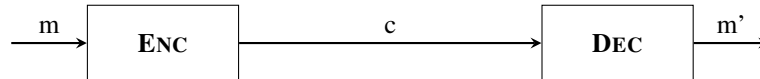




1 One Time Pad

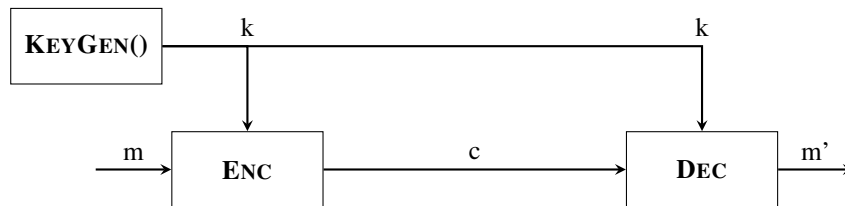
1.1 What is [NOT] CRYPTOGRAPHY

1.1.1 Introduction



The method must not be required to be secret, and it must be able to fall into the enemy's hands without causing any inconvenience.

So if the algorithm do not need to be secret, there must be additional information in the system, which is kept secret from any EAVESDROPPER. This information is called a **(secret) key**.



1.2 Specifics of One Time Pad