DES: THE FEISTEL CIPHER

MATH 195

The Hill cipher allows us to create large invertible maps by specifying only a small amount of data (the key). However, the linearity in the cipher is its downfall: it is too easy for the eavesdropper to collect enough data and discover the key.

The central mathematical idea behind the Feistel cipher is to take random maps (which may or may not be invertible) and turning them into invertible maps. For example, for any matrix $A \in M(k, R)$, we can find a larger matrix which is invertible:

$$\begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \in GL(2k, R).$$

In fact, the inverse is

$$\begin{pmatrix} I & 0 \\ -A & I \end{pmatrix}.$$

Let V be a group, written additively. Think of V as a vector space of k bits, e.g. $V = (\mathbb{Z}/2\mathbb{Z})^k$. Let $g : V \to V$ be any map. (This gives us many options: the number of elements is $(\#V)^{\#V} = 2^{k2^k}$. Typically, $k = 4$ or $k = 32$, which give us huge numbers!) Define

$$\begin{aligned} G : V \times V &\to V \times V \\ G(x, y) &= (x, g(x) + y), \end{aligned}$$

e.g. if A was the above matrix, we would have

$$\begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ Ax + y \end{pmatrix}.$$

Claim. G is bijective.

Proof. Define $h : V \to V$ by $h(x) = -g(x)$. (Note: if $V = (\mathbb{Z}/2\mathbb{Z})^k$, then $h = g$.) h gives rise to $H : V \times V \to V \times V$, $H(x, y) = (x, h(x) + y) = (x, -g(x) + y)$.

We now calculate $H \circ G = \mathrm{id}_{V \times V}$:

$$\begin{aligned} (H \circ G)(x, y) = H(G(x, y)) = H(x, g(x) + y) &= (x, h(x) + (g(x) + y)) \\ &= (x, -g(x) + g(x) + y) = (x, y). \end{aligned}$$

In the same way, $G \circ H = \mathrm{id}_{V \times V}$. Therefore G is bijective. □

Note: For $V = (\mathbb{Z}/2\mathbb{Z})^k$, $H = G$ so $G^2 = G \circ G = \mathrm{id}_{V \times V}$.

Example. Let $V = \mathbb{Z}/5\mathbb{Z}$, so $V \times V = (\mathbb{Z}/5\mathbb{Z})^2$, a set of 25 elements, the alphabet if we do not use the letter J.

Define $g : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ by $g(0) = 3$, $g(1) = 1$, $g(2) = 4$, $g(3) = 1$, $g(4) = 0$. If $x = 3$, since $g(3) = 1$, we have $G(3, y) = (3, g(3) + y) = (3, y + 1)$, so everything in

---

This is some of the material covered February 14, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

this "column" is increased by 1. Likewise, $g(2) = 4$, so $G(4, y) = (4, y + 4)$ so we "shift" by 4.

Notice that every other block is unchanged by G (it is unencrypted!), so we need to do better. Therefore: use your key K to produce t functions $g_1, \ldots, g_t : V \to V$ (usually $t = 2$ or $t = 16$), where $V = (\mathbb{Z}/2\mathbb{Z})^k$. These give rise to t bijections $G_1, \ldots, G_t : V \times V \to V \times V$ with $V \times V = (\mathbb{Z}/2\mathbb{Z})^{2k} = \mathcal{P} = \mathcal{C}$. Now

$$E_K : V \times V \to V \times V$$

is defined by

$$E_K = G_t \circ s \circ \cdots \circ G_2 \circ s \circ G_1,$$

with $s(x, y) = (y, x)$ the "swap".

Note that $D_K = E_K^{-1} = G_1 \circ s \circ \cdots \circ s \circ G_t$.

We would also like our cryptosystem to be secure, which means we must make sure that any statistical probabilities in the English language are erased when we garble the message.

So what is the key space $\mathcal{K}$ and how does an element $K \in \mathcal{K}$ produce t functions $g_1, \ldots, g_t$? Let $\mathcal{K} = (\mathbb{Z}/2\mathbb{Z})^{10 \text{ or } 56}$, and $\mathcal{S} = (\mathbb{Z}/2\mathbb{Z})^{8 \text{ or } 48}$ be the space of subkeys. Each $K \in \mathcal{K}$ produces t subkeys $K_1, \ldots, K_t \in \mathcal{S}$. Next there is a round function $F : V \times \mathcal{S} \to V$ given once and for all which uses S-boxes, and now $g_i : V \to V$ are defined by $g_i(x) = F(x, K_i)$.