MATH 233: ASSIGNMENT 2

DUE: FRIDAY, FEBRUARY 9, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2024

Problem 1 (2.8.14)**.** The ciphertext XVASDW was encrypted using an affine function $\alpha x + 1 \pmod{26}$. Determine α and decrypt the message. (**The plaintext should be meaningful**.)

Solution. The corresponding decryption function is $x \mapsto \alpha^*(x-1) \pmod{26}$, where α^* is the multiplicative inverse of α. If α is one of 12 elements in $\mathbb{Z}_{26}$, then α^* is also one of these elements. For each possible α^*, we decrypt the ciphertext as follows.

$\alpha^* \pmod{26}$	$\mathtt{X} = 23$	$\mathtt{V} = 21$	$\mathtt{A} = 0$	$\mathtt{S} = 18$	$\mathtt{D} = 3$	$\mathtt{W} = 22$
1	$\mathtt{w} = 22$	$\mathtt{u} = 20$	$\mathtt{z} = 25$	$\mathtt{r} = 17$	$\mathtt{c} = 2$	$\mathtt{v} = 21$
3	$\mathtt{o} = 14$	$\mathtt{i} = 8$	$\mathtt{x} = 23$	$\mathtt{z} = 25$	$\mathtt{g} = 6$	$\mathtt{l} = 11$
5	$\mathtt{g} = 6$	$\mathtt{w} = 22$	$\mathtt{v} = 21$	$\mathtt{h} = 7$	$\mathtt{k} = 10$	$\mathtt{b} = 1$
7	$\mathtt{y} = 24$	$\mathtt{k} = 10$	$\mathtt{t} = 19$	$\mathtt{p} = 15$	$\mathtt{o} = 14$	$\mathtt{r} = 17$
9	$\mathtt{q} = 16$	$\mathtt{y} = 24$	$\mathtt{r} = 17$	$\mathtt{x} = 23$	$\mathtt{s} = 18$	$\mathtt{h} = 7$
11	$\mathtt{i} = 8$	$\mathtt{m} = 12$	$\mathtt{p} = 15$	$\mathtt{f} = 5$	$\mathtt{w} = 22$	$\mathtt{x} = 23$
15	$\mathtt{s} = 18$	$\mathtt{o} = 14$	$\mathtt{l} = 11$	$\mathtt{v} = 21$	$\mathtt{e} = 4$	$\mathtt{d} = 3$
17	$\mathtt{k} = 10$	$\mathtt{c} = 2$	$\mathtt{j} = 9$	$\mathtt{d} = 3$	$\mathtt{i} = 8$	$\mathtt{t} = 19$
19	$\mathtt{c} = 2$	$\mathtt{q} = 16$	$\mathtt{h} = 7$	$\mathtt{l} = 11$	$\mathtt{m} = 12$	$\mathtt{j} = 9$
21	$\mathtt{u} = 20$	$\mathtt{e} = 4$	$\mathtt{f} = 5$	$\mathtt{t} = 19$	$\mathtt{q} = 16$	$\mathtt{z} = 25$
23	$\mathtt{m} = 12$	$\mathtt{s} = 18$	$\mathtt{d} = 3$	$\mathtt{b} = 1$	$\mathtt{u} = 20$	$\mathtt{p} = 15$
25	$\mathtt{e} = 4$	$\mathtt{g} = 6$	$\mathtt{b} = 1$	$\mathtt{j} = 9$	$\mathtt{y} = 24$	$\mathtt{f} = 5$

The only meaningful message solved occurs when $\alpha^* \equiv 15$ (corresponding to $\alpha \equiv 7$). □

Comment. If $\gcd(\alpha^*, 26) = 1$ and x is even, then $\alpha^*(x-1)$ is odd $\pmod{26}$, which cannot be a vowel. (See Problem 2(b).) This implies that D is likely to be decrypted to a vowel, otherwise there is no vowel in the last 4 letters. Furthermore, $\mathtt{D} = 3$ cannot be decrypted to $\mathtt{a} = 0$, so we can narrow down to 4 candidates of α^*.

