Lecture 3:

Classical Encryption Techniques II

4th Year- Course, CCSIT, UoA

Lecture Goals

1. To trace the history of some early approaches to cryptography.
2. To emphasize the basic principles of *substitution* and *transposition*, which are still valid till now (despite of the change of technology).

The Hill Cipher (1)

The Hill cipher is another multi-letter cipher that takes a very different (more mathematical) approach to multi-letter substitution:

- You assign an integer to each letter of the alphabet. For the sake of discussion, let's say that you have assigned the integers 0 through 25 to the letters 'a' through 'z' of the plaintext.
- The encryption key, call it K, consists of a 3 ×3 matrix of integers:

$$\mathbf{K} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$$

The Hill Cipher (2)

- Now we can transform ***three letters*** at a time from plaintext, the letters being represented by the numbers p_1, p_2, and p_3, into three ciphertext letters c_1, c_2, and c_3 in their numerical representations by

$$
\begin{aligned}
c_1 &= (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \; mod \; 26 \\
c_2 &= (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \; mod \; 26 \\
c_3 &= (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \; mod \; 26
\end{aligned}
$$

- The above set of linear equations can be written more compactly in the following vector-matrix form:

$$
\vec{\mathbf{C}} = [\mathbf{K}] \, \vec{\mathbf{P}} \; mod \; 26
$$

The Hill Cipher (3)

- Obviously, the decryption would require the ***inverse*** of K matrix.

$$\vec{\mathbf{P}} = \left[\mathbf{K}^{-1}\right] \vec{\mathbf{C}} \; mod \; 26$$

This works because

$$\vec{\mathbf{P}} = \left[\mathbf{K}^{-1}\right] [\mathbf{K}] \vec{\mathbf{P}} \; mod \; 26 = \vec{\mathbf{P}}$$

- This can be illustrated in the following example.

Example

- Consider the plaintext "***paymoremoney***" and use the encryption Key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

- The first three letters of the plaintext (p a y) are represented by the vector (15 0 24).
- Then, (15 0 24) **K** = (303 303 531) *mod 26*
  = (17 17 11) = R R L.
- Continuing in this fashion, the ciphertext for the entire plaintext is: *RRLMWBKASPDH* .

Example (cont.)

- Decryption requires using the inverse of the matrix K which is:

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- Note that:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- It is easily seen that if the matrix $\mathbf{K}^{-1}$ is applied to the ciphertext, then the plaintext is recovered.

- **H.W.:** Do the complete encryption and decryption process for this example.

How Secure is the Hill Cipher?

- As with Playfair, the strength of the Hill cipher is that it completely hides single-letter frequencies.
- It is extremely secure against ***ciphertext only attacks***. That is because the key space can be made extremely large by choosing the matrix elements from a large set of integers.
- The key space can be made even large by generalizing the technique to larger-sized matrices.
- But it has zero security when the plaintext-ciphertext pairs are known. The key matrix can be calculated easily from a set of known P, C pairs.