Greatest Common Divisor:

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

① c is a divisor a and b.
② any divisor a and b is a divisor of c.

