Chapter 2

Classical Cryptography

2.1 Evaluate the following:

(a) 7503 mod 81.

Answer: $7503 \bmod 81 = 51$.

(b) $(-7503) \bmod 81$.

Answer: $(-7503) \bmod 81 = 45$.

(c) 81 mod 7503.

Answer: $81 \bmod 7503 = 81$.

(d) $(-81) \bmod 7503$.

Answer: $(-81) \bmod 7503 = 7422$.

2.2 Suppose that $a, m > 0$, and $a \not\equiv 0 \pmod{m}$. Prove that

$$(-a) \bmod m = m - (a \bmod m).$$

Answer: We have $a = qm + r$, where $1 \leq r \leq m-1$ and $r = a \bmod m$. Then $-a = -(q+1)m + (m-r)$, where $1 \leq m - r \leq m - 1$. Therefore $(-a) \bmod m = m - r = m - (a \bmod m)$.

2.3 Prove that $a \bmod m = b \bmod m$ if and only if $a \equiv b \pmod{m}$.

Answer: $a \bmod m = b \bmod m$ implies that $a = q_1 m + r$ and $b = q_2 m + r$, where $0 \leq r \leq m-1$. Then $a - b = (q_1 - q_2)m$, so $a \equiv b \pmod{m}$. Conversely, suppose $a \equiv b \pmod{m}$. Then $a - b = qm$. Let $r = a \bmod m$. Then $a = q_1 m + r$ for some q_1, and hence $b = a - qm = (q_1 - q)m + r$, so $b \bmod m = r$.

2.4 Prove that $a \bmod m = a - \lfloor \frac{a}{m} \rfloor m$, where $\lfloor x \rfloor = \max\{y \in \mathbb{Z} : y \leq x\}$.

Answer: $(a - m + 1)/m \leq \lfloor \frac{a}{m} \rfloor \leq a/m$, so $a - m + 1 \leq m\lfloor \frac{a}{m} \rfloor \leq a$, and hence $0 \leq a - \lfloor \frac{a}{m} \rfloor m \leq m - 1$.

2.5 Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a *Shift Cipher*:

`BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.`

Answer: The key is 16, and the plaintext is the following:

Look, up in the air, it's a bird, it's a plane, it's Superman!

2.6 If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an ***involutory key***. Find all the involutory keys in the *Shift Cipher* over $\mathbb{Z}_{26}$.

Answer: The involutory keys are 0 and 13.

2.7 Determine the number of keys in an *Affine Cipher* over $\mathbb{Z}_m$ for $m = 30, 100$ and 1225.

Answer: $30 = 2 \times 3 \times 5$, so $\phi(30) = 1 \times 2 \times 4 = 8$. The affine cipher over $\mathbb{Z}_{30}$ has $30 \times 8 = 240$ keys.
$100 = 2^2 \times 5^2$, so $\phi(100) = (2^2 - 2)(5^2 - 5) = 40$. The affine cipher over $\mathbb{Z}_{100}$ has $100 \times 40 = 4000$ keys.
$1225 = 5^2 \times 7^2$, so $\phi(1225) = (5^2 - 5)(7^2 - 7) = 840$. The affine cipher over $\mathbb{Z}_{1225}$ has $1225 \times 840 = 1029000$ keys.

2.8 List all the invertible elements in $\mathbb{Z}_m$ for $m = 28, 33$, and 35.

Answer: The invertible elements in $\mathbb{Z}_{28}$ are 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25 and 27.
The invertible elements in $\mathbb{Z}_{33}$ are 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31 and 32.
The invertible elements in $\mathbb{Z}_{35}$ are 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33 and 34.

