ ▬

The simplest algebra

The set $\mathbb{Z}_2 = \{0, 1\}$ admits the following algebraic operations: with the binary addition

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0,$$

and the binary multiplication

$$0 \times 0 = 0, \quad 0 \times 1 = 0, \quad 1 \times 0 = 0, \quad 1 \times 1 = 1,$$

The binary 0 and 1 represent parities, so that 0 stands for "even" and 1 stands for "odd." Having this in mind it is not surprising that $1 + 1 = 0$, because it simply means that "odd"+"odd"="even."

One-time pad 2

Suppose that parties share a very long string k of randomly chosen 0's and 1's (the key).

If Alice wishes to send a message, which is a string of zeros and ones

$$m = m_1 m_2 \dots m_n,$$

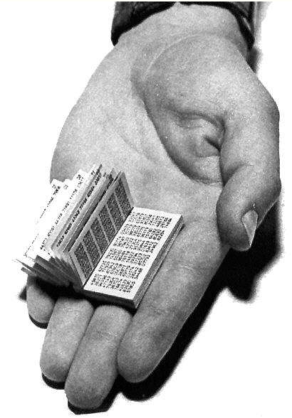
she takes the first n numbers from k, that is $k^{'} = k_1 k_2 \dots k_n$ and add these two strings component-wise mod 2 to get the encrypted message

$$c = m + k^{'} := c_1 c_2 \dots c_n, \quad \text{where} \quad c_i = m_i + k_i.$$

Then Alice destroys the first n numbers of the key.

The code book

In the past spies would be regularly caught with code books



It is absolutely crucial that the key represents random noise.

Another useful algebra

The set $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ can be made an algebra by redefining the addition

$$a + b := a + b \mod 26$$

and multiplication

$$ab := ab \mod 26.$$

Another useful algebra

The set $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ can be made an algebra by redefining the addition

$$a + b := a + b \mod 26$$

and multiplication

$$ab := ab \mod 26.$$

We can define the subtraction defining:

$$-0 := 0 \quad \text{and} \quad -a := 26 - a \quad \text{for } a \neq 0.$$

Another useful algebra

The set $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ can be made an algebra by redefining the addition

$$a + b := a + b \mod 26$$

and multiplication

$$ab := ab \mod 26.$$

We can define the subtraction defining:

$$-0 := 0 \quad \text{and} \quad -a := 26 - a \quad \text{for } a \neq 0.$$

This algebra has interesting properties which are fun to explore. A new phenomenon is divisors of zero:

$$2 \cdot 13 = 4 \cdot 13 = \ldots = 24 \cdot 13 = 0.$$

One-time pad 4

For written communication it was modified by giving the letters of the alphabet numerical encodings:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

The key is a secret book from the library. For example, "The Complete Poems of Emily Dickinson." Suppose that the first unused poem from the book is

Best Witchcraft is Geometry
To the magician's mind -
His ordinary acts are feats
To thinking of mankind.

Then you add this poem to your message $\mod 26$.

One-Time Pad 5

Suppose we need to send a message “BUY TELECOM SHARES”. We calculate

B	*U*	*Y*	*T*	*E*	*L*	*E*	*C*	*O*	*M*	*S*	*H*	*A*	*R*	*E*	*S*
1	20	24	19	4	11	4	2	14	12	18	7	0	17	4	18

and the first 16 letters from the poem will be

B	*E*	*S*	*T*	*W*	*I*	*T*	*C*	*H*	*C*	*R*	*A*	*F*	*T*	*I*	*S*
1	4	18	19	22	8	19	2	7	2	17	0	5	19	8	18

Adding these two messages $\mod 26$ we get

2	24	16	12	0	19	23	4	21	14	9	7	5	10	12	10
C	*Y*	*Q*	*M*	*A*	*T*	*X*	*E*	*V*	*O*	*J*	*H*	*F*	*K*	*M*	*K*

and send “CYQMATXEVOJHFKMK”.

