RSA

(i) Select two large prime num. "p" & "q"

(ii) calculate $n = p * q$

(iii) calculate $\phi(n) = (p-1) * (q-1)$

(iv) choose value of e

$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$

(v) calculate $d \equiv e^{-1} \bmod \phi(n)$

$\Rightarrow$ i.e. $ed \equiv 1 \bmod \phi(n)$

$\Rightarrow ed \bmod \phi(n) = 1$

(vi) public key $= \{e, n\}$

(vii) private key $= \{d, n\}$

Encryption:- $c = M^e \bmod n$

M = no. of plaintext will be given in block $\therefore M < n$

$c \rightarrow$ ciphertext

Decryption:- $M = c^d \bmod n$

20) 21(1
20
1

Let, $p=3, q=11$

$n = pq = 3*11 = 33$

$\phi(n) = 2*10 = 20$ $\quad \because \phi(n) = (p-1)(q-1)$

So, let $e=7$ as $1 < 7 < 20$ and $\gcd(7,20)=1$

Now, $d \equiv e^{-1} \bmod \phi(n)$

$de \equiv 1 \bmod \phi(n) \rightarrow de \bmod \phi(n) = 1$

$7*d \equiv 1 \bmod \phi(n)$

20→21
40→41
60→61

$(7*d) \bmod 20 = 1 \quad (\because d=3)$

↓ multiplicative inverse of 7

* multiply 7 with such a number which's remainder will 1 extra than the multiplers. like: 20, 40, 60 → 21, 41, 61

$(7*3) \Rightarrow 21 \bmod 20 = 1$, like this way.

since $e=7, d=3$

public key $= \{e, n\} = \{7, 33\}$

private key $= \{d, n\} = \{3, 33\}$

Encryption: $C = M^e \bmod n$

$= 31^7 \bmod 33 = 4$

Decryption: $M = C^d \bmod n$

$= 4^3 \bmod 33$

$= 31$

Let, $M = 31$

$31^1 \bmod 33 = 31$

$31^2 \bmod 33 = 4$

$31^4 \bmod 33 = 16$

$(31 \times 4 \times 16) \bmod 33 = 4$

Mod

* $23^3 \bmod 30$

$= 12167 \mid 30$

$= 17$

* $31^{500} \bmod 30$

$= 1^{500} \bmod 30$

$= 1 \bmod 30$

$= 1$

* ~~$242 \bmod 243$~~ 329

* $13^{23} \bmod 287 = 181$ (17)

