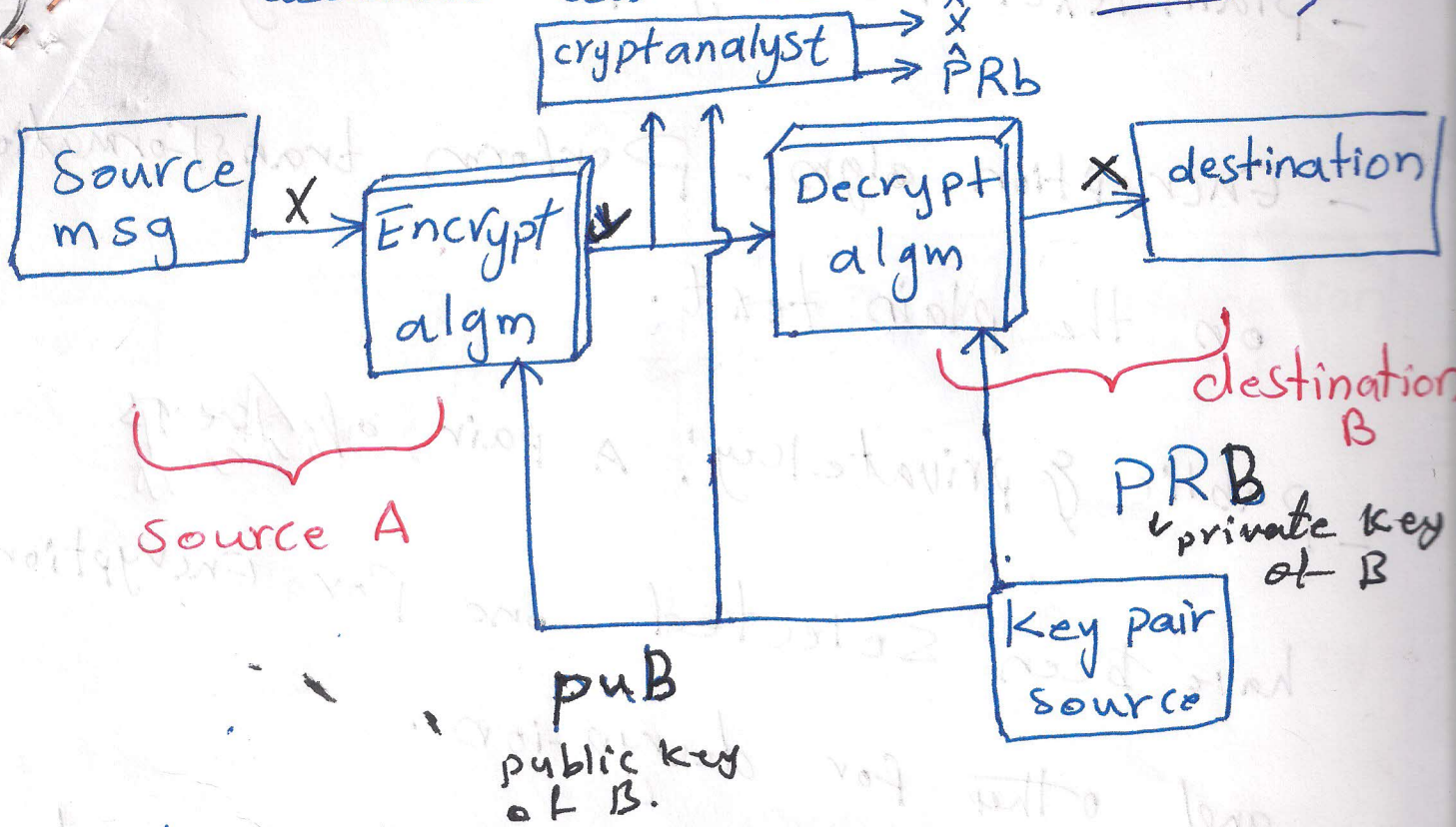
"public key cryptosystem"



where:

* Pub is a public key. For Encrypt.
* PRb is aprivate key. For Decrypt.

this Fig is:

"public key cryptosystem Secrecy"