2.9 For $1 \leq a \leq 28$, determine $a^{-1} \bmod 29$ by trial and error.

Answer: $1^{-1} = 28$, $2^{-1} = 15$, $3^{-1} = 10$, $4^{-1} = 22$, $5^{-1} = 6$, $6^{-1} = 5$, $7^{-1} = 25$, $8^{-1} = 11$, $9^{-1} = 13$, $10^{-1} = 3$, $11^{-1} = 8$, $12^{-1} = 17$, $13^{-1} = 9$, $14^{-1} = 27$, $15^{-1} = 2$, $16^{-1} = 20$, $17^{-1} = 12$, $18^{-1} = 21$, $19^{-1} = 26$, $20^{-1} = 16$, $21^{-1} = 18$, $22^{-1} = 4$, $23^{-1} = 24$, $24^{-1} = 23$, $25^{-1} = 7$, $26^{-1} = 19$, $27^{-1} = 14$ and $28^{-1} = 28$.

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

(a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a'y + b'$, where $a', b' \in \mathbb{Z}_{29}$.

Answer: $d_K(y) = 6y + 19$.

(b) Prove that $d_K(e_K(x)) = x$ for all $x \in \mathbb{Z}_{29}$.

Answer: $6(5x + 21) + 19 \equiv 30x + 145 \equiv x \pmod{29}$.

2.11 (a) Suppose that $K = (a, b)$ is a key in an *Affine Cipher* over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a + 1) \equiv 0 \pmod{n}$.

Answer: $K = (a, b)$ is an involutory key if and only if $a(ax + b) + b \equiv x \pmod{n}$ for all $x \in \mathbb{Z}_n$. Clearly $a(ax + b) + b \equiv a^2x + b(a + 1) \pmod{n}$, so we require that $a^2 \equiv 1 \pmod{n}$ and $b(a + 1) \equiv 0 \pmod{n}$.

(b) Determine all the involutory keys in the *Affine Cipher* over $\mathbb{Z}_{15}$.

Answer: $a^2 \equiv 1 \pmod{15}$ if and only if $a = 1, 4, 11$ or 14. If $a = 1$, then $b = 0$. If $a = 4$, then $b = 0, 3, 6, 9$ or 12. If $a = 11$, then $b = 0, 5$ or 10. Finally, if $a = 14$, then b can be any element of $\mathbb{Z}_{15}$.

(c) Suppose that $n = pq$, where p and q are distinct odd primes. Prove that the number of involutory keys in the *Affine Cipher* over $\mathbb{Z}_n$ is $n + p + q + 1$.

Answer: There are four possible values for a, namely, $a = 1$; $a = -1 \bmod n$; the solution to the system $a \equiv 1 \pmod{p}$, $a \equiv -1 \pmod{q}$; and the solution to the system $a \equiv -1 \pmod{p}$, $a \equiv 1 \pmod{q}$. If $a = 1$, then $b = 0$. If $a = -1$, then b can be any element in $\mathbb{Z}_n$. In the third case, we require that $b \equiv 0 \pmod{q}$, so there are p possible values for b. In the fourth case, we require that $b \equiv 0 \pmod{p}$, so there are q possible values for b. The total number of involutory keys is therefore $n + p + q + 1$.

2.12 (a) Let p be prime. Prove that the number of 2×2 matrices that are invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$.

HINT Since p is prime, $\mathbb{Z}_p$ is a field. Use the fact that a matrix over a field is invertible if and only if its rows are linearly independent vectors (i.e., there does not exist a non-zero linear combination of the rows whose sum is the vector of all 0's).

Answer: The first row can be any non-zero vector, so there are $p^2 - 1$ possibilities. Given the first row, say r, the second row can be any vector that is not a scalar multiple of r. Therefore there are $p^2 - p$ possibilities for the second row, given the first row. Hence, the total number of 2×2 invertible matrices is $(p^2 - 1)(p^2 - p)$.

(b) For p prime and $m \geq 2$ an integer, find a formula for the number of $m \times m$ matrices that are invertible over $\mathbb{Z}_p$.

