## 1.1 Attacks

Before we describe any cryptosystem in detail, however, let us say a few words about ***cryptosystem attacks***. The science of attacking cryptosystems is known as ***cryptanalysis*** and its practitioners are called ***cryptanalysts***. In performing cryptanalysis, we assume that the cryptanalyst knows the algorithms for encryption and decryption, but that he does not know anything about the keys used. This assumption follows the open design principle. In fact, it is dangerous for us to assume that we gain any degree of security from the fact that the cryptanalyst doesn't know which algorithms we are using. Such ***security by obscurity*** approach is likely to fail, since there are a number of different ways that such information can be leaked. For example, internal company documents could be published or stolen, a programmer who coded an encryption algorithm could be bribed or could voluntarily disclose the algorithm, or the software or hardware that implements an encryption algorithm could be reverse engineered. So we assume the cryptanalyst knows which cryptosystem we are using.

There are four primary types of attacks that a cryptanalyst can attempt to perform on a given cryptosystem.

- *Ciphertext-only attack.* In this attack, the cryptanalyst has access to the ciphertext of one or more messages, all of which were encrypted using the same key, $K$. His or her goal is to determine the plaintext for one or more of these ciphertexts or, better yet, to discover $K$.

- *Known-plaintext attack.* Inthis attack, the cryptanalyst has access to one or more plaintext-ciphertext pairs, such that each plaintext was encrypted using the same key, $K$. His or her goal in this case is to determine the key, $K$.

- *Chosen-plaintext attack.* In this attack, the cryptanalyst can chose one or more plaintext messages and get the ciphertext that is associated with each one, based on the use of same key, $K$. In the ***offline chosen-plaintext attack***, the cryptanalyst must choose all the plaintexts in advance, whereas in the ***adaptive chosen-plaintext attack***, the cryptanalyst can choose plaintexts in an iterative fashion, where each plaintext choice can be based on information he gained from previous plaintext encryptions.

- *Chosen-ciphertext attack.* In this attack, the cryptanalyst can choose one or more ciphertext messages and get the plaintext that is associated with each one, based on the use of same key, $K$. As with the chosen-plaintext attack, this attack also has both offline and adaptive versions.