CPA Security Theory

The task is to use the previously constructed PRF to get an encryption and decryption algorithm that is secure against CPA.

As the textbook suggests, the probability of getting back the input string given PRF's output is negligibly above 1/2, i.e., random chance. This implies that PRF is also pseudo-random.

The encryption scheme is as follows:
$c =< r, F_k(r) \oplus m >$
And the decryption scheme is as follows:
$m = F_k(r) \oplus F_k(r) \oplus m$
This decryption is possible because of the concatenation of random string r and PRF-xor-message cipher $F_k(r) \oplus m$.

The proof given in the textbook can be analogously applied to the given settings, as this is a flavour of the problem described there