1.1.1 Encryption function block diagram

Each instance of the encryption function includes the Encryption Key Activation process (see 11.6.2.4 and 11.6.2.6) and the Encryption process (see 11.7.2). The block diagram of the encryption function is illustrated in Figure 11-2.

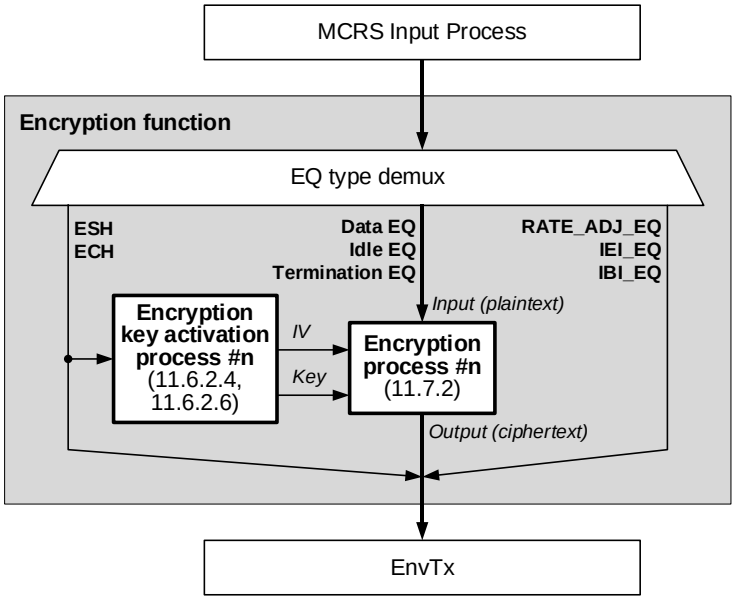

Figure 11-2–Encryption function block diagram.

The Encryption Key Activation process detects the transmission of either the envelope start header (ESH) or the envelope continuation header (ECH) and uses the data inside the header to generate an initialization vector IV and the encryption key. These two parameters are passed to the Encryption process, which encrypts the given envelope as one cryptographic message.

The encryption function encrypts the envelope payload, which consists of data EQs, idle EQs, and termination EQs. The envelope header itself bypasses the Encryption process and is transmitted unencrypted (see 11.7.5.2).

The inter-envelope control EQs include rate adjustment (RATE_ADJ_EQ), inter-envelope-idle (IEI_EQ), and inter-burst idle (IBI_EQ) (see 11.7.5.1). These control EQs bypass the Encryption process and are transmitted unencrypted.

1.1.2 Decryption function block diagram

Each instance of the decryption function includes the Decryption Key Activation process (see 11.6.2.5) and the Decryption process (see 11.7.3). The block diagram of the decryption function is illustrated in Figure 11-3.

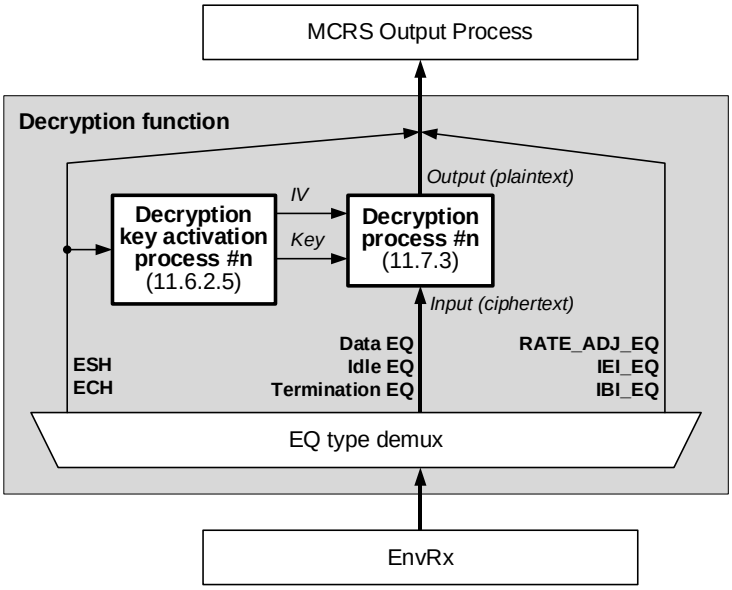

Figure 11-3–Decryption function block diagram.

The Decryption Key Activation process detects the reception of either the envelope start header (ESH) or the envelope continuation header (ECH) and uses the data inside the header to generate an initialization vector IV and the decryption key. These two parameters are passed to the Decryption process, which decrypts the given envelope as one cryptographic message.

The decryption function decrypts only the envelope payload, which consists of data EQs, idle EQs, and termination EQs. The envelope header itself is received unencrypted and bypasses the Decryption process (see 11.7.5.2).

The inter-envelope control EQs include rate adjustment (RATE_ADJ_EQ), inter-envelope-idle (IEI_EQ), and inter-burst idle (IBI-EQ) (see 11.7.5.1). These control EQs are received unencrypted and bypass the Decryption process.