→

- plain text: the msg to be encrypted

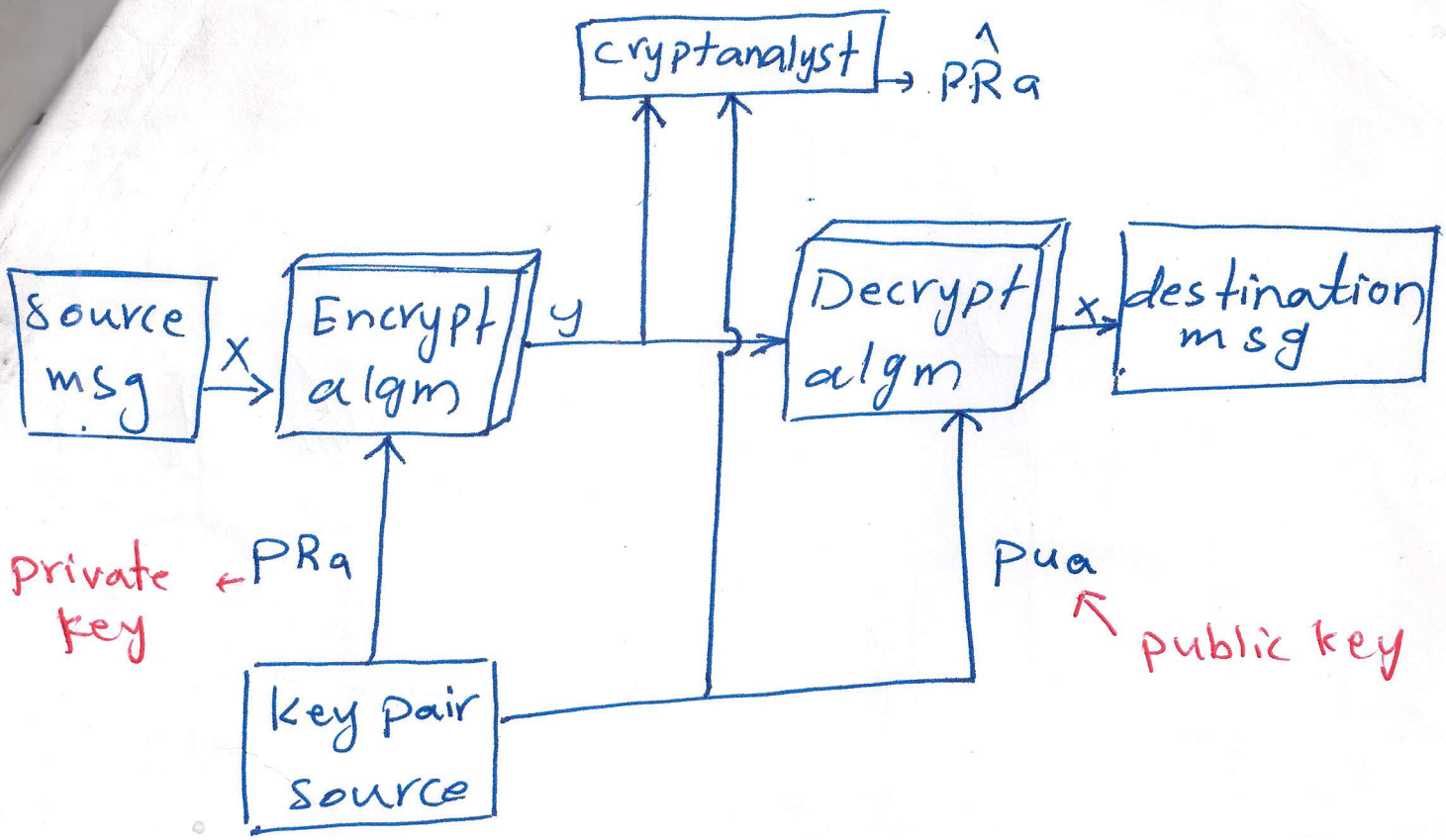
- Encryption algm:- Perform transformation on the plain text.

