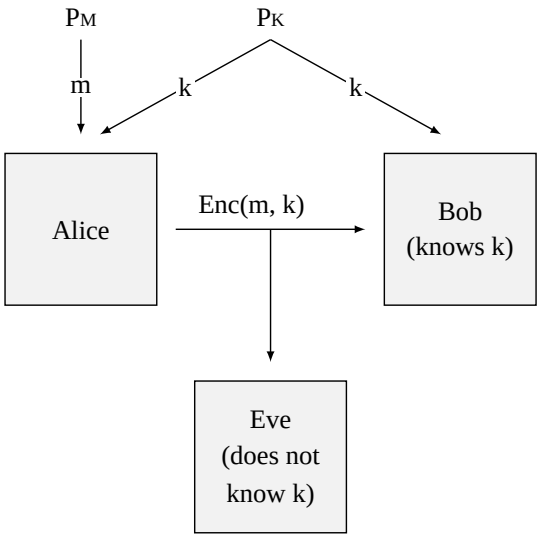
Definition: Perfectly Secure Encryption

Information theory is very useful when analyzing the security of perfectly secure encryption schemes. Consider a scenario where one party, Alice, wants to send a message m (sampled from some distribution P_M) to another party, Bob, over some public channel, for example the internet. Alice and Bob share a key k (sampled from another distribution P_K), which is a piece of information that is known only to them. Alice can use the key to encrypt her message (the **plaintext**), and Bob can use the same key to decrypt the **ciphertext** that Alice created, and read the message. The goal is to do this in such a way that if an eavesdropper (who usually goes by the name 'Eve') listens in on the channel and intercepts the encrypted message, she cannot derive any information about the message as long as she does not know the key k.



Let us formalize the above notion of encryption in the following definition:

Definition: Encryption scheme

An encryption scheme for (the message) M consists of a key K and a ciphertext $C = Enc(M, K)$, such that

- $I(M;K) = 0$ (the key is independent of the message -- this is a **setup assumption**), and

- $H(M|KC) = 0$ (given the key and the ciphertext, Bob can recover the original message)

Note that M, K and C are random variables.

Note that in order to satisfy the second requirement, the encryption function $Enc(\cdot, \cdot)$ needs to be injective: every message is mapped to a *unique* ciphertext.

The above definition does not put any constraints on the amount of information that Eve can get from the ciphertext: we still need to explicitly require the scheme to be secure.

Definition: Perfect security

An encryption scheme is perfectly secure if

$$I(M;C) = 0.$$

This is equivalent to saying $H(M|C) = H(M)$, or to saying that M and C are independent.

This type of security is also sometimes called perfect **information-theoric security**, in order to stress that the ciphertext really does not contain *any* information about the plaintext message. Many commonly used encryption schemes do not provide this type of security. In **computationally secure** schemes, a lot of information about the message may be contained in the ciphertext, but it would take a ridiculous amount of resources (such as computation time or memory) to compute the information about the message from the ciphertext.