

That malicious person do not misuse
the keys. Important to note
that anyone with a secret key
can decrypt the message.

* Symmetric encryption uses a single
key that needs to be shared
among the people who need
to receive the message
while asymmetrical encryption uses
a pair of public key and
a private key to encrypt and
decrypt the message when
communicating.

* Symmetric encryption was an old
technique while asymmetric encryption
is relatively new.

* Symmetric encryption was introduced
to complement the Internet
problem of the need to share
the key in Symmetrical encryption
model.