APPENDIX E
BASIC CONCEPTS FROM LINEAR ALGEBRA

William Stallings

Supplement to
Cryptography and Network Security, Fifth Edition
William Stallings
Prentice Hall 2010
ISBN-10: 0136097049
http://williamstallings.com/Crypto/Crypto5e.html

E.1 OPERATIONS ON VECTORS AND MATRICES

We use the following conventions:

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_m \end{pmatrix} \qquad \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \qquad \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{11} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{n2} & \cdots & a_{mn} \end{pmatrix}$$

row vector **X** column vector **Y** matrix **A**

Note that in a matrix, the first subscript of an element refers to the row and the second subscript refers to the column.

Arithmetic

Two matrices of the same dimensions can be added or subtracted element by element. Thus, for **C** = **A** + **B**, the elements of **C** are $c_{ij} = a_{ij} + b_{ij}$.

Example:

$$\begin{pmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \\ 3 & 6 & 9 \end{pmatrix} + \begin{pmatrix} 3 & 0 & -6 \\ 2 & -3 & 1 \\ 9 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 4 & -2 & -3 \\ 2 & 1 & 6 \\ 12 & 12 & 12 \end{pmatrix}$$

To multiply a matrix by a scalar, every element of the matrix is multiplied by the scalar. Thus, for **C** = k**A**, we have $c_{ij} = k \times a_{ij}$.

Example:

$$3\begin{pmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \\ 3 & 6 & 9 \end{pmatrix} = \begin{pmatrix} 3 & -6 & 9 \\ 0 & 12 & 15 \\ 9 & 18 & 27 \end{pmatrix}$$

The product of a row vector of dimension m and a column vector of dimension m is a scalar:

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_m \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = x_1 y_1 + x_2 y_2 + \ldots + x_m y_m$$

Two matrices **A** and **B** are conformable for multiplication, in that order, if the number of columns in **A** is the same as the number of rows in **B**. Let **A** be of order $m \times n$ (m rows and n columns) and **B** be of order $n \times p$. The product is obtained by multiply every row of **A** into every column of **B**, using the rules just defined for the product of a row vector and a column vector. Thus, for **C** = **AB**, we have $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$, and the resulting matrix is of order $m \times p$. Notice that, by these rules, we can multiply a row vector by a matrix that has the same number of rows as the dimension of the vector; and we can multiply a matrix by a column vector if the matrix has the same number of columns as the dimension of the vector. Thus, using the notation at the beginning of this section: For **D** = **XA**, we end up with a row vector with elements $d_i = \sum_{k=1}^{m} x_k a_{ki}$. For **E** = **AY**, we end up with a column vector with elements $e_i = \sum_{k=1}^{m} a_{ik} y_k$.

Example:

$$\begin{pmatrix} 2 & -5 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \\ 3 & 6 & 9 \end{pmatrix} = \begin{pmatrix} 2 + 3 \times 3 & 2 \times (-2) + (-5) \times 4 + 3 \times 6 & 2 \times 3 + (-5) \times 5 + 3 \times 9 \end{pmatrix} = \begin{pmatrix} 11 & 6 & 8 \end{pmatrix}$$

Example: $$\begin{pmatrix}1 & -2 & 3\\0 & 4 & 5\\3 & 6 & 9\end{pmatrix}\begin{pmatrix}2\\-5\\3\end{pmatrix}=\begin{pmatrix}1\times 2+(-2)\times(-5)+3\times 3\\4\times(-5)+5\times 3\\3\times 2+6\times(-5)+9\times 3\end{pmatrix}=\begin{pmatrix}21\\-5\\3\end{pmatrix}$$

Determinants

The determinant of the square matrix **A**, denoted by det(**A**), is a scalar value representing sums and products of the elements of the matrix. For details, see any text on linear algebra. Here, we simply report the results.

For a 2×2 matrix **A**, det(**A**) = $a_{11}a_{22} - a_{21}a_{12}$.

For a 3×3 matrix **A**, det(**A**) = $a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$

$- a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$

In general, the determinant of a square matrix can be calculated in terms of its cofactors. A **cofactor** of **A** is denoted by cof_{ij}(**A**) and is defined as the determinant of the reduced matrix formed by deleting the ith row and jth column of **A** and choosing positive sign if $i + j$ is even and the negative sign if $i + j$ is odd. For example:

$$\text{cof}_{23}\begin{pmatrix}2 & 4 & 3\\6 & 1 & 5\\-2 & 1 & 3\end{pmatrix}=-\det\begin{pmatrix}2 & 4\\-2 & 1\end{pmatrix}=-10$$

The determinant of an arbitrary $n\times n$ square matrix can be evaluated as:

$$\det(\mathbf{A})=\sum_{j=1}^{n}\left[a_{ij}\text{cof}_{ij}(\mathbf{A})\right] \quad \text{for any } i$$

or

$$\det(\mathbf{A})=\sum_{i=1}^{n}\left[a_{ij}\text{cof}_{ij}(\mathbf{A})\right] \quad \text{for any } j$$

