# Blind Signature Based on RSA and Elgamal

Ashutosh Sharma (M120467CS) Pushpendra Singh (M120469CS)

Blind signature is the signing scheme where signer don't know the content of the message he/she is signing. It has vast applications in future application like digital cash, E-voting. We implimented blind signature in RSA and Elgamal using Python language. RSA blind signature scheme is quite easy to impliment but it is prone to RSA blinding attack and also, if the message is same user gets same signature every time. In Elgamal blind signature we use a random parameter which changes the signature every time. In our implimentation blind signature using Elgamal can be used as normal signature scheme if we take the value of blinding factor as 1.