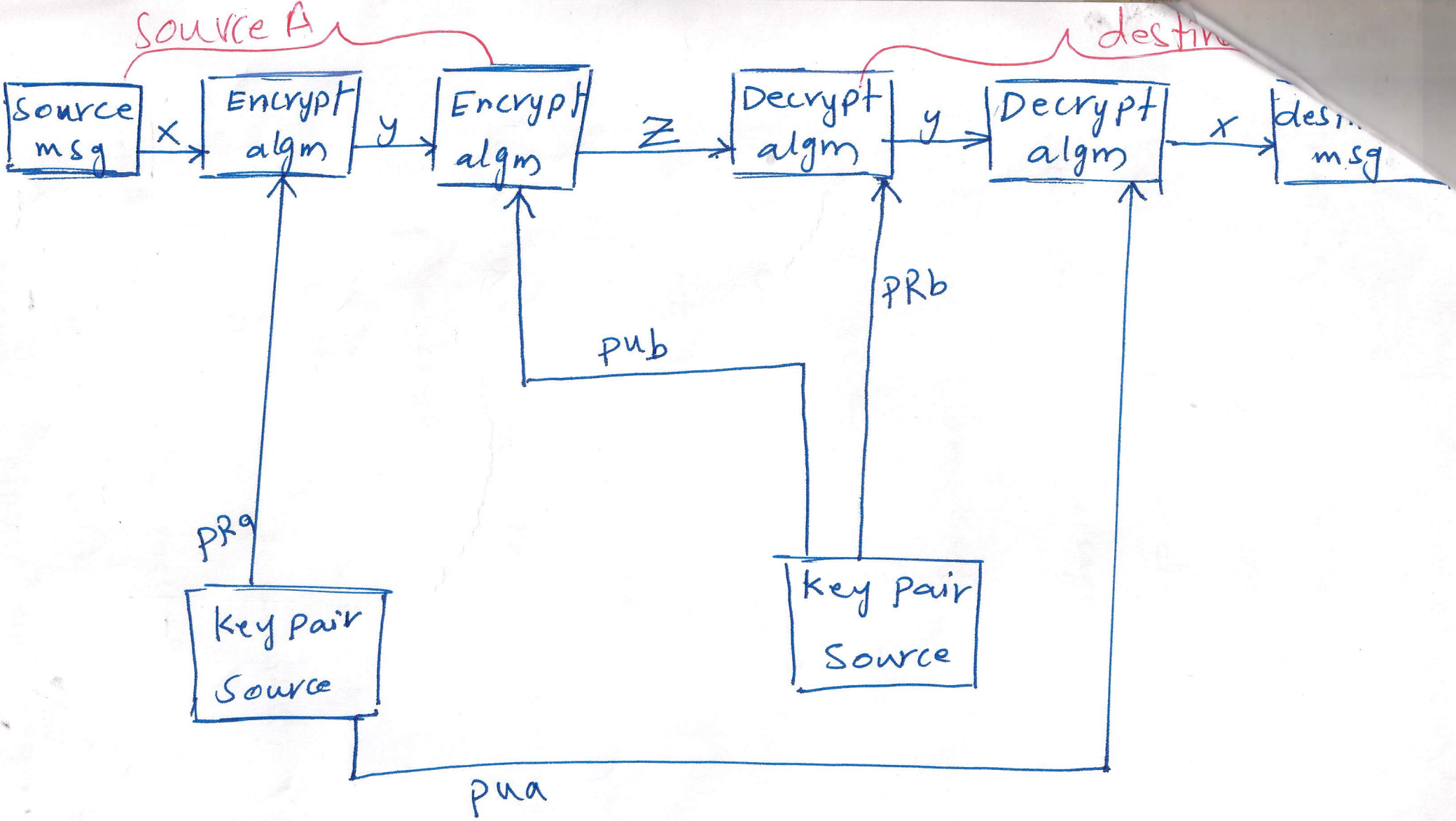
- public & private key: A pair of keys have been selected one for Encryption and ~~other~~ for decryption.

- cipher text:. scrambled message produced as o/p.

- Decryption algm:- the algorithm accepts the cipher text with matching key and produces ge. original plain text.

ublic key crypto system authentication"





" public_key cryptosystem authentication & secrecy "