Answer: The number of invertible matrices is

$$(p^m - 1)(p^m - p)(p^m - p^2) \cdots (p^m - p^{m-1}).$$

2.13 For $n = 6, 9$, and 26, how many 2×2 matrices are there that are invertible over $\mathbb{Z}_n$?

Answer: For $n = 6$, there are $(2^2 - 1)(2^2 - 2)(3^2 - 1)(3^2 - 3) = 1728$ invertible matrices (use the Chinese remainder theorem and Exercise 2.12). Similarly, for $n = 26$, there are $(2^2 - 1)(2^2 - 2)(13^2 - 1)(13^2 - 13) = 157248$ invertible matrices. For $n = 9$, there are $3^4(3^2 - 1)(3^2 - 3) = 3888$ invertible matrices.

2.14 (a) Prove that $\det A \equiv \pm 1 \pmod{26}$ if A is a matrix over $\mathbb{Z}_{26}$ such that $A = A^{-1}$.

Answer: If $A = A^{-1}$, then $A^2 = I$ and hence $(\det A)^2 \equiv 1 \pmod{26}$. This implies that $\det A \equiv \pm 1 \pmod{26}$.

(b) Use the formula given in Corollary 2.4 to determine the number of involutory keys in the *Hill Cipher* (over $\mathbb{Z}_{26}$) in the case $m = 2$.

Answer: If $\det A \equiv 1 \pmod{26}$ then there are 8 involutory matrices, and if $\det A \equiv -1 \pmod{26}$ then there are 728 involutory matrices, for a total of 736 involutory matrices.

The eight involutory matrices with determinant 1 are as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 25 & 0 \\ 0 & 25 \end{pmatrix}, \quad \begin{pmatrix} 1 & 13 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 25 & 13 \\ 0 & 25 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ 13 & 1 \end{pmatrix}, \quad \begin{pmatrix} 25 & 0 \\ 13 & 25 \end{pmatrix}, \quad \begin{pmatrix} 12 & 13 \\ 13 & 12 \end{pmatrix}, \quad \begin{pmatrix} 14 & 13 \\ 13 & 14 \end{pmatrix}.$$

The involutory matrices with determinant -1 have the following forms when reduced modulo 2:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

When reduced modulo 13, an involutory matrix with determinant -1 has the following form:

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix},$$

where $x^2 + yz \equiv 1 \pmod{13}$. The number of triples $(x, y, z) \in (\mathbb{Z}_{13})^3$ that satisfy this congruence is easily computed: if $x = 2$ or 12, then there are 25 ordered pairs (y, z); and if $x \neq 2, 12$, then there are 12 ordered pairs (y, z). Hence, the total number of triples is $2 \times 25 + 11 \times 12 = 182$. Now we can use the Chinese remainder theorem to combine any solution modulo 2 with any solution modulo 13, so the total number of solutions modulo 26 is $4 \times 182 = 728$, as stated above.

2.15 Determine the inverses of the following matrices over $\mathbb{Z}_{26}$:

(a) $\begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}$

Answer: The inverse matrix is

$$\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}.$$

(b) $\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$

Answer: The inverse matrix is

$$\begin{pmatrix} 25 & 11 & 22 \\ 10 & 13 & 4 \\ 17 & 24 & 1 \end{pmatrix}.$$

2.16 (a) Suppose that π is the following permutation of $\{1,\ldots,8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}.

Answer: The permutation π^{-1} is as follows:

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

(b) Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.

Answer: The plaintext is the following:

Gentlemen do not read each other's mail.

2.17 (a) Prove that a permutation π in the *Permutation Cipher* is an involutory key if and only if $\pi(i) = j$ implies $\pi(j) = i$, for all $i, j \in \{1,\ldots,m\}$.

Answer: A permutation π is involutory if and only if $\pi(\pi(i)) = i$ for all i. Denoting $\pi(i) = j$, it must be the case that $\pi(j) = i$.

(b) Determine the number of involutory keys in the *Permutation Cipher* for $m = 2, 3, 4, 5$, and 6.