16 8 4 2 1

Step1: $(23)_{10} = 10111$

Step2: $13^1 \bmod 287 = 13$ ✓

$13^2 \quad " \quad 287 = 169$ ✓

$13^4 \quad " \quad 287 = 148$ ✓

8157307721

$\times 13^8 \quad " \quad 287 = (148)^2 = 92$ ✗

21904 ÷ 287 − 76 × 287

$13^{16} \bmod 287 = (92)^2 = 141$ ✓

Step3: $(13 \times 169 \times 148 \times 141) \bmod 287$

$= 184$

#1) $P = 17, q = 11$

$n = pq = 17 \times 11 = 187$

$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

$\gcd(\phi(n), e) = 1 \quad 1 < e < \phi(n)$

Let, $e = 7$ & $\gcd(160, 7) = 1$

Now, $de \equiv 1 \bmod \phi(n)$

$\Rightarrow de \bmod \phi(n) = 1$

$\Rightarrow (d * 7) \bmod 160 = 1$

$\therefore d = 23$

Since $e = 7, d = 23$

$PU_k = \{e, n\} = \{7, 187\}$

$PR_k = \{d, n\} = \{23, 187\}$

Encr: $C = M^e \bmod n$

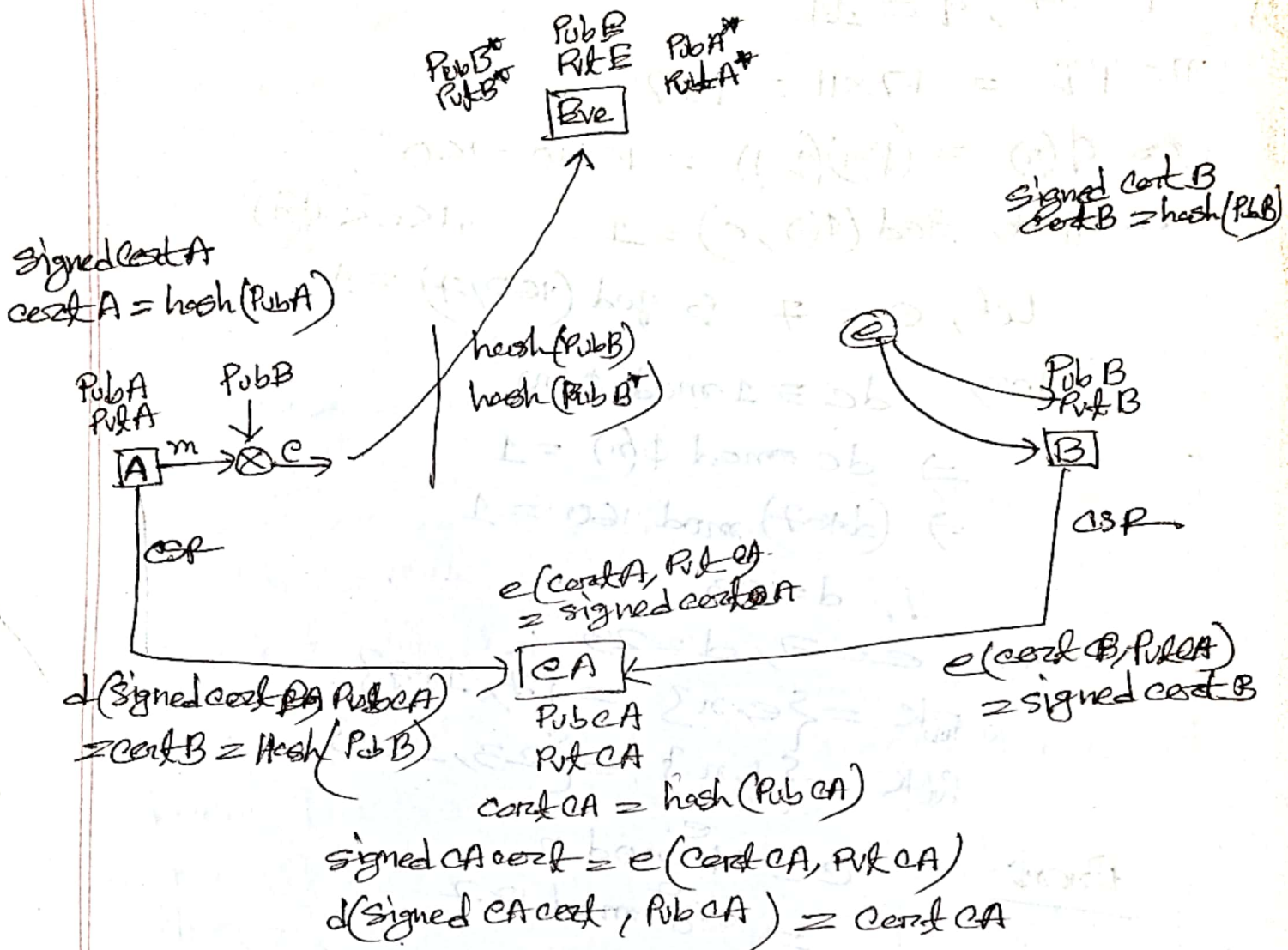
$= 88^7 \bmod 187$

$= 11$

Decr: $M = C^d \bmod n$

$= 11^{23} \bmod 187$

$= 88$


cert E = hash(Pub E)
Pub E
Pub B*
Pub A*
Priv E
Priv B*
Priv A*
Eve
Signed cert B
cert B = hash(Pub B)
Signed cert A
cert A = hash(Pub A)
hash(Pub B)
hash(Pub B*)
Pub A
Priv A
Pub B
A
m
C
e
Pub B
Priv B
B
CSR
CSR
e(cert A, Priv CA)
= signed cert A
CA
Pub CA
Priv CA
d(Signed cert B, Pub CA)
= cert B = Hash(Pub B)
e(cert B, Priv CA)
= signed cert B
cert CA = hash(Pub CA)
signed CA cert = e(Cert CA, Priv CA)
d(Signed CA cert, Pub CA) = Cert CA

Attacks

1) Denial of Service (DoS) & (DDoS) Distributed Denial of Service attack:-

⇒ A denial of service attack overwhelmes a systems resource 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 machines that are infected by malicious software controlled by the attackers.

