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:

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$$

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

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

$\underline{\mathsf{Enc}(k, m)}$:

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

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

Encrypting Variable Length Messages

Suppose we have a fixed-length PRF:

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$$

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

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

$\underline{\mathsf{Enc}(k, m)}$:

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

$\underline{\mathsf{Dec}\big(k, \big((r_1, c_1), \ldots, (r_\ell, c_\ell)\big)\big)}$:

- Compute $m_i = F_k(r_i) \oplus c_i$.
- Output $m = m_1 || \cdots || m_\ell$.

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