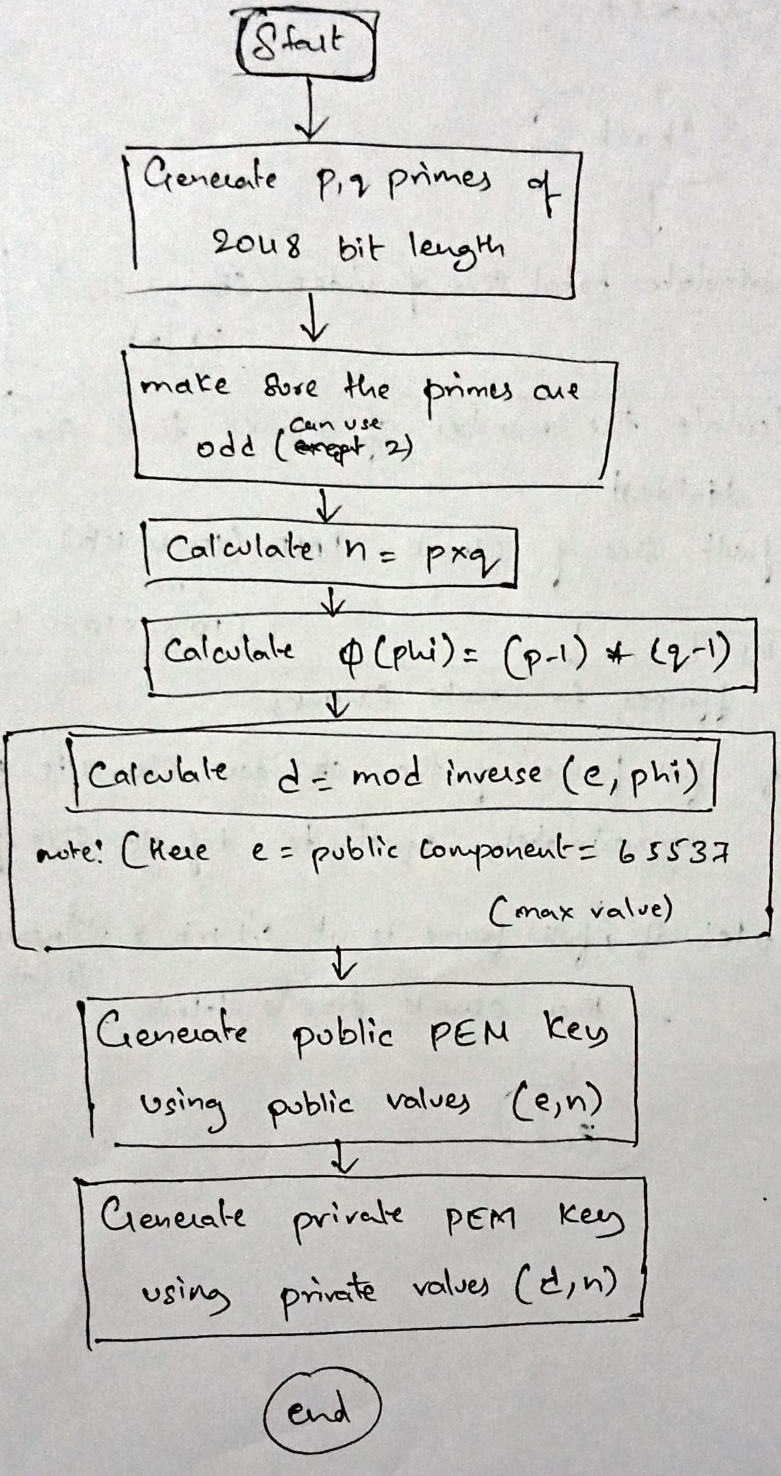
Key generation


Start
Generate p,q primes of 2048 bit length
make sure the primes are odd (~~except~~ can use 2)
Calculate n = pxq
Calculate ϕ (phi) = (p-1) * (q-1)
Calculate d = mod inverse (e, phi)
note: (Here e = public component = 65537 (max value)
Generate public PEM key using public values (e,n)
Generate private PEM key using private values (d,n)
end

