Reading

Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell.

What is the main problem this section attacks?

Recall that one main drawback of the One-time pad encryption schemeand its simple encryption operation is that the key k needs to be as long as the message m.

What solution does the section propose?

Instead of requiring that encryptions of any two messages are identically distributed (as in the definition of perfect secrecy), the authors try to attain the secrecy by the computational notion of secure encryption requires only that encryptions of any two messages are indistinguishable.

What central idea did the authors use to solve it?

A natural approach for making the scheme more efficient would be to start off with a short random key k and then try to use some pseudo-random generator g to expand it into a longer random-looking key k = g(k), and finally use k as the key in the One-time pad. In this chapter, the authors introduced the notion of pseudorandomness the idea that things can look completely random (in a sense we precisely define) even though they are not and see how this can be used to achieve secure encryption beating the bounds of the previous chapter. Specifically, they showed the encryption schemes whereby a short key can be used to securely encrypt many long messages; such schemes are able to bypass the inherent limitations of perfect secrecy because they achieve the weaker (but sufficient) notion of computational secrecy.

What is a weakness or limitation of this section?

The authors did not prove unconditionally that the private-key construction which mentioned in this chapter is secure. Rather, they prove that it is secure under the assumption that G is a pseudorandom generator. This approach of reducing the security of a construction to some underlying primitive is of great importance for a number of reasons. They also did not know how to prove the existence of an encryption scheme satisfying Definition 3.9(in the book) and such a proof seems far out of reach today.