Doing algebra in $\mathbb{Z}_{26}$

Division is possible only a number relatively prime with 26, e.g.,

$$3^{-1} = 9, \quad 5^{-1} = 21, \quad 7^{-1} = 15.$$

Doing algebra in $\mathbb{Z}_{26}$

Division is possible only a number relatively prime with 26, e.g.,

$$3^{-1} = 9, \quad 5^{-1} = 21, \quad 7^{-1} = 15.$$

Corresponding linear equations have unique solutions:

$$3x = 8 \quad \Longrightarrow \quad x = 3^{-1} \cdot 8 = 9 \cdot 8 = 20.$$

Doing algebra in $\mathbb{Z}_{26}$

Division is possible only a number relatively prime with 26, e.g.,

$$3^{-1} = 9, \quad 5^{-1} = 21, \quad 7^{-1} = 15.$$

Corresponding linear equations have unique solutions:

$$3x = 8 \quad \Longrightarrow \quad x = 3^{-1} \cdot 8 = 9 \cdot 8 = 20.$$

On the other hand, 2^{-1} does not exist and 2 is a divisor of zero.

$$2x = 3 \quad \Longrightarrow \quad \text{has no solution.}$$

and

$$2x = 4 \quad \Longrightarrow \quad \text{has solutions } x = 2 \text{ and } x = 15.$$

Doing algebra in $\mathbb{Z}_{26}$

Division is possible only a number relatively prime with 26, e.g.,

$$3^{-1} = 9, \quad 5^{-1} = 21, \quad 7^{-1} = 15.$$

Corresponding linear equations have unique solutions:

$$3x = 8 \quad \Longrightarrow \quad x = 3^{-1} \cdot 8 = 9 \cdot 8 = 20.$$

On the other hand, 2^{-1} does not exist and 2 is a divisor of zero.

$$2x = 3 \quad \Longrightarrow \quad \text{has no solution.}$$

and

$$2x = 4 \quad \Longrightarrow \quad \text{has solutions } x = 2 \text{ and } x = 15.$$

The set of invertible numbers is denoted $\mathbb{Z}_{26}^{*}$.

An affine cryptosystem

This is a substitution cypher which is also based on modular arithmetic. The key to this cryptosystem is a pair $k = (a, b)$ of numbers $a \in \mathbb{Z}_{26}^*$, $b \in \mathbb{Z}_{26}$.

Under this system a number in $\mathbb{Z}_{26}$ is assigned to every letter of the alphabet as before. Each letter is encoded into the corresponding number x and then into the letter which numerical encoding is $ax + b$.

For instance, if $a = 3$ and $b = 5$,

$$H \longrightarrow 7 \longrightarrow 3 \cdot 7 + 5 = 0 \longrightarrow A.$$

The message

BUY TELECOM SHARES

will be encrypted into

INZKRMRLVPHAFERH

Matrix algebra over $\mathbb{Z}_{26}$

Matrices can be added and multiplied as usual. Division is again slightly different, for example, the usual formula works

$$M^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{\det M} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

but $\det M$ must be invertible in $\mathbb{Z}_{26}$.

Let

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \quad \text{with} \quad \det K = 3 \cdot 5 - 3 \cdot 2 = 9.$$

Then

$$K^{-1} = 9^{-1} \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} = 3 \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}.$$

Hill's cryptosystem

The whole message is divided into such m-tuples and each m-tuple is encrypted separately. The key for this cryptosystem is an invertible $m \times m$ matrix over $\mathbb{Z}_{26}$.

We will consider the case $m = 2$ and therefore pairs of letters and 2×2 matrices. Let the key-matrix be

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

The encryption of a pair of letters (P_1, P_2) is carried out by

$$(P_1, P_2) \to \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \to K \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \to (C_1, C_2),$$

where x_1, x_2 are the numerical codes for P_1, P_2 and y_1, y_2 are the numerical codes for C_1, C_2.

Hill's cryptosystem. Example

Let

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}.$$

The matrix K is invertible, hence an inverse K^{-1} exists such that

$$KK^{-1} = K^{-1}K = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We know that

$$K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}.$$

It follows that

$$K^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = K^{-1}K \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},$$

which makes decryption is possible.

