Constructing MAC using a PRF.

Gen (1^n) chooses k to be random n-bit string.
$MAC_k(m) = F_k(m) = t$ (tag)
$Verify_k(m,t)$ = Accept, if and only if $t = F_k(m)$

Theorem: If F is a pseudorandom function, the above scheme is a secure fixed length MAC.

~~Variable length MACs~~

Final Protocol:

Construction: Let $\Pi' = (Gen', Mac', Vrfy')$ be a fixed length MAC for messages of length n. Define a MAC as follows:

- **Gen:** this is identical to Gen'.
- **Mac:** On input key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^*$ of length $l < 2^{n/4}$, parse m into d blocks $m_1, \ldots, m_d$, each of length $n/4$. Next choose a random Identifier $r \leftarrow \{0,1\}^{n/4}$. For $i = 1, \ldots, d$, compute $t_i \leftarrow MAC'_k(r \| l \| i \| m_i)$ where i and l are uniquely encoded as strings of length $n/4$. Finally the output is tag $t := \langle r, t_1, \ldots, t_d \rangle$.
- **Vrfy:** On input a key $k \in \{0,1\}^n$, a message $m \in \{0,1\}^*$ of length $l < 2^{n/4}$, and a tag $t = \langle r, t_1, \ldots, t_d \rangle$ parse m into d blocks $m_1, m_2, \ldots, m_d$ each of length $n/4$. Output 1 if and only if $d' = d$ and $Vrfy'_k(r \| l \| i \| m_i, t) = 1$ for $1 \le i \le d$.

A variable length MAC from a fixed length MAC