PROOF. Our main step in the proof is to replace the underlying block cipher e_k by a pseudo-random permutation. This can be done by the assumption that e_k is a secure PRP, namely there is some adversary B such that

$$\text{Adv}^{\mathsf{PRP}}_{e_k}(B) = \Big|\Pr[A \text{ wins } \mathsf{ECB}[e_k]] - \Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]]\Big| \tag{18}$$

where we let $\mathcal{P}$ denote a random permutation. We now need to bound the probability that A wins this latter game, i.e. $\Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]]$. It is easier to bound the probability that A does not win. Since for a PRP the adversary cannot learn anything about the output value of the permutation until she queries the permutation on the specific input value, the probability that she does not win is given by the probability that out of the q_e distinct queries to the encryption oracle we do not obtain *all* of the ℓ blocks in the challenge ciphertext. Setting $N = 2^n$ this gives us, where ${}^xC_y$ is the function which returns the number of combinations of y objects selected from n,

$$\begin{aligned}
\Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]] &= 1 - \Pr[A \text{ does not win } \mathsf{ECB}[\mathcal{P}]] \\
&\leq 1 - \frac{{}^{N-\ell}C_{q_e}}{{}^{N}C_{q_e}} \\
&= 1 - \prod_{i=0}^{\ell-1}\left(\frac{N-q_e-i}{N-i}\right) \\
&\approx 1 - \left(\frac{N-q_e}{N}\right)^{\ell} && \text{Since } \ell \ll q_e \ll N \\
&= \ell \cdot q_e/N.
\end{aligned}$$

Hence,

$$\begin{aligned}
\Pr[A \text{ wins } \mathsf{ECB}[e_k]] &= \Big|\Pr[A \text{ wins } \mathsf{ECB}[e_k]] \\
&\qquad + (\Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]] - \Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]])\Big| && \text{adding in zero} \\
&\leq \Big|\Pr[A \text{ wins } \mathsf{ECB}[e_k]] - \Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]]\Big| \\
&\qquad + \Big|\Pr[A \text{ wins } \mathsf{ECB}[\mathcal{P}]]\Big| && \text{triangle inequality} \\
&\leq \text{Adv}^{\mathsf{PRP}}_{e_k}(B) + \ell \cdot \frac{q_e}{2^n}.
\end{aligned}$$

□

Notice that when q_e is small relative to 2^n the probability $q_e/2^n$ is very close to zero, whereas as q_e approaches 2^n we obtain a probability close to one.

13.4.2. CBC Mode: One way of countering the problems with ECB Mode is to chain the cipher, and in this way add context to each ciphertext block. The easiest way of doing this is to use Cipher Block Chaining Mode, or CBC Mode. Again, the plaintext must first be divided into a series of blocks

$$m_1, \ldots, m_q,$$

and as before the final block may need padding to make the plaintext length a multiple of the block length. Encryption is then performed as in Figure 13.9, or equivalently via the equations

$$\begin{aligned}
c_1 &\leftarrow e_k(m_1 \oplus IV), \\
c_i &\leftarrow e_k(m_i \oplus c_{i-1}) \text{ for } i > 1.
\end{aligned}$$

With the output ciphertext being $IV \| c_1 \| c_2 \| \ldots$. The transmission of IV with the ciphertext can be dropped if the receiver will know what the value will be a priori.