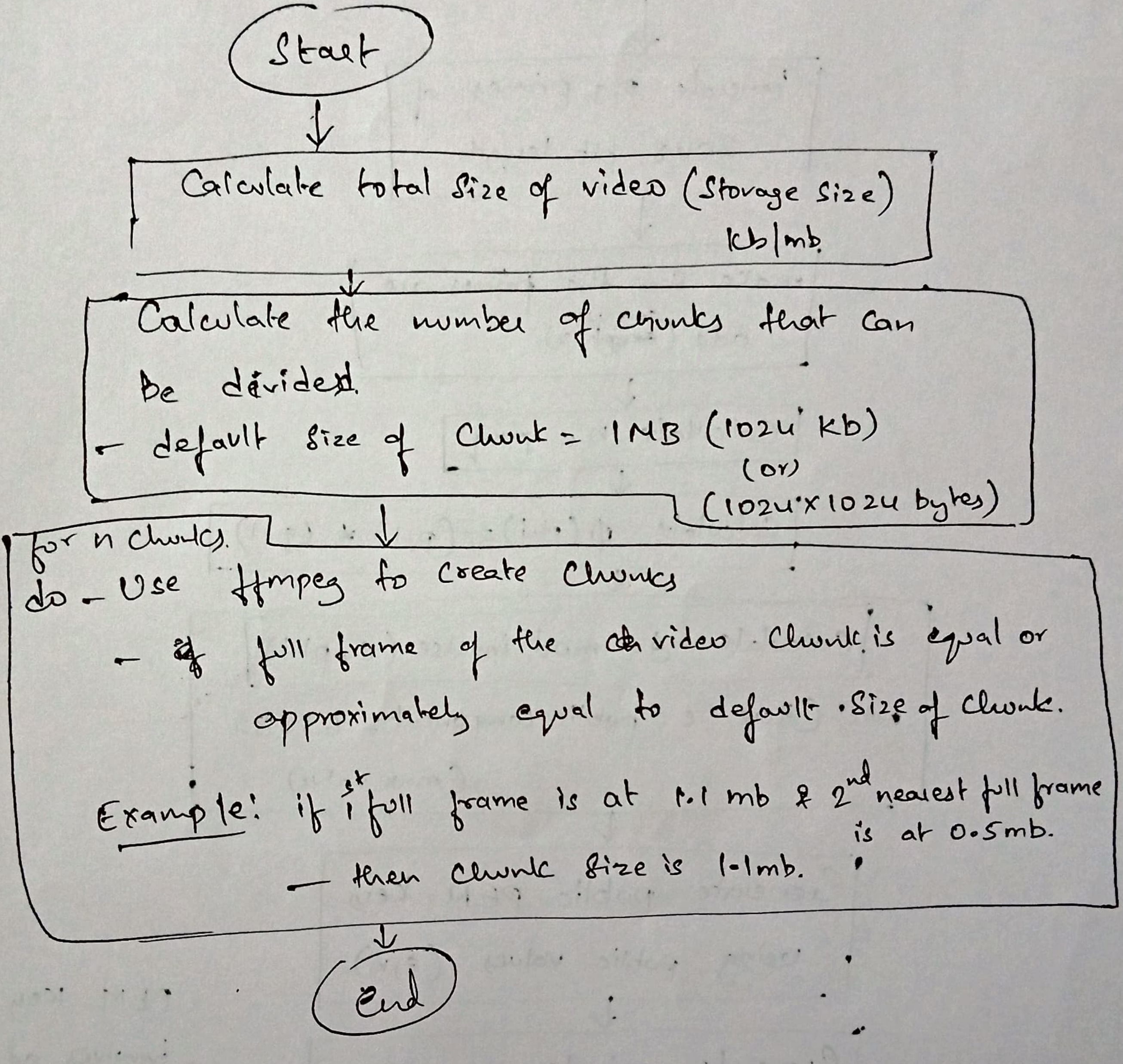
PEM key generation involves additional data appended & prefixed
<- BEGIN PUBLIC KEY->
<- END PRIVATE KEY->

final:

publickey length = 2048
private key length = 2048.

Encryption

Chunking



Start

Calculate total size of video (Storage size) kb/mb

Calculate the number of chunks that can be divided.

- default size of Chunk = 1MB (1024 kb) (or) (1024 x 1024 bytes)

for n chunks.
do - Use ffmpeg to create Chunks

- ~~if~~ full frame of the ~~ch~~ video Chunk is equal or approximately equal to default Size of Chunk.

Example: if 1st full frame is at 1.1 mb & 2nd nearest full frame is at 0.5mb.

- then chunk size is 1.1mb.

End

Encryption.

