Greatest Common Divisors:

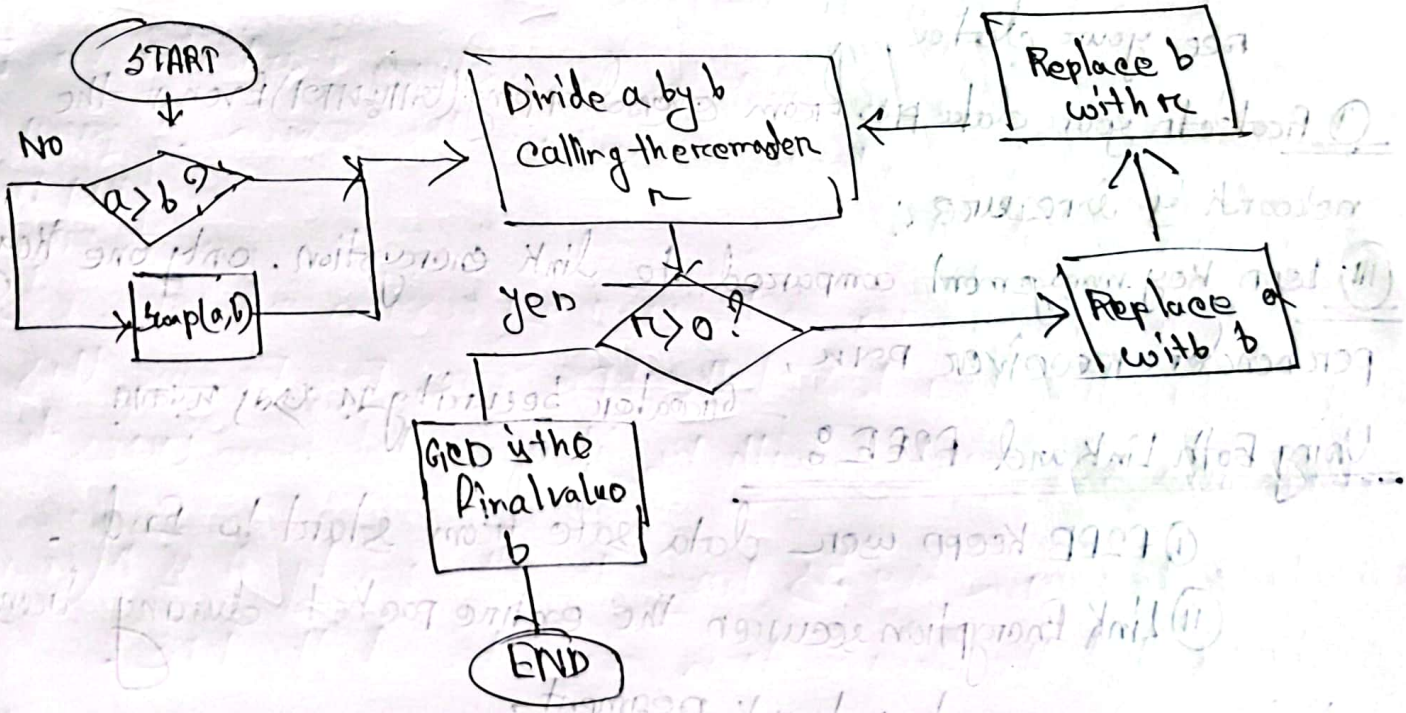
⇒ More formally the positive integer c is said to be the greatest common divisors of a and b if

(i) c is a divisors a and b
(ii) any divisor a and b is a divisor of c.

@ gcd(a,b) = gcd(|a|, |b|)
gcd(60,24) = gcd(60,24) = 12
gte gcd(a,0) = |a|

⇒ Two integers a and b relatively prime if and only if their only common positive factors is 1. This is equivalent to saying that a and b are relatively prime if gcd(a,b) = 1.

gt: gcd(8,15) = 1 → relatively prime.



→ Link Encryption secures data by encrypting and decrypting information at every node or network switch it passes through, rather just at the end points.

This ensures that all data including headers and routing information is protected

Disadvantage: প্রত্যেক Switch এ Message decrypt করতে হয় Address জানার জন্য পড়তে Header থেকে। তখন Message vulnerable হয়ে পড়ে। তাছাড়া Link এ প্রতিটির Key ব্যবহার করতে হবে.

⇒ End To End Encryption (E2EE)

→ Sender Encrypts the message
→ Message travels the network without being decrypted.
→ Only receiver can decrypt it.

Advantage: (i) Routers, switches and network operation can't see your data.

(ii) Protects your data ~~pro~~ from eavesdropping (আড়িপাতা) Even if the network is insecure:

(iii) Less key management compared to link encryption. only one key per sender receiver pair.

Using Both Link and E2EE: — Greater security এর জন্য দরকার

(i) E2EE Keeps user data safe from start to End.

(ii) Link Encryption secures the entire packet during transmission across each network segment.

[Router 1] Link Decrypt
Read Header
Link Encrypt (Again

[Router 2] Link Decrypt
Read Header
Link Encrypt.

Key Distribution:

For Symmentric Encryption both sender and receiver need to use same secret key to encrypt and decrypt message. Key must be protected from access by others.

The main challenge is sharing the key to parties. A —— B

(i) A selects a key and physically delivers it to B.

(ii) Third party select the key and physically deliver it to A and B.

(iii) If A and B have previously recently used a key, one party can transmit the new key to other, encrypted using old key.

(iv) If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

(i), (ii) practically অসম্ভব।

যদি Network node level encryption ব্যবহার করা হয় 100 Node থাকে তাহলে তো বিভিন্ন key distribute করতে হবে।

⇒ KDC (Key distribution Center) → used for key sharing easy and safe way তে.

Master Key → প্রত্যেক user এর জন্য unique. Session key/ temporary key.

↳ two levels of keys are used.

⇒ Session key usually used for the duration of a logical connection.

⇒ Session Keys are transmitted in encrypted form using a master key that is shared by the key distribution center and an end system.

⇒ For N entity session key $\frac{N(N-1)}{2}$ master key N.

⇒ যত frequently session key change করবে তত ভালো, কিন্তু বেশি frequent change করলে তত Network slow হবে কেননা Resource খরচ হবে.

Transpositi
↳ Plai
Rail Fence:
. Plain

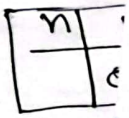
Key distribution scenario.

1) The scenario assumes that each users shares a unique master key with the key distribution center. (KDC).

2) Let assume a wishes to establish a logical connection with B and require a one time session key to protect data transmitted over the connection.

A has a master key K_a known only to itself and the KDC.

B " " " " K_b " " " " " "



The following steps occur:

① A issues a request to the KDC for a session key to protect a logical connection to B. This message includ A, B and unique identifier N1 for this transaction. which we refer to as a nonce.

Colum
plai

A should be diffi... to guess ← nonce → timestamp/counter/ random number

Ke

The KDC responds with a message encrypted using K_a.

Message includes → ① One time session key K_s.
② The original request msg including nonce.

to enable A to match this response with appropriate request.

In addition the message includes two items intended for B.
→ The one time session key K_s to be used for the session.
→ An identifier of A.

(पहला: K_b, दूसरा: Encrypt करना.)

A stores the session key for use in the upcoming session and forwards to B the information generated at the KDC for B. Because this information is encrypted with K_b it is protected from eavesdropping.

B Now knows the session key K_s, knows the other party A is A (from ID_A) and knows that the information originated at the KDC.

At this point a session key has been securely delivered to A and B and they may begin their protected exchange