Cryptography Homework 1

Michael Nelson

1 Problem 1

Exercise 1. Encrypt your first and last name using the following methods. Show your work:

1. Vigenere Cipher with key TIGER.
2. Permutation Cipher with permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Solution 1. 1. The key TIGER corresponds to $K := (19, 8, 6, 4, 17)$ and the plaintext MICHAELNELSON corresponds to $\boldsymbol{x} := (12, 8, 2, 7, 0, 4, 11, 13, 4, 11, 18, 14, 13)$. Therefore set $\boldsymbol{k} = (19, 8, 6, 4, 17, 19, 8, 6, 4, 17, 19, 8, 6)$ (in order to make the keyword the same length as the plaintext) and we set

$$\begin{aligned} \boldsymbol{y} &:= \mathrm{e}_K(\boldsymbol{x}) \\ &= \boldsymbol{x} + \boldsymbol{k} \mod 26 \\ &\equiv (5, 16, 8, 11, 17, 23, 19, 19, 8, 2, 11, 22, 19) \mod 26. \end{aligned}$$

In particular, $\boldsymbol{y}$ corresponds to the ciphertext FQILRXTTICLWT.

2. Note that the key $K = (1243)$ can only permute four letters at a time whereas the plaintext MICHAELNELSON has length 13. Thus in order to encrypt this plaintext, we first need to break the plaintext MICHAELNELSON into groups of four (plus some remainder):

MICHAELNELSON = MICH AELN ELSO N,

then we use the key to encrypt MICH, AELN, and ELSO (we leave the last N alone). Equivalently, if we set $\pi = (1\ 2\ 4\ 3\ 5\ 6\ 8\ 7\ 9\ 10\ 12\ 11)$, then we have

$$\begin{aligned} \boldsymbol{y} &:= \mathrm{e}_K(\boldsymbol{x}) \\ &= (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(12)}, x_{13}) \\ &= (2, 12, 7, 8, 11, 0, 13, 4, 18, 4, 14, 11, 13). \end{aligned}$$

In particular, $\boldsymbol{y}$ corresponds to the ciphertext CMHILANESEOLN.

2 Problem 2

Exercise 2. Decryption.

1. The ciphertext (R, P) was encrypted using a Hill Cipher with key
$$K = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}.$$
   (a) What matrix should be used for decryption?
   (b) What was the original message?

2. The message

"CTGT BXP HGT QTNGBAMFUZ H RTJJHZT BHB BXP"

was encrypted using an affine cipher with the plaintext found in part 1.b above as the key.

(a) What function should be used for decryption?

Solution 2. 1. To decrypt the cipher text (R,P), we use the inverse of K which is given by

$$K^{-1} = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}.$$

Setting $\boldsymbol{y} = (\mathrm{R},\mathrm{P}) = (17,15)$, we see that the original message is given by

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{y}K^{-1} \\ &= (17,15)\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} \\ &= (17,15)\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} \\ &\equiv (3,7) \mod 26, \end{aligned}$$

where the calculation is performed mod 26. In particular, $\boldsymbol{x}$ corresponds to the plaintext (D,G).

2. The plaintext (D,G) corresponds to the affine cipher key $K = (3,7)$. Thus the affine cipher encryption function corresponding to K is given by $\mathrm{e}_K(x) = 3x + 7$. Observe that this encryption function can be be represented in the following matrix form:

$$\widetilde{K}\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 3x+7 \\ 1 \end{pmatrix} = \begin{pmatrix} \mathrm{e}_K(x) \\ 1 \end{pmatrix},$$

where we set $\widetilde{K} = \left(\begin{smallmatrix} 3 & 7 \\ 0 & 1 \end{smallmatrix}\right)$. Thus to find the affine cipher decryption function corresponding to K, it suffices to find the matrix inverse of $\widetilde{K}$ modulo 26. This is given by

$$\begin{aligned} \widetilde{K}^{-1} &= \frac{1}{3}\begin{pmatrix} 1 & -7 \\ 0 & 3 \end{pmatrix} \mod 26 \\ &\equiv \begin{pmatrix} 1/3 & -7/3 \\ 0 & 1 \end{pmatrix} \mod 26 \\ &\equiv \begin{pmatrix} 9 & 15 \\ 0 & 1 \end{pmatrix} \mod 26. \end{aligned}$$

Thus the decryption function is given by $\mathrm{d}_K(y) = 9y + 15$. Using an online affine cipher decoder, we find that original plaintext message is

"HERE YOU ARE DECRYPTING A MESSAGE YAY YOU"

3 Problem 3

Exercise 3. Suppose that $K = (5,21)$ is a key in an Affine Cipher over $\mathbb{Z}_{29}$.