Problem 2 (2.8.16, modified)**.** You are trying to encrypt using the affine function $13x + 22 \pmod{26}$.

(a) Encrypt hate and love. Why is decryption impossible?

(b) How many (not necessarily meaningful) three-letter words are encrypted to WWW?

Solution. (a) Both are encrypted to JWJW, so it is impossible to decrypt it.

(b) A letter is encrypted to W if and only if it is equivalent to an even element in $\mathbb{Z}_{26}$ (it is encrypted to J otherwise), or equivalently it is one of a,c,e,g,i,k,m,o,q,s,u,w,y. Therefore, there are 13^3 three-letter words which are encrypted to WWW.

□

Problem 3 (2.8.20)**.** Suppose you have a language with only the three letters a, b, c, and they occur with frequencies .9, .09, and .01, respectively. The ciphertext `BCCCBCBCBC` was encrypted by the Vegenère cipher (the shifts are now mod 3, not mod 26). Find the plaintext.

Solution. We first find the number of coincidences for each displacement:

displacement	1	2	3	4	5
coincidences	2	6	1	5	1

so we may assume that the key length is 2. Now the frequency vectors are

$$\mathbf{A}_0 = (.9, .09, .01), \quad \mathbf{A}_1 = (.01, .9, .09), \quad \mathbf{A}_2 = (.09, .01, .9),$$

and from the given ciphertext we have

$$\mathbf{W}_1 = (0, .8, .2), \quad \mathbf{W}_2 = (0, 0, 1).$$

Then

$$\mathbf{W}_1 \cdot \mathbf{A}_0 = .074, \quad \mathbf{W}_1 \cdot \mathbf{A}_1 = .738, \quad \mathbf{W}_1 \cdot \mathbf{A}_2 = .188$$

implies the first letter of the keyword is b, and

$$\mathbf{W}_2 \cdot \mathbf{A}_0 = .01, \quad \mathbf{W}_1 \cdot \mathbf{A}_1 = .09, \quad \mathbf{W}_1 \cdot \mathbf{A}_2 = .9$$

implies that the second letter is c. Therefore, the keyword is *bc* and the plaintext is

`aabaaaaaaa`.

□

Comment. It may seem to be possible that the key length is 4, but the resulting keyword is *bcbc* in this case.

Problem 4 (2.8.28)**.** The ciphertext

`BP EG FC AI MA MG PO KB HU`

was encrypted using the Playfair cipher with keyword *archimedes*. (Spaces were inserted for convenience, so you may ignore them.) Find the plaintext.

Solution. From the matrix

$$\begin{bmatrix} a & r & c & h & i \\ m & e & d & s & b \\ f & g & k & l & n \\ o & p & q & t & u \\ v & w & x & y & z \end{bmatrix},$$

we can retrieve the plaintext

`eu re ka ih av ef ou nd it` → `Eureka, I have found it!`

□

Problem 5. You intercepted the following three ciphertexts

FAGGXFVFGVAVAFGGXXDXVGXA

FAGGXFVAGVAVAFGAXXDXVGVF

FAGGXFAAGVAVAFFVXXDXVGAV

which were encrypted using the ADFGVX cipher with the following 6×6 matrix.

$$\begin{array}{c|cccccc} & A & D & F & G & V & X \\ \hline A & p & g & 5 & c & 3 & e \\ D & n & b & q & j & o & z \\ F & 2 & r & 8 & s & l & a \\ G & 0 & f & t & m & 1 & d \\ V & 6 & v & i & w & 9 & k \\ X & u & y & x & 4 & h & 7 \end{array}$$

You do not know the keyword, but you know that it is one of the following words.

ton, end, map, very, beat, done, light, build, model

It is likely that the plaintexts are meaningful sentences and they are identical except for the last few letters. Find the correct keyword and the plaintext corresponding to the first ciphertext.

Solution. Observe the identical parts of the ciphertexts as follows:

FAGGXFVFGVAVAFGGXXDXVGXA

FAGGXFVAGVAVAFGAXXDXVGVF

FAGGXFAAGVAVAFFVXXDXVGAV

We can guess that the length of the keyword is 3. For each of the given keywords with length 3, we may try to decrypt the beginning of the ciphertexts.

