Encrypting Variable Length Messages

Suppose we have a fixed-length PRF:

\[ F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n \]
Encrypting Variable Length Messages

Suppose we have a fixed-length PRF:

\[ F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \]

We construct an encryption scheme for arbitrary-length messages as follows.

\[ \text{Gen}(1^n) : k \leftarrow \{0,1\}^n \]

\[ \text{Enc}(k,m) : \]

- Let \( \ell = |m|/n \). (*)
- Break \( m \) into \( \ell \) blocks, each of length \( n \): \( m = m_1 || \ldots || m_\ell \)
- Sample \( r_1, \ldots, r_\ell \leftarrow \{0,1\}^n \).
- Output \( (r_1, F_k(r_1) \oplus m_1) \ldots, (r_\ell, F_k(r_\ell) \oplus m_\ell)) \).

(*) For the moment, assume \( |m| \) is a multiple of \( n \). If not, we can use an appropriate padding scheme to pad the last block.
Enciphering Variable Length Messages

Suppose we have a fixed-length PRF:

\[ F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \]

We construct an encryption scheme for arbitrary-length messages as follows.

Gen\((1^n) : k \leftarrow \{0,1\}^n\)

Enc\((k, m) : \)

\begin{itemize}
  \item Let \( \ell = |m|/n \). (*)
  \item Break \( m \) into \( \ell \) blocks, each of length \( n \): \( m = m_1 || \ldots || m_\ell \)
  \item Sample \( r_1, \ldots, r_\ell \leftarrow \{0,1\}^n \).
  \item Output \( ((r_1, F_k(r_1) \oplus m_1) \ldots, (r_\ell, F_k(r_\ell) \oplus m_\ell)). \)
\end{itemize}

Dec\((k, ((r_1, c_1), \ldots, (r_\ell, c_\ell))) : \)

\begin{itemize}
  \item Compute \( m_i = F_k(r_i) \oplus c_i \).
  \item Output \( m = m_1 || \ldots || m_\ell \).
\end{itemize}

(*) For the moment, assume \( |m| \) is a multiple of \( n \). If not, we can use an appropriate padding scheme to pad the last block.