For example:

$$\det\begin{pmatrix} 2 & 4 & 3 \\ 6 & 1 & 5 \\ -2 & 1 & 3 \end{pmatrix} = a_{21}\text{cof}_{21} + a_{22}\text{cof}_{22} + a_{23}\text{cof}_{23}$$
$$= 6 \times \left(-\det\begin{pmatrix} 4 & 3 \\ 1 & 3 \end{pmatrix}\right) + 1 \times \det\begin{pmatrix} 2 & 3 \\ -2 & 3 \end{pmatrix} + 5 \times \left(-\det\begin{pmatrix} 2 & 4 \\ -2 & 1 \end{pmatrix}\right)$$
$$= 6(-9) + 1(12) + 5(-10) = -92$$

Inverse of a Matrix

If a matrix **A** has a nonzero determinant, then it has an inverse, denoted as $\mathbf{A}^{-1}$. The inverse has that property that $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$, where **I** is the matrix that is all zeros except for ones along the main diagonal from upper left to lower right. **I** is known as the identity matrix because any vector or matrix multiplied by **I** results in the original vector or matrix. The inverse of a matrix is calculated as follows. For $\mathbf{B} = \mathbf{A}^{-1}$,

$$b_{ij} = \frac{\text{cof}_{ji}(\mathbf{A})}{\det(\mathbf{A})}$$

For example, if **A** is the matrix in the preceding example, then for the inverse matrix **B**, we can calculate:

$$b_{32} = \frac{\text{cof}_{23}(\mathbf{A})}{\det(\mathbf{A})} = \frac{-10}{-92} = \frac{10}{92}$$

Continuing in the fashion, we can compute all nine elements of **B**. Using Sage, we can easily calculate the inverse:

```
sage: A = Matrix([[2,4,3],[6,1,5],[-2,1,3]])
sage: A

[ 2  4  3]
[ 6  1  5]
[-2  1  3]
sage: A^-1

[  1/46   9/92 -17/92]
[  7/23  -3/23  -2/23]
[ -2/23   5/46  11/46]
```

And we have:

$$\begin{pmatrix} 2 & 4 & 3 \\ 6 & 1 & 5 \\ -2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 2/92 & 9/92 & -17/92 \\ 28/92 & -12/92 & -8/92 \\ -8/92 & 10/92 & 22/92 \end{pmatrix} = \begin{pmatrix} 2/92 & 9/92 & -17/92 \\ 28/92 & -12/92 & -8/92 \\ -8/92 & 10/92 & 22/92 \end{pmatrix} \begin{pmatrix} 2 & 4 & 3 \\ 6 & 1 & 5 \\ -2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

E.2 LINEAR ALGEBRA OPERATIONS OVER Z_n

Arithmetic operations on vectors and matrices can be carried out over Z_n; that is, all operations can be carried out modulo *n*. The only restriction is that division is only allowed if the divisor has an multiplicative inverse in Z_n. For our purposes, we are interested primarily in operations over Z_{26}. Because 26 is not a prime, not every integer in Z_{26} has a multiplicative inverse. Table E.1 lists all the multiplicative inverses modulo 26. For example $3 \times 9 = 1 \bmod 26$, so 3 and 9 are multiplicative inverses of each other.

Table 1.1 Multiplicative Inverses mod 26

Value	Inverse		Value	Inverse
1	1		15	7
3	9		17	23
5	21		19	11
7	15		21	5
9	3		23	17
11	19			

As an example, consider the following matrix in Z_{26}. $\mathbf{A} = \begin{pmatrix} 4 & 3 \\ 9 & 6 \end{pmatrix}$. Then,

$$\det(\mathbf{A}) = (4 \times 6) - (3 \times 9) \bmod 26 = -3 \bmod 26 = 23$$

From Table E.1, we have $(\det(\mathbf{A}))^{-1} = 17$. We can now calculate the inverse matrix:

$$\mathbf{A}^{-1} = \left(\det(\mathbf{A})\right)^{-1} \begin{pmatrix} \text{cof}_{11}(\mathbf{A}) & \text{cof}_{21}(\mathbf{A}) \\ \text{cof}_{12}(\mathbf{A}) & \text{cof}_{22}(\mathbf{A}) \end{pmatrix} = 17 \times \begin{pmatrix} 6 & -3 \\ -9 & 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} 24 & 1 \\ 3 & 16 \end{pmatrix}$$

To verify:

$$\mathbf{A}\mathbf{A}^{-1} = \begin{pmatrix} 4 & 3 \\ 9 & 6 \end{pmatrix} \begin{pmatrix} 24 & 1 \\ 3 & 16 \end{pmatrix} \bmod 26 = \begin{pmatrix} 105 & 52 \\ 234 & 105 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{A}^{-1}\mathbf{A} = \begin{pmatrix} 24 & 1 \\ 3 & 16 \end{pmatrix} \begin{pmatrix} 4 & 3 \\ 9 & 6 \end{pmatrix} \bmod 26 = \begin{pmatrix} 105 & 78 \\ 156 & 105 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$