Hill's cryptosystem. Example 2

and the plaintext message be HELP. Then this plaintext is represented by two pairs

$$\text{HELP} \to \begin{bmatrix} H \\ E \end{bmatrix}, \begin{bmatrix} L \\ P \end{bmatrix} \to \begin{bmatrix} 7 \\ 4 \end{bmatrix}, \begin{bmatrix} 11 \\ 15 \end{bmatrix}.$$

Then we compute using K:

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix}, \qquad \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

and continue encryption as follows:

$$\begin{bmatrix} 7 \\ 8 \end{bmatrix}, \begin{bmatrix} 0 \\ 19 \end{bmatrix} \to \begin{bmatrix} H \\ I \end{bmatrix}, \begin{bmatrix} A \\ T \end{bmatrix} \to \text{HIAT}$$

Hill's cryptosystem. Example 3

Let us see how we can decrypt the cyphertext HIAT:

$$\text{HIAT} \to \begin{bmatrix} H \\ I \end{bmatrix}, \begin{bmatrix} A \\ T \end{bmatrix} \to \begin{bmatrix} 7 \\ 8 \end{bmatrix}, \begin{bmatrix} 0 \\ 19 \end{bmatrix}.$$

Then we compute using K^{-1}:

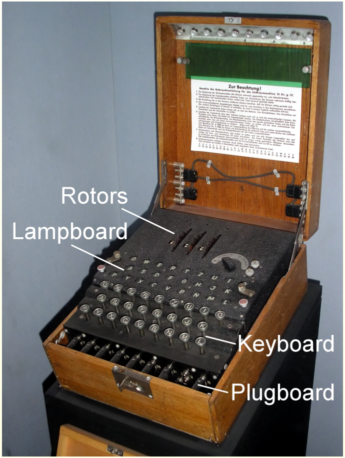
$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix}, \qquad \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$$

and continue decryption as follows:

$$\begin{bmatrix} 7 \\ 4 \end{bmatrix}, \begin{bmatrix} 11 \\ 15 \end{bmatrix} \to \begin{bmatrix} H \\ E \end{bmatrix}, \begin{bmatrix} L \\ P \end{bmatrix} \to \text{HELP}.$$

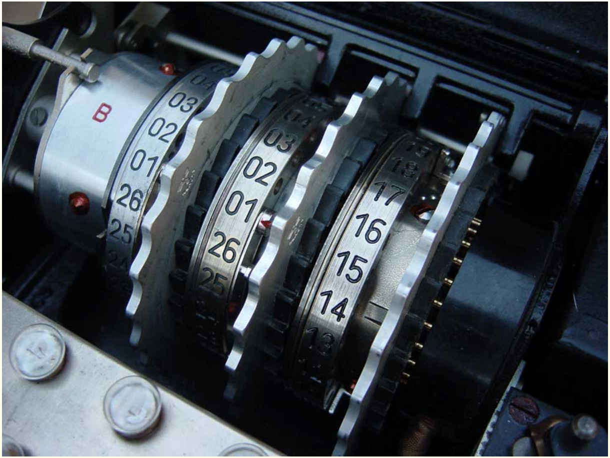
Enigma

An Enigma machine is an electro-mechanical rotor cipher machine perfected at the end of World War I.



Wheels of Enigma

The mechanical parts act in such a way as to form a varying electrical circuit.



Enigma

The cryptographic key was an Enigma machine's initial state which had several changeable aspects:

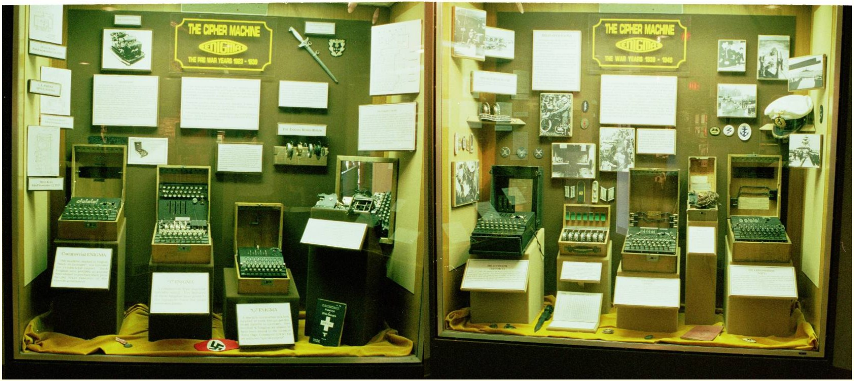
- Wheel order - the choice of rotors and the order in which they are fitted.
- Initial position of the rotors.
- Ring settings - the position of the alphabet ring relative to the rotor wiring.
- Plug connections - the connections of the plugs in the plugboard.

