DES
Cipher system consists — Rounds

RSA : e= n= private key = —

- A signed statmet by a trusted authority ----

- security goal of ensuring that a communication arrives at recep in form of identical ----

- Property of hash hard to find msg hashed to given num ---

- Security goal ensures data can be read only in intended rec ----

- mention two block modes allow block cipher encr func calls to be made before the data available

TF : digital signature can be verified using sender's public key

- Ceaser Cipher is Poly alphabetic subst

- Properly used, a MAC provide both Confidentialy integrity

- Assymetric : diff. keys used Enc & dec

Which DES is used operating short data

= num unique substit boxes in DES after 48 bit XOR (8, 4, 6, 12)

- roundkey is — bit, Round input —

- provide one-time session key two parties

4] difference:
1- block cipher & stream cipher
2- active attacks & Passive
3- diffus & confu
4- monolalphabetic & Poly
5- Stegnog & Encr
6- SSL Connec & SSL sessi

5] Vigennote

6] C3 erro 5th howmany affected
1- 16-bit CFB 2- 8-bit OFB

7] SSL protocol sketch

operations performed	serurity services does provide
SSL record Proto	
SSL Hand shake	
SSL Alert	
SSL change cipher spec	

diff bet SSL Con & SSL Sess

8] Malicous SW type	descrip

Phases of Virus

recurm certificate issud
Public key sketch

9] search hash func req : desc
types of attacks
draw one round of DES