- (1) select two large prime num. "p" & "a"
- (11) calculate n=p\*9
- La (m) abulate of (n) = (P-1) \* (a-1)
  - (iv) choose value of e 1  $\langle e \langle \phi(n) \rangle$  and  $ged(\phi(n),e) = 1$
  - (V) calculate d= = mod d(n)
  - =) ed Mod (n) =1 (vi) public key = {e,n} (vii) private key = {d,n}

Breightion: C=Momodon

M=no, of plaintent will begiven in order

Series mell

18/4 count that

e->ciphesterol

to he into I The The I To the Life to

Decryptions M= d mod n

Let, P=3,9=11 71 = pq = 3\*11 = 33· . · · · · (9-1) (9-1) φ(a) = 2\*10 = 20 1<7420 So, let e= = as and ged (7,20)=1 Now,  $d = e^{-1} \mod \Phi(n)$ de = 1 mod & (n) -> de mod &(n) = 1 20-)24 7\*d= 1 mod \$(0) 40-741 (7\*d) mod 20=1 (: d=3) multiplicative inverse of 7 \* multiply 7 with such a number conds remainder will 1 extra than the multiples like: 20, 40,60 > (7×3) +21 mod 20 =1, like this way. Public Key = {e, n3 = & {7,33} since e=7, d=3 private key = {d a 3 = {3,33} Let, # M= 34 c= Memodn = 31 mod 33 = 4 | 31 mod 332 31 Encomption! 312 u 33=4 314 n 33 2 16 M= comod on Decomption; B1X4X16) mod 33 = 4 = 43 mod 33 = 31

Mod

\* 23 mod 30 でかっ はずむ - ゴザー = 12-167 1 30 = 17 or late or and in = 1500 mod 30 = 1 mod 30 (1) / (1) / bom to = 15 (00)/ = Ampliformation (10) to borne to -= -242 mod 243 (6) 1 Long 1 - 141. 23 mod 287 = 1891 = 25 born (145) 110 step 1 = (2-3) 10 = 10 110 mod gillons Step 2! 13 mod 227 = 13 13 4 257 = 169 1 X138 2 287 2(148) = 9: 21904 -287 -76×287 1316 and 287 = (92) = 141 SP3: (13×169×148×141) mod 287 (New Man Cashed at 1 - 48A

P=17, 9=14 K n= Pq = 17×11 = 187 \$ \$60) = (P-1)(9-1) = 16×10 > 160 e (ged, ged (06), e) =1 (xex 0(n) let, e = 7 & gcd (160,7) = 1 Noo, de = 1 mod p(n) => de =mod p(n) = 1 => (d\*=7) mod 160 = 1 1. d=23 Since e=7, d=23 RK = Sen3 = {7, 1873 PAK = {4n} = {23,1873 Monod or who born 28 mod 187 = 11 M = cd moda = 11<sup>23</sup> mod 187 Deer

z 88

carte = hash(RbE)

Bue Signedesta cesal A = hoch (PubA) PULA PULA 03P e (costA, RILO). e (cook BANDA) 2 signed coats d (Signed cool pa Ruber) PUSCA zcentB = Hook PJB) RILCA cord CA = hach (Rub CA) signed choost = e (contrA, PVRCA) d(Signed CA cost, Rub CA) = conf CA

## Alfealo

- Denial of Service (Dos) & (DDO) Distoilabled Denial of service cellack:
- => A denial of service attack overcohelmes a systems resurce so that it cannot respond to service requests.
- A DDOS attack is also on systems resources, but it is launched from a large no. of other host muchines that are infected by makings software controlled by the attackerc.

There are different types of Dos and Dos attacks Tep syn flood adlack: [molania]

In this attack, an attacker exploits the use of the buffer space during a tep session handshake.

## Teardrop aldeak;

This cause the length & & fragmentation offset fields in sequential IP packets to overclap one another on the attacked host. If users don't have partches to protect against the Dos attack, disable SMBv2 and block ports 139 and 445.

\* Smurchaldeak.

This attack involves using IP spoofing & the TOMP to saturate a target metwork with landfie. B protect you need to disable IP-directed broadeast at the routers. This will prevent echo Temp request at the network davices Another option is configure the end systems.

This uses IP packet to ping a larget system with an IP size over the max of cs, 535 bytes. Ping of death attacks can be blocked by using a fireful that will chack fragmented IP prickets for man ene

\*(2) Man-in-the-middle aldockt. It occurs when a hacker inserts itself bet the

communications of a client and a server. The is vulnerable to RSA algorithm like it can allack RSA by session hijacking like this wayt

- a) A client connects to a server.
- 5) The odtackers computer goins control of the cherk
- a) the attackers computer lisconnects the elient from the sowete.
- of the affections computer replaces the clients If address with its own IP and spools the clients sequence numbers.
- e) The attackers computer continues dicitog with the server and it believes it is still communicating with the client.

Popaevent sonsider using a VAN and look for ATTIPS at the beginning of each UPL.

And PVD solves it by generating SSL certificates on coebsites to that visitors know they are sending infects a securite contribe treeiphent, Ds.

3) Phishing & Spearz Phisihing HI as Marine Aby (6)

Phishing is the practice of sending anails that appeare to be from forwstend sources with the goal of gaining personal info.

Speare is largeled type of autily it recomments

the targets and other attacks of abording into

4) Resourced Attack:

Because possiboreds arre most commonly used mechanism so it can be done in brante force and dictionary allack. To prevent this you need to implement an account lockout policy.

x 5) sal Direction Allach!

It is which is specific to sat databases. To prevent set injection ensurce that the web dev. have properly sanitize all inputs.

6) Bavesdropping Addackt It occurs knough the interception of network douther

X7) Birathday Atlack! The made against hash algorithm that are used to verify the integrity of a mag, softwark or digital signatura.

Malicious softwarze can be degraphed as unwanted softwarze that is installed in your system without your consent. \* 89 Makoarce Altrokt

8 Boffer ovareflow Attack # 31/9 5100092 & Builderidg (8 Dt typically involves in programming languages and overcurating the bounds of the buffers they exist on. (10) Social Engineering Attent: It impacts heavily on human intercetion and often involves manipulating people into breaking normal security expendences. securate procedures. incolourisms so it can be done in braile force and dichionary alkack. To prevent-this goined to implement an account locked policy. 3) sal Injection Ablack! THE IS WHICH IS SPECIFIC TO SEL JAKEDOSES To prevent set lijection encourse. That the web for House propered samilies all impoles. (3) Paverdondhing Affecti The second of mileson of the Reserve of malecond for the X D Bire Hiday Altook! at been stored for sens a go thing the one of the stored to Hard HA syttodel-1 (3/8 Maticions software can be described as unacovoled software I mences stood Quarties mestage stoot in Latherkenn it Just

## Kenberros

ockett 11 off c - olient AS > authentication server V -) SOCVOR IDc -> identifier of user on C DDV -> identifier of V Pe -> passwork of user on a ADe -> network address of e KV -> secret enoughtion key sharred by AS&V. 2) AS VOTAPIES USOR access right in destabase someodes TEXT & session key. Perolls wire VCIE Once Por energipled using ked Auth Request 767 SOTHER i) user logs onto decived from nicket-rsession key user's password workstation and treg. Used on host. Request service grante 3) World of thon prompts user prostodearypt Pichot-15000 kg mooning mag then send soniae ticket and authenticodor that contains users name, na , and time to Tos 4) 765 Leaght tick of & Request service Once por sovice authenticator, verifics request and then creates taked for 5) Workstation sends ticket and authenticator to host. travested application Schrez server. 9 whentication 6) Host vertifies that and then grant access to sorvice . If makeral Host outh is required, application returns an author SESVEZ

Vorsion 6 Massage Exchange! 1) C->AS PDc 11 PDtgs 11 731 2) AS -> C E (Ke [Kentgs 11 ID/43 11 B2 11 Lifetime 2 Micketys])
Ticketings = E (Kys, [Kentgs 11 IDe 11 ADe 11 ID/43 11732 11 Lifetime]) 2) C-> PEZS ID 11 Mickelyge 11 Authenticatorce 4) PBS JC & (ke, kgs [Ke, V 11 IDV 11 Psy 11 Picket V]) Ticketigs = E(Kigs, [ke, Igs 11 DDe 11 ADe 11 TDigs 11 762 11 Lifetime 2] Rickety = E(Ky, [Ke, VIIIDe 11ADe 112DV 11784 11 Lifetimey ) Authenticolorse = E(Ke, tgs, [IDe11ADe11733]) 5) c-> V Tickety 11 Authenticatorice

6) v-> c P (Ve, v, [755+1]) Tickely = 2 (ky, [key 11 TDe 11 ADe 11 PDv 11 Psy

Nickely = 2 (ky, [key 11 TDe 11 ADe 11 PDv 11 Psy Authenticatore = E(Ke,v; [IDe 11 ADe 11755])

and a section highless

request and then

" Hotal cohoso

The fact is a south

toll - sittings built (2

haloide eligen middle direct 12

e field the pulse of him from from

4 Big Boothor (the government employer) # CORPA -> Children's Online Ponacy Protection Act oplains under age of 13. This stated purpose is to product children from micro-tengetting by advartises and to minimize the potential for content with daysous individuals through that recome, e-mail & bolletin boards by involving parcents in kids online activities.

# GIDPP -> Greneral Deda Prodection Regulation.

It can be considered as worlds strongest set of data protection rules, which enhances how the people can access information about them I limits on what expossations can do with personal data.

He first principle for altrical treatment of posonal information is a

- Desportant Consent

  Despor
  - 2 To give people a choice about whether decta collected about them is distensisted to other businesses on org. & is used to seed sond

Himosis (car shows on a souther , 17 of the

Under an opt-in policy! to Personal information is not distantated to other tousinasses on organizations un less the consumous has explicitly checked a box orz signed a foren. 1) collect only the data needed 2) Interior people when date about them are being collected a) what is collected b) how it will be used Ist and Iranstor of their data to other people. 9) Provide Arronger protection for sensitive data. 3) keep data only as long as needed. 6) Maintain accurracy and security of data. 7) Provide a way forz people to across and connect -their storced data a) Licence grant & restanting # Brooklows & conditions; 10) Copyright 1) Responsibility 11) Intellactual property rights e) Securing your Pin and Olp 12) Conitations 3) Mislakes John 13) Persona Halaprotection 4) Sowkes & Fres 14) Access pormiseion 3) Acknowledgment B) communication with you 15) Indemnification 16) Other Rights & Limitations Customers support Representations & warmonties 17) Seaunity