1 Agenda

- Assignments: 9 will be due on Jan 31.
- Hill and Modular Arithmetic
- Feistel and Bit Operations

2 Hill and Modular Arithmetic

The key is a $k \times k$ matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{bmatrix}$$

We require that $\gcd(\det(A), 29) = 1$. Given a sequence of values $p_1, p_2, ..., p_k \to c_1, c_2, ..., c_k$, where for each i,

$$c_i = a_{i1}p_1 + a_{i2}p_2 + \cdots + a_{ik}p_k \pmod{29}$$

or

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix} \pmod{29}$$

then

$$\begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{bmatrix}^{-1} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix} \pmod{29}$$

Example 1. If the key $A = \begin{bmatrix} 5 & 13 \\ 1 & 17 \end{bmatrix}$ and the plaintext is GIFT, or 6-8-5-19 then

$$\begin{bmatrix} 5 & 13 \\ 1 & 17 \end{bmatrix} \begin{bmatrix} 6 \\ 8 \end{bmatrix} = \begin{bmatrix} 5 \cdot_{29} 6 +_{29} 8 \cdot_{29} 13 \\ 1 \cdot_{29} 6 +_{29} 17 \cdot_{29} 8 \end{bmatrix} = \begin{bmatrix} 18 \\ 26 \end{bmatrix} = \begin{bmatrix} S \\ . \end{bmatrix}$$

and

$$\begin{bmatrix} 5 & 13 \\ 1 & 17 \end{bmatrix} \begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 5 \cdot_{29} 5 +_{29} 13 \cdot_{29} 19 \\ 1 \cdot_{29} 5 +_{29} 17 \cdot_{29} 19 \end{bmatrix} = \begin{bmatrix} 11 \\ 9 \end{bmatrix} \nexists [$$

or alternatively,

$$\begin{bmatrix} 5 & 13 \\ 1 & 17 \end{bmatrix} \begin{bmatrix} 6 & 5 \\ 8 & 19 \end{bmatrix} = \begin{bmatrix} 18 & 11 \\ 26 & 9 \end{bmatrix}$$

Example 2. Recover the plaintext from the ciphertext FVGLNPCJSG given that it was enrypted using the Hill encipherment system with a 2×2 matrix mod 29 and the plaintext begins with the letters tell.

We seek a key of the form $k = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Our plaintext is tell which translates to 19 4 11 11, and so in ciphertext we have FVGL which translates to 5 21 6 11. Then we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 19 \\ 4 \end{bmatrix} = \begin{bmatrix} 5 \\ 21 \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 6 \\ 11 \end{bmatrix}$$

Or in other words,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 19 & 11 \\ 4 & 11 \end{bmatrix} \begin{bmatrix} 19 & 11 \\ 4 & 11 \end{bmatrix}^{-1} = \begin{bmatrix} 5 & 6 \\ 21 & 11 \end{bmatrix} \begin{bmatrix} 19 & 11 \\ 4 & 11 \end{bmatrix}^{-1}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 5 & 6 \\ 21 & 11 \end{bmatrix} \begin{bmatrix} 19 & 11 \\ 4 & 11 \end{bmatrix}^{-1}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \cdots$$

But then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} 5 & 6 & 13 & 2 & 18 \\ 21 & 11 & 15 & 9 & 6 \end{bmatrix} = \cdots$$