Lecture 18

Hill ciphers Encoding groups of n letters — n-grams — when n is larger than average word length is a way of making a frequency-based attack very difficult. To keep things simple, I shall concentrate on the case $n=2$, but the generalization to arbitrary n will be clear.

Divide the plaintext into digrams. If the cleartext has odd length then add a dummy letter to the end to make it of even length. Replace each digram (P_1, P_2) by its numerical equivalent (N_1, N_2). We shall encode using a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and calculate mod 26. Thus

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} N_1 \\ N_2 \end{pmatrix} = \begin{pmatrix} aN_1 + bN_2 \\ cN_1 + dN_2 \end{pmatrix}$$

which can then be converted to letter form giving the ciphertext (C_1, C_2). Put $E = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

We cannot use an arbitrary matrix because we need to be able to decrypt messages. Thus we need a matrix D such that $DE = I$ where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the 2×2 identity matrix.

Observe that

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

where $ad - bc = \det(E) = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$.

We need $\det(E)$ to be invertible mod 26
i.e. coprime to 26

* If this holds then $\det(E)^{-1}$ means the inverse of $\det(E)$ mod 26. *

In this case,

$$D = \det(E)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and $DE = I$, as required.

Example Show that $E = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ is an enciphering matrix. Here $\det(E) = 3$ and $\gcd(3, 26) = 1$
$\therefore$ 3 is invertible mod 26 and its inverse is 9.

Thus

$$E^{-1} = 3^{-1} \begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = 9 \begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix}$$

$$= \underline{\underline{\begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix}}}$$

Check $\begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ mod 26.

We shall now show how to use the matrix E to encrypt a plaintext.

Plaintext: I AM IN HIDING.
Length is odd so we add a padding letter to the end
— I choose Z.

IA MI NH ID IN GZ

numerical equivalents of these digrams

(8,0), (12,8), (13,7), (8,3), (8,13), (6,25)

Encrypting

$A\begin{pmatrix}8\\0\end{pmatrix} = \begin{pmatrix}8\\0\end{pmatrix} = \begin{pmatrix}I\\A\end{pmatrix}$ $\quad A\begin{pmatrix}8\\3\end{pmatrix} = \begin{pmatrix}14\\9\end{pmatrix} = \begin{pmatrix}O\\J\end{pmatrix}$

$A\begin{pmatrix}12\\8\end{pmatrix} = \begin{pmatrix}2\\24\end{pmatrix} = \begin{pmatrix}C\\Y\end{pmatrix}$ $\quad A\begin{pmatrix}5\\13\end{pmatrix} = \begin{pmatrix}17\\13\end{pmatrix} = \begin{pmatrix}R\\N\end{pmatrix}$

$A\begin{pmatrix}13\\7\end{pmatrix} = \begin{pmatrix}1\\21\end{pmatrix} = \begin{pmatrix}B\\V\end{pmatrix}$ $\quad A\begin{pmatrix}4\\25\end{pmatrix} = \begin{pmatrix}4\\23\end{pmatrix} = \begin{pmatrix}E\\X\end{pmatrix}$

Ciphertext: IACYBVOJINEX

Affine block ciphers

Caesar, Vigenère and Hill ciphers are all special cases of the following general construction.

n-grams are mapped to n-grams

$$E: \mathbb{Z}_{26}^n \longrightarrow \mathbb{Z}_{26}^n$$

is defined by $E(\underline{x}) = A\underline{x} + \underline{b}$ where $\det(A)$ is invertible mod 26 so that A^{-1} exists, $\underline{b} \in \mathbb{Z}_{26}^n$ is an arbitrary vector. The key in this case is $(A, \underline{b})$.

- Vigenère ciphers are of this type: they arise when $A = I$.
- Hill ciphers arise when $\underline{b} = \underline{0}$

I shall now prove that if Eve can obtain certain information she can find the enciphering key and break the code.

We assume that she has obtained by some means $n+1$ pairs $(\underline{w}_i, \underline{c}_i)$ where $\underline{c}_i$ is ciphertext corresponding to the plaintext $\underline{w}_i$. Thus

$$\underline{c}_i = A\underline{w}_i + \underline{b} \quad \text{where } 0 \le i \le n$$

For each $i \neq 0$, we have that

$$\underline{c}_i - \underline{c}_0 = A(\underline{w}_i - \underline{w}_0) \quad (*)$$

Put $W = (\underline{w}_1 - \underline{w}_0, \ldots, \underline{w}_n - \underline{w}_0)$

$$C = (\underline{c}_1 - \underline{c}_0, \ldots, \underline{c}_n - \underline{c}_0)$$

Then we get from $(*)$ the matrix equation

$$AW = C.$$

We assume that Eve has been clever and chosen (or found) the $\underline{w}_i$ so that $\det(W)$ is invertible mod 26. It follows that $A = CW^{-1}$.

Now C and W and so W^{-1} are known from which it follows that A can be found. Once we have found A, we can find $\underline{b}$ by

$$\underline{b} = \underline{c}_0 - A\underline{w}_0.$$

Thus the enciphering key $(A, \underline{b})$ has been calculated.
