Reading
Introduction to Modern Cryptography, chapers 1 and 2. Johnathan Katz and Yehuda Lindell. 2008.

What is the main problem this section attacks?
Classical cryptographic schemes, and even some modern ones, have failed due to ambiguous notions of what it means for a scheme to be secure.

Chapter 1 presents some simple cryptographic schemes from classical cyptography, and explains how they are easy to break using statistical analysis.

What solution does the section propose?
Chapter 1's attacks are presented in the context of some informal principles for doing cryptography properly.

Chapter 2 begins exploration of a more formal approach to cryptography in the context of a probabilistic definition of perfect secrecy. It also explores proofs of equivalency between notions of perfect secrecy, and that a given scheme attains perfect secrecy.

What central idea did the authors use?
Kirchoffs' principle states that the secrecy of cryptographic secrets should depend on only the secrecy of the cryptographic key and not the cryptographic scheme itself.

Problems and approaches in cryptography should be accompanied by

1. Definition of security in the model
2. Assumptions of the model
3. Rigorous proof that the definition of security is satisfied with respect to the assumptions

The relationships between the distributions of keys, plaintext, and cyphertext are critical in determining how effective a scheme really is.
One-time pads can be used to attain perfect secrecy in a cryptographic scheme.

What is a weakness or limitation of the section?
The main weakness of the ideas in Chapter 1 is that they are largely informal. Chapter 2 explores formally limitations of cryptographic schemes with perfect secrecy, for example that the keys must be at least as long as the messages, and that the keys cannot be reused.