Alice	Bob
Public key : Pu(A)	Public key : Pu(B)
Private key : Pr(A)	Private key : Pr(B)

M_1 $M\_1^{E\_K}$ $C = M\_1^{E\_K} \text{ Mod } Pu(B)$

The message from Alice would be sent using RSA encryption

Alice encrypts with bobs public key and bob decrypts it with his private key

M_3 $M\_3^{D\_K}$ $m = M\_3^{D\_K} \text{ Mod } Pr(B)$

if Alice encrypts it with her public key and send it to bob with her private key bob then can decrypt it with knowledge that it came from Alice

M_2 $M\_2^{E\_K}$ $C = M\_2^{E\_K} \text{ Mod } Pu(A)$

M_2 $M\_2^{D\_K}$ $m = M\_2^{D\_K} \text{ Mod } Pr(A)$