(i) Keyword: *ton*

$$\begin{array}{ccc} n & o & t \\ \hline \mathtt{F} & \mathtt{G} & \mathtt{X} \\ \mathtt{A} & \mathtt{V} & \mathtt{X} \\ \vdots & \vdots & \vdots \end{array} \quad \Rightarrow \quad \begin{array}{ccc} t & o & n \\ \hline \mathtt{X} & \mathtt{G} & \mathtt{F} \\ \mathtt{X} & \mathtt{V} & \mathtt{A} \\ \vdots & \vdots & \vdots \end{array} \quad \Rightarrow \quad \mathtt{XG\ FX\ VA}\ldots \quad \Rightarrow \quad \mathtt{4a6}\ldots$$

(ii) Keyword: *end*

$$\begin{array}{ccc} d & e & n \\ \hline \mathtt{F} & \mathtt{G} & \mathtt{X} \\ \mathtt{A} & \mathtt{V} & \mathtt{X} \\ \vdots & \vdots & \vdots \end{array} \quad \Rightarrow \quad \begin{array}{ccc} e & n & d \\ \hline \mathtt{G} & \mathtt{X} & \mathtt{F} \\ \mathtt{V} & \mathtt{X} & \mathtt{A} \\ \vdots & \vdots & \vdots \end{array} \quad \Rightarrow \quad \mathtt{GX\ FV\ XA}\ldots \quad \Rightarrow \quad \mathtt{dlu}\ldots$$

(iii) Keyword: *map*

$$\begin{array}{ccc} a & m & p \\ \hline \mathtt{F} & \mathtt{G} & \mathtt{X} \\ \mathtt{A} & \mathtt{V} & \mathtt{X} \\ \vdots & \vdots & \vdots \end{array} \quad \Rightarrow \quad \begin{array}{ccc} e & n & d \\ \hline \mathtt{G} & \mathtt{F} & \mathtt{X} \\ \mathtt{V} & \mathtt{A} & \mathtt{X} \\ \vdots & \vdots & \vdots \end{array} \quad \Rightarrow \quad \texttt{GF XV AX}\ldots \quad \Rightarrow \quad \texttt{the}\ldots$$

Therefore, *map* is the most promising candidate for the keyword. We may continue with the first ciphertext to get the plaintext as follows.

$$\begin{array}{ccc} a & m & p \\ \hline \mathtt{F} & \mathtt{G} & \mathtt{X} \\ \mathtt{A} & \mathtt{V} & \mathtt{X} \\ \mathtt{G} & \mathtt{A} & \mathtt{D} \\ \mathtt{G} & \mathtt{V} & \mathtt{X} \\ \mathtt{X} & \mathtt{A} & \mathtt{V} \\ \mathtt{F} & \mathtt{F} & \mathtt{G} \\ \mathtt{V} & \mathtt{G} & \mathtt{X} \\ \mathtt{F} & \mathtt{G} & \mathtt{A} \end{array} \quad \Rightarrow \quad \begin{array}{ccc} e & n & d \\ \hline \mathtt{G} & \mathtt{F} & \mathtt{X} \\ \mathtt{V} & \mathtt{A} & \mathtt{X} \\ \mathtt{A} & \mathtt{G} & \mathtt{D} \\ \mathtt{V} & \mathtt{G} & \mathtt{X} \\ \mathtt{A} & \mathtt{X} & \mathtt{V} \\ \mathtt{F} & \mathtt{F} & \mathtt{G} \\ \mathtt{G} & \mathtt{V} & \mathtt{X} \\ \mathtt{G} & \mathtt{F} & \mathtt{A} \end{array}$$

$$\Rightarrow \quad \texttt{GF XV AX AG DV GX AX VF FG GV XG FA}$$

$$\Rightarrow \quad \texttt{thecodeis142}$$

$$\Rightarrow \quad \texttt{The code is 142.}$$

□

Comment. The other two ciphertexts correspond to

`The code is 165` and `The code is 233`,

respectively.