For first Chunk; & rest of Chunks.

input ! ~~first~~ first 16 Bytes of Chunk video

① Generate AES Key with ECC equation.

ecc equation= $y^2 = x^3 + ax + b$.

$y = \sqrt{x^3 + ax + b}$.

ecc-eq = $\sqrt{x^3 + ax + b}$.

x - random integer from windows Os cryptography API

- entropy is from OS

a= first 16 bytes of first video chunk. for first video chunk

for rest of chunks a= the key generated during ~~previous~~ encryption of previous chunk.

B= integer casted from Concatenated String of System timestamp;
process id,
machine id

Hash(base 64 encoded (ecc number)) → aeskey.

sha 256 ∴ size of aeskey = 256.

128 bit nonce.

② cipher_aes = encrypt(video chunk data, nonce, aes key) — aes - GCM mode.

③ ~~cipher aes = cipher a.~~

encrypted_aes_key = RSA(public key, aes key).

④ Final cipher = ~~hash~~ (encrypted-aeskey + nonce + encrypted-video)

~~keys~~ .

hash(final_cipher) is appended

Decryption

Start

1. extract below from cipher chunk.
   - encrypted aes key
   - nonce
   - encrypted video
   - hash

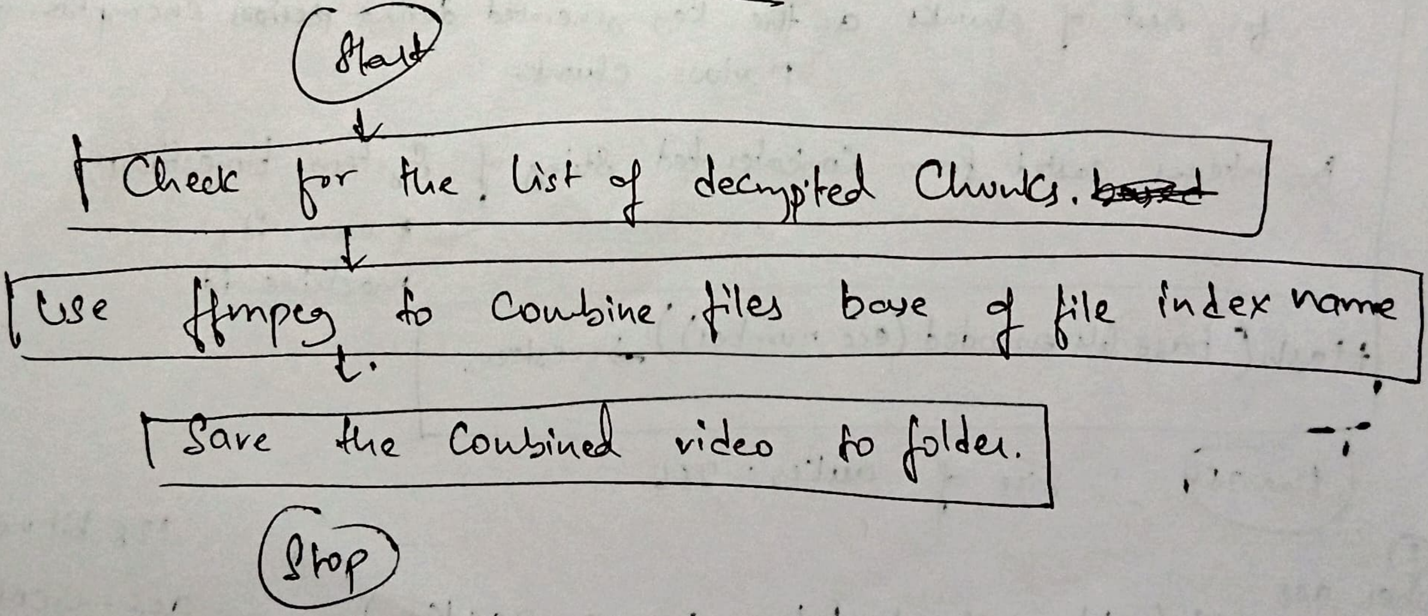
2. decrypt (encrypted aes key, private key) → aes key

3. use aes key, nonce to decrypt (encrypted video)

4. verify by calculating hash with extracted hash.

Stop

Combine Chunks



Start

Check for the list of decrypted Chunks. ~~based~~

Use ffmpeg to combine files base of file index name

Save the Combined video to folder.

Stop