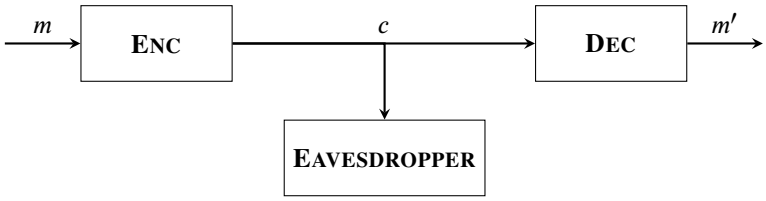
1 One Time Pad

1.1 What is [NOT] CRYPTOGRAPHY

1.1.1 Introduction

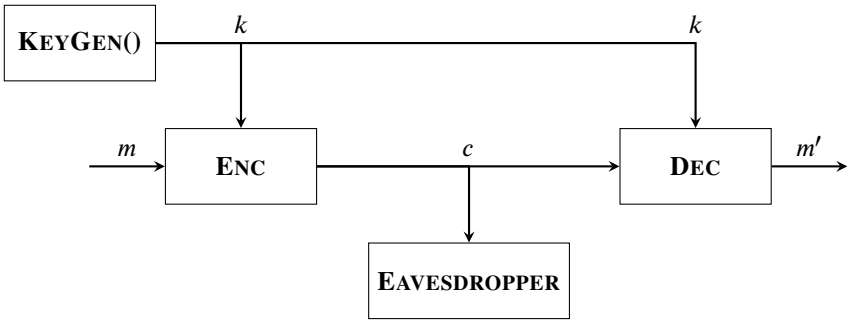
In the idealized model we assume that Alice wants to send a message m (*privately*) to Bob. Alice will modify the message m, also called ***plaintext***, with any method to create a ***ciphertext*** c which will be actually sent to Bob. This transformation is also called encryption (***Enc***). After receiving the ciphertext c, Bob will reverse the step of transforming by using a decription algorithm (***Dec***) to (*hopefully*) get the original plaintext m.
NOTE: We are not trying to hide that a message is sent, so an **EAVESDROPPER** (an attacker between Alice and Bob) can obtain the ciphertext c at any instance. Hiding the existence of communication is called *steganography*.



1.1.2 Kerckhoff's principle

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** k.



1.2 Specifics of ONE-TIME PAD

A *one-time pad* often uses a secret key in the form of a bit string of length λ. The plain- and ciphertexts are also λbit-strings.
The construction of such an one-time pad looks as follows:

KEYGEN()	ENC(k, $m \in \{0,1\}^\lambda$)	DEC(k, $c \in \{0,1\}^\lambda$)
$k \leftarrow \{0,1\}^\lambda$	$c := k \oplus m$	$m' := k \oplus c$
return k	**return** c	**return** m'

Recapture that $k \leftarrow \{0,1\}^\lambda$ means that k is sampled uniformly from the set of λbit-strings.
Further we claim that for all $k, m \in \{0,1\}^\lambda$ it is true, that $Dec(k, Enc(k, m)) = m$.
Otherwise the usage of one-time pad would be silly.
For security reasons we want to say about the encryption scheme that an EAVESDROPPER (who does not know k) cannot leran anything about the message m.
In the end we need to claim that an encryption algorithm is secure if for every $m \in \{0,1\}^\lambda$ the distribution EAVESDROP(m) is the **uniform distribution** of $\{0,1\}^\lambda$, explicitly for every $m, m' \in \{0,1\}^\lambda$ the distributions EAVESDROP(m) and EAVESDROP(m') are identical.

2 The Basics of Proveable Security