Answer: An involutory permutation must consist of fixed points and cycles of length two.
For $m = 2$, there are 2 involutory permutations.
For $m = 3$, there are 4 involutory permutations.
For $m = 4$, there are 3 permutations consisting of two cycles of length 2; 6 permutations having one cycle of length 2 and two fixed points; and 1 permutation consisting of 4 fixed points. The total number of involutory permutations is 10.
For $m = 5$, there are 15 permutations consisting of two cycles of length 2 and one fixed point; 10 permutations having one cycle of length 2 and three fixed points; and 1 permutation consisting of 5 fixed points. The total number of involutory permutations is 26.
For $m = 6$, there are 15 permutations consisting of three cycles of length 2; 45 permutations consisting of two cycles of length 2 and two fixed points; 15 permutations having one cycle of length 2 and four fixed points; and 1 permutation consisting of 5 fixed points. The total number of involutory permutations is 76.

2.18 Consider the following linear recurrence over $\mathbb{Z}_2$ of degree four:

$$z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2,$$

$i \geq 0$. For each of the 16 possible initialization vectors $(z_0, z_1, z_2, z_3) \in (\mathbb{Z}_2)^4$, determine the period of the resulting keystream.

Answer: $(0, 0, 0, 0)$ produces a keystream with period 1, and all other initialization vectors produce a keystream with period 5.

2.19 Redo the preceding question, using the recurrence

$$z_{i+4} = (z_i + z_{i+3}) \bmod 2,$$

$i \geq 0$.

Answer: $(0, 0, 0, 0)$ produces a keystream with period 1, and all other initialization vectors produce a keystream with period 15.

2.20 Suppose we construct a keystream in a synchronous stream cipher using the following method. Let $K \in \mathcal{K}$ be the key, let $\mathcal{L}$ be the keystream alphabet, and let Σ be a finite set of states. First, an initial state $\sigma_0 \in \Sigma$ is determined from K by some method. For all $i \geq 1$, the state σ_i is computed from the previous state σ_{i-1} according to the following rule:

$$\sigma_i = f(\sigma_{i-1}, K),$$

where $f : \Sigma \times \mathcal{K} \rightarrow \Sigma$. Also, for all $i \geq 1$, the keystream element z_i is computed using the following rule:

$$z_i = g(\sigma_i, K),$$

where $g : \Sigma \times \mathcal{K} \rightarrow \mathcal{L}$. Prove that any keystream produced by this method has period at most $|\Sigma|$.

Answer: For a fixed key K, each σ_i can be regarded as a function of σ_{i-1}. Define

$$t = \min\{i \geq 1 : \sigma_i \in \{\sigma_0, \ldots, \sigma_{i-1}\}\}.$$

It follows from the pigeon-hole principle that $t \leq |\Sigma|$, because $\sigma_i \in \Sigma$ for all $i \geq 0$. Suppose that $\sigma_t = \sigma_s$, where $0 \leq s < t$. Then it $\sigma_{i+t-s} = \sigma_i$ for all $i \geq s$. Hence, $z_{i+t-s} = z_i$ for all $i \geq s$, and the keystream has period $t - s \leq |\Sigma|$.

2.21 Below are given four examples of ciphertext, one obtained from a *Substitution Cipher*, one from a *Vigenère Cipher*, one from an *Affine Cipher*, and one unspecified. In each case, the task is to determine the plaintext.

Give a clearly written description of the steps you followed to decrypt each ciphertext. This should include all statistical analysis and computations you performed.

The first two plaintexts were taken from *The Diary of Samuel Marchbanks*, by Robertson Davies, Clarke Irwin, 1947; the fourth was taken from *Lake Wobegon Days*, by Garrison Keillor, Viking Penguin, Inc., 1985.

(a) *Substitution Cipher*:

```
EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
```

HINT F decrypts to w.

Answer: The plaintext is as follows:

> I may not be able to grow flowers, but my garden produces just as many dead leaves, old overshoes, pieces of rope, and bushels of dead grass as anybody's, and today I bought a wheelbarrow to help in clearing it up. I have always loved and respected the wheelbarrow. It is the one wheeled vehicle of which I am perfect master.