1. Express the decryption function $\mathrm{d}_K(y)$ in the form $\mathrm{d}_K(y) = a'y + b'$ where $a', b' \in \mathbb{Z}_{29}$.
2. Prove that $\mathrm{d}_K(\mathrm{e}_K(x)) = x$ for all $x \in \mathbb{Z}_{29}$.

Solution 3. 1. To find the decryption function d_K, we just need to find the inverse to the matrix $\widetilde{K} = \left(\begin{smallmatrix} 5 & 21 \\ 0 & 1 \end{smallmatrix}\right)$ modulo 26: this is given by

$$\begin{aligned} \widetilde{K}^{-1} &= \frac{1}{5}\begin{pmatrix} 1 & -21 \\ 0 & 5 \end{pmatrix} \mod 26 \\ &\equiv \begin{pmatrix} 1/5 & 1 \\ 0 & 1 \end{pmatrix} \mod 26 \\ &\equiv \begin{pmatrix} 21 & 1 \\ 0 & 1 \end{pmatrix} \mod 26. \end{aligned}$$

Therefore we have $\mathrm{d}_K(y) = 21y + 1$.

2. For any $x \in \mathbb{Z}_{29}$, we have

$$\begin{aligned}\begin{pmatrix}\mathrm{d}_K(\mathrm{e}_K(x))\\1\end{pmatrix} &= \widetilde{K}^{-1}\begin{pmatrix}\mathrm{e}_K(x)\\1\end{pmatrix}\\ &= \widetilde{K}^{-1}\left(\widetilde{K}\begin{pmatrix}x\\1\end{pmatrix}\right)\\ &= (\widetilde{K}^{-1}\widetilde{K})\begin{pmatrix}x\\1\end{pmatrix}\\ &= \begin{pmatrix}x\\1\end{pmatrix}.\end{aligned}$$

It follows that $\mathrm{d}_K(\mathrm{e}_K(x)) = x$.

4 Problem 4

Exercise 4. Let p be a prime and let $n \geq 2$ an integer.

1. Prove that the number of 2×2 matrices that are invertible over $\mathbb{F}_p$ is $(p^2-1)(p^2-p)$.
2. Find a formula for the number of $n \times n$ matrices that are invertible over $\mathbb{F}_p$.

Solution 4. We will prove that the size of $\mathrm{GL}_n(\mathbb{F}_p)$ is given by

$$\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=0}^{n-1}(p^n - p^j).$$

This will solve both problems 1 and 2 (where problem 1 is the special case $n = 2$). Let A be a random matrix in $\mathrm{GL}_n(\mathbb{F}_p)$ and let $v_1, \ldots, v_n$ denote the column vectors of A. Note that counting the number of matrices A in $\mathrm{GL}_n(\mathbb{F}_p)$ is equivalent to counting the number of ordered tuples of linearly independent vectors $(v_1, \ldots, v_n)$. So it suffices to count the latter.

There are $p^n - 1$ different possible vectors in $\mathbb{F}_p^n$ for which v_1 can be. The only vector which is not allowed is the zero vector. This is because the vectors $(v_1, \ldots, v_n)$ must be linearly independent, so no zero vectors allowed. Now we fix v_1. Then there are $p^n - p$ different possible vectors in $\mathbb{F}_p^n$ for which v_2 can be. Indeed, v_1 and v_2 must be linearly independent, so v_2 cannot equal to any vectors of the form av_1 where $a \in \mathbb{F}_p$. If we had fixed v_1 to be a different vector, then the same counting argument would apply, so altogether, the number of pairs of linearly independent vectors (v_1, v_2) is $(p^n - 1)(p^n - p)$.

More generally, for $1 \leq j \leq n$, if the vectors $v_1, \ldots, v_{j-1}$ are fixed, then there are $p^n - p^{j-1}$ different possible vectors in $\mathbb{F}_p^n$ for which v_j can be. Again, varying the vectors $v_1, \ldots, v_{j-1}$ to a new set of fixed vectors results in the same counting argument, so altogether the number of j-tuples of linearly independent vectors $(v_1, v_2, \ldots, v_j)$ is $(p^n - 1)(p^n - p)\cdots(p^n - p^{j-1})$. In particular, taking $j = n$ gives us

$$\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=1}^{n}(p^n - p^{j-1}) = \prod_{j=0}^{n-1}(p^n - p^j).$$