Programming Assignment (Due date 23/07/2021, 5:00 PM)

1. Implement message authentication and confidentiality by using S-DES (Simplified DES) and RSA.
   A. (5 marks) Implement S-DES
   B. (2.5 marks) Implement CBC-MAC; let us call it HCBC.
   C. (5 marks) Implement encryption, decryption using RSA
   D. (2.5 marks) Implement message authentication and confidentiality using above cryptographic schemes.
   Let k be a symmetric key used for S-DES and (s,p) be the public and secret key for RSA.
   Alice will send $Enc_k(M||Enc_s(HCBC(M)))$
   Bob will check $Dec_k(Enc_k(M'||Enc_s(HCBC(M))))= M'||Enc_s(HCBC(M))$
   $Dec_p(Enc_s(HCBC(M)))=HCBC(M)$
   Compare HCBC(M')==HCBC(M)

   Important Points:
   1. Implementation must be done in C language.
   2. A zip file will be submitted by sending an email to the email id *mrityunjay.singh@hyderabad.bits-pilani.ac.in*. The zip file must be named as STUDENT-NAME_STUDENT-ID.
   3. The zip file must contain only *.c, *.h and make files. No other files will be allowed in your zip folder.
   4. Copied code will be penalized heavily.