The military Enigma has 158,962,555,217,826,360,000 (158 quintillion) different settings.

In use, the Enigma required a list of daily key settings, normally transmitted by radio.

Enigmas

A selection of seven Enigma machines exhibited at the USA's National Cryptologic Museum.



From left to right, the models are: 1) Commercial Enigma; 2) Enigma T; 3) Enigma G; 4) Unidentified; 5) Luftwaffe (Air Force) Enigma; 6) Heer (Army) Enigma; 7) Kriegsmarine (Naval) Enigma.

Enigma. Breaking the code

The Polish Cipher Bureau first broke Germany's military Enigma ciphers in December 1932.

Marian Rejewski (on the photo), Jerzy Rozycki and Henryk Zygalski, the three mathematicians broke the code using the algebra of permutation groups.

From 1938 onwards, additional complexity was repeatedly added to the Enigma, making the initial decryption techniques unsuccessful.

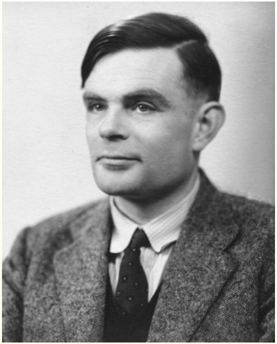
Enigma. Breaking the code 2

The Polish breakthrough was a basis for the later British effort.

During the war, British codebreakers were able to decrypt a vast number of messages enciphered by the Enigma in a secret project in Bletchley Park.

Alan Turing (1912 - 1954)

The team at Bletchly Park was led by Alan Turing.



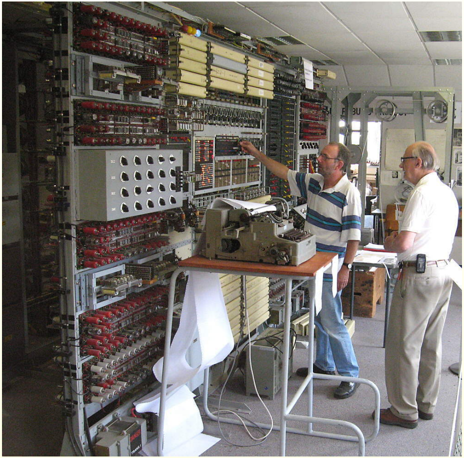
Turing formalised the concepts of "algorithm" and "computation" with the Turing machine. Widely considered to be the father of computer science and artificial intelligence.

Thomas "Tommy" Harold Flowers (1905 - 1998)

Was a British engineer working at Bletchly Park. Flowers designed Colossus, the world's first programmable electronic computer, to help solve encrypted German messages.

Colossus Rebuild

Colossus has been rebuild by enthusiasts and outperformed a modern (1994) computer.



The Role of Cryptographers in WW II

The exact influence of Ultra[1] on the course of the war is debated.

However Winston Churchill told the United Kingdom's King George VI after World War II: "It was thanks to Ultra that we won the war."

[1] this was the code for intelligence obtained from Bletchley Park.

Fun problem 1

1. Which one of the two functions

$$\begin{aligned} E_1(x) &= 13x + 15 \mod 26, \\ E_2(x) &= 15x + 13 \mod 26, \end{aligned}$$

   is suitable to be an encryption function in affine cryptosystem? Find the decryption function for it.

2. Using the encryption and decryption functions from (a) encrypt

   FRIGATE IS IN THE GULF

   and decrypt

   XBCLNIDAVONXXBAH.

Fun problem 2

Suppose Alice and Bob use the affine cryptosystem for private communications. Eve knows that Bob always concludes his letters to Alice with the abbreviation “XU”.

1. Show that she can then decrypt the following message that Bob sent to Alice

   NQRHSUNBZMJAYJ

2. Show how Eve, pretending to be Alice, can encode and send to Bob the message

   STUIPID

   to Bob.

Fun problem 3

Eve eavesdrops on the correspondence of Ark, Pip and Tom who use Hill's cryptosystem to communicate. She discovered that they split messages into segments which are three letters long and that the names (signatures)

ARK, PIP and TOM

are encoded as

GCB, APM and BWZ,

respectively. Find the matrix K which is used as the key.