Unit — V

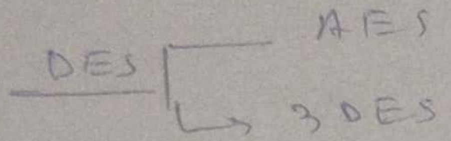
(1) Cryptography →

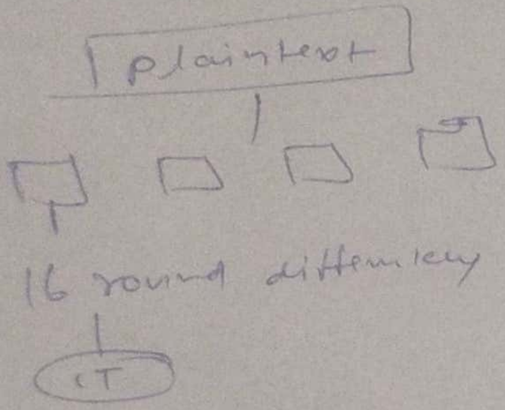
~~Ata~~ plain text को कुछ algoritham का use करके cipher text मे convert करना cryptography कहलाता है

Symmetric key (same key) private key

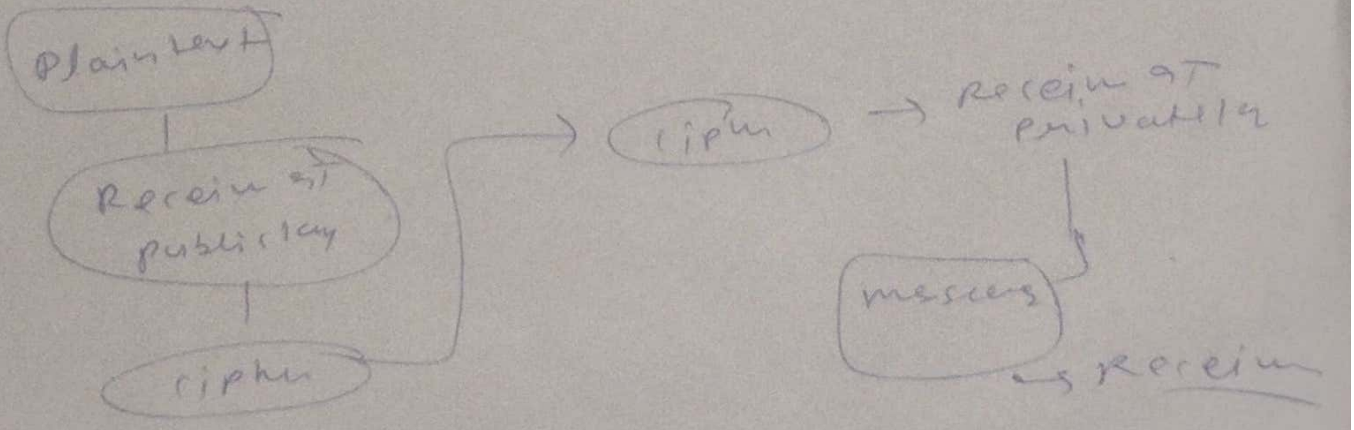
plain text को same key से encrypt करते है फिर samekey का use करके decrypt करते है।

DES, AES, 3 DES.



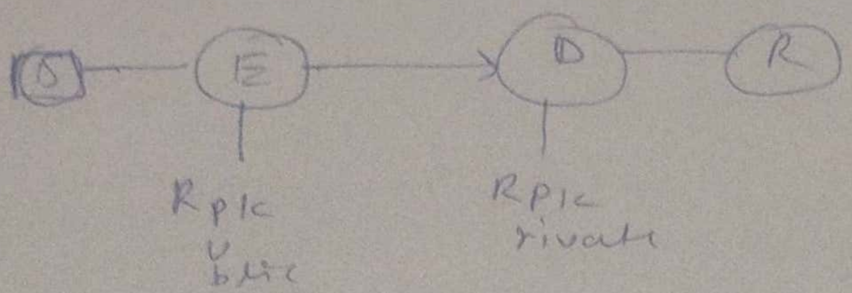


Asymmetric key (2 key)

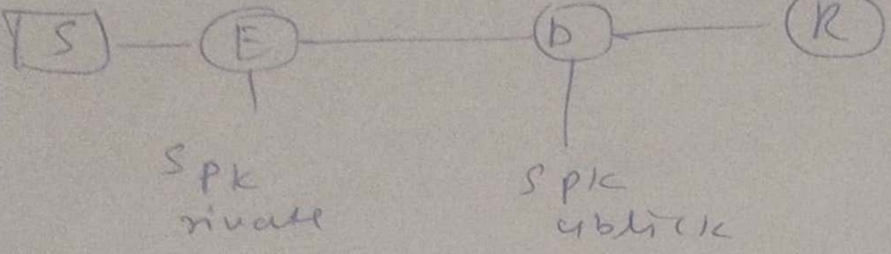


RSA

confidentiality

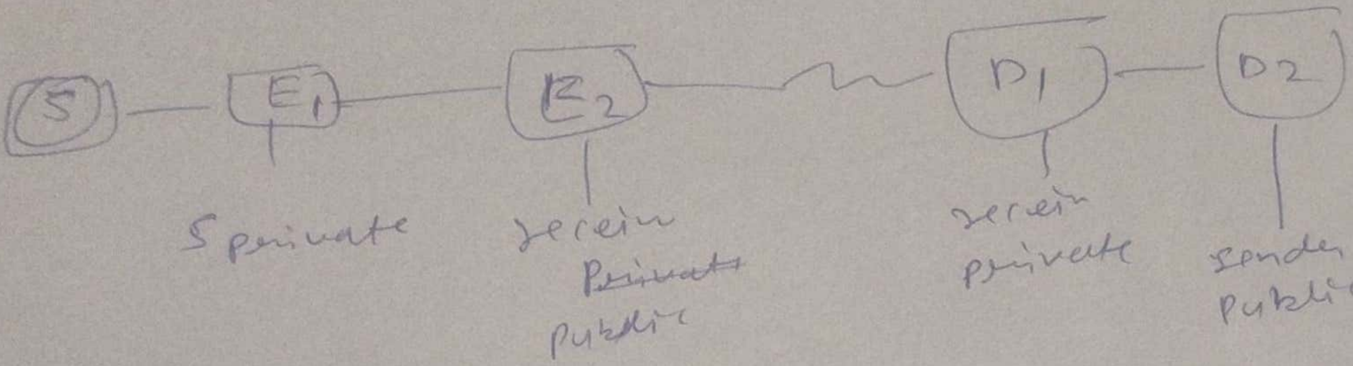


authentication.



confidentiali

authentias



RSA

① 2 large ~~numbers~~ prime numbers p and q and calculate $n = p \times q$, and $\phi n = (p-1) \times (q-1)$

② mod करो ê, $e \times d \bmod \phi n = 1$

③ e and n public key, and d as private key.

$c = p^e \bmod n$; ~~only~~ $p = c^d \bmod n$

$c = 5^{13} = 26 \bmod 77$

$c = 26$

$=$

$26^{37} =$

$5 \bmod 77$

plain 5