(b) *Vigenère Cipher*:

```
KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNPIST
```

Answer: The keyword is *CRYPTO*, and the plaintext is as follows:

> I learned how to calculate the amount of paper needed for a room when I was at school. You multiply the square footage of the walls by the cubic contents of the floor and ceiling combined, and double it. You then allow half the total for openings such as windows and doors. Then you allow the other half for matching the pattern. Then you double the whole thing again to give a margin of error, and then you order the paper.

(c) *Affine Cipher*:

```
KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP
KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKP
BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF
ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK
IVKSCPICBRKIJPKABI
```

Answer: The key is $(19, 4)$. The plaintext consists of the French lyrics to "O Canada":

Ô Canada!
Terre de nos aïeux.
Ton front est ceint,
De fleurons glorieux.
Car ton bras
Sait porter l'épée,
Il sait porter la croix.
Ton histoire est une épopée,
des plus brillants exploits.
Et ta valeur,
de foi trempée,
protègera nos foyers et nos droits.

(d) unspecified cipher:

```
BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVT
DVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXM
MASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ
OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC
GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLR
FFJELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWM
NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUM
ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUU
HYHGGCKTMBLRX
```

Answer: This is a *Vigenère Cipher*. The keyword is *THEORY*, and the plaintext is as follows:

> I grew up among slow talkers, men in particular, who dropped words a few at a time like beans in a hill, and when I got to Minneapolis where people took a Lake Wobegon comma to mean the end of a story, I couldn't speak a whole sentence in company and was considered not too bright. So I enrolled in a speech course taught by Orville Sand, the founder of reflexive relaxology, a self-hypnotic technique that enabled a person to speak up to three hundred words per minute.

2.22 (a) Suppose that $p_1, \ldots, p_n$ and $q_1, \ldots, q_n$ are both probability distributions, and $p_1 \geq \cdots \geq p_n$. Let $q'_1, \ldots, q'_n$ be any permutation of $q_1, \ldots, q_n$. Prove that the quantity

$$\sum_{i=1}^{n} p_i q'_i$$

is maximized when $q'_1 \geq \cdots \geq q'_n$.

Answer: Suppose that $q'_j < q'_k$ for some $j < k$. Define

$$q''_i = \begin{cases} q'_i & \text{if } i \notin \{j,k\} \\ q'_k & \text{if } i = j \\ q'_j & \text{if } i = k. \end{cases}$$

Then we have

$$\sum_{i=1}^{n} p_i q''_i - \sum_{i=1}^{n} p_i q'_i = (p_j - p_k)(q'_k - q'_j) \geq 0.$$

Therefore the desired sum is not decreased when q'_j and q'_k are exchanged. By a sequence of exchanges of this type, we see that the sum attains its maximum possible value when $q'_1 \geq \cdots \geq q'_n$.

(b) Explain why the expression in Equation (2.1) is likely to be maximized when $g = k_i$.

Answer: (Note: this equation is on page 47.) Suppose that π is a permutation of $\{0,\ldots,25\}$ such that $p_{\pi(0)} \geq \cdots \geq p_{\pi(25)}$. Then it is "likely" that $f_{\pi(0)} \geq \cdots \geq f_{\pi(25)}$. Assuming that this is the case, we proceed. When $g = 0$, the following equation holds:

$$\sum_{i=0}^{25} \frac{p_i f_i}{n'} = \sum_{i=0}^{25} \frac{p_{\pi(i)} f_{\pi(i)}}{n'}.$$

By the result proven in part (a), this sum is at least as great as any sum

$$\sum_{i=0}^{25} \frac{p_i f_{i+g}}{n'},$$

where $g \neq 0$.

2.23 Suppose we are told that the plaintext

`breathtaking`

yields the ciphertext

`RUPOTENTOIFV`

where the *Hill Cipher* is used (but m is not specified). Determine the encryption matrix.

Answer: Using the first 9 plaintext and ciphertext characters, we compute

$$K = \begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix}^{-1} \begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix} = \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix}.$$