There are different types of DoS and DDOS attack &

TCP SYN flood attack:-

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

Teardrop attack:

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

Smurf attack:

This attack involves using IP spoofing & the ICMP to saturate a target network with traffic. To protect you need to disable IP-directed broadcast at the routers. This will prevent echo ICMP request at the network devices. Another option is configure the end systems.

Ping of death attack:

This uses IP packet to ping a target system with an IP size over the max of 65,535 bytes.

Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for max size.

** 2) Man-in-the-middle attack:

It occurs when a hacker inserts itself betn the communications of a client and a server.

It is vulnerable to RSA algorithm like it can attack RSA by session hijacking like this way:

a) A client connects to a server.
b) The attackers computer gains control of the client
c) the attackers computer disconnects the client from the server.
d) the attackers computer replaces the clients IP address with its own IP and spoofs the clients sequence numbers.
e) The attackers computer continues dialog with the server and it believes it is still communicating with the client.

To prevent consider using a VPN and look for 'HTTPS' at the beginning of each URL.

And PKI solves it by generating SSL certificates on websites so that visitors know they are sending info to a secure ~~website~~ recipient, DS.

3) Phishing & Spearc Phishing:-

Phishing is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal info.

Spearc is targeted type of activity it research into the targets and then attacks.

4) Password Attack:-

Because passwords are most commonly used mechanism so it can be done in brute force and dictionary attack. To prevent this you need to implement an account lockout policy.

* 5) SQL Injection Attack:

It is which is specific to SQL databases. To prevent SQL injection ensure that the web dev. have properly sanitize all inputs.

6) Eavesdropping Attack:

It occurs through the interception of network traffic

* 7) Birthday Attack:

Its made against hash algorithm that are used to verify the integrity of a msg, software or digital signature.

* 8) Malware Attack:

Malicious software can be described as unwanted software that is installed in your system without your consent.

* 9) Buffer overflow Attack:

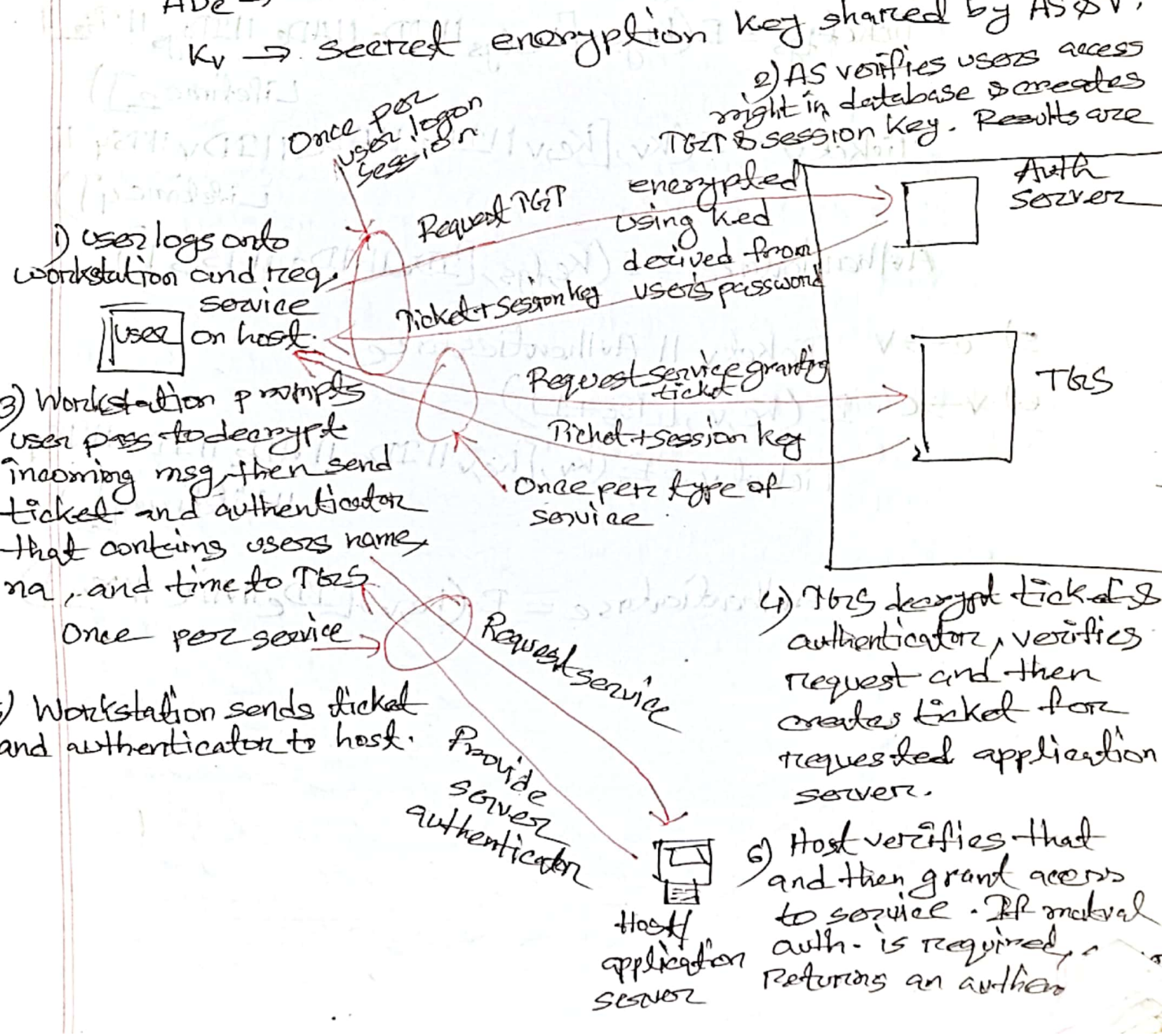
It typically involves in programming languages and overwriting the bounds of the buffers they exist on.

* 10) Social Engineering Attack:

It impacts heavily on human interaction and often involves manipulating people into breaking normal security procedures.

Kerberos

C → client
AS → authentication server
V → server
ID_C → identifier of user on C
ID_V → identifier of V
P_C → password of user on C
AD_C → network address of C
K_V → secret encryption key shared by AS & V.



Version 4 Message Exchange:

1) $C \rightarrow AS \quad ID_c \| ID_{tgs} \| TS_1$

2) $AS \rightarrow C \quad E(K_c[K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Lifetime_2])$

3) $C \rightarrow TGS \quad ID_v \| Ticket_{tgs} \| Authenticator_c$

4) $TGS \rightarrow C \quad E(K_{c,tgs}[K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_c \| AD_c \| TS_3])$

5) $C \rightarrow V \quad Ticket_v \| Authenticator_c$

6) $V \rightarrow C \quad E(K_{c,v}, [TS_5 + 1])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_c \| AD_c \| TS_5])$

Law

Big Brother (the government/employer)

COPPA → Children's Online Privacy Protection Act.
Ordering FTC Under age of 13. This stated purpose is to protect children from micro-targetting by advertisers and to minimize the potential for contact with dangerous individuals through chat rooms, e-mail & bulletin boards by involving parents in kids' online activities.

GDPR → General Data Protection Regulation.
It can be considered as worlds strongest set of data protection rules, which enhances how the people can access information about them & limits on what organisations can do with personal data.

Principle for Data Collection & Use :-
The first principle for ethical treatment of personal information is :-

1) Informed Consent
   (i) what information they are collecting?
   (ii) How they will use it?

2) To give people a choice about whether data collected about them is distributed to other businesses or org. & is used to send ads or not.

Under an opt-in policy:-

* Personal information is not distributed to other businesses or organizations unless the consumer has explicitly checked a box or signed a form.

1) Collect only the data needed
2) Inform people when data about them are being collected
   a) What is collected
   b) how it will be used
3) Offer a way for people to opt out from mailing lists and transfer of their data to other parties.
4) Provide stronger protection for sensitive data.
5) Keep data only as long as needed.
6) Maintain accuracy and security of data.
7) Provide a way for people to access and correct their stored data.

Bkash terms & conditions:-

1) Responsibility
2) Securing your Pin and Otp
3) Mistakes
4) Service & Fees
5) Acknowledgment
6) Communication with you
7) Customers support
8) Representations & warranties
9) Licence grant & restrictions
10) Copyright
11) Intellectual property rights
12) Limitations
13) Personal data protection
14) Access permission
15) Indemnification
16) Other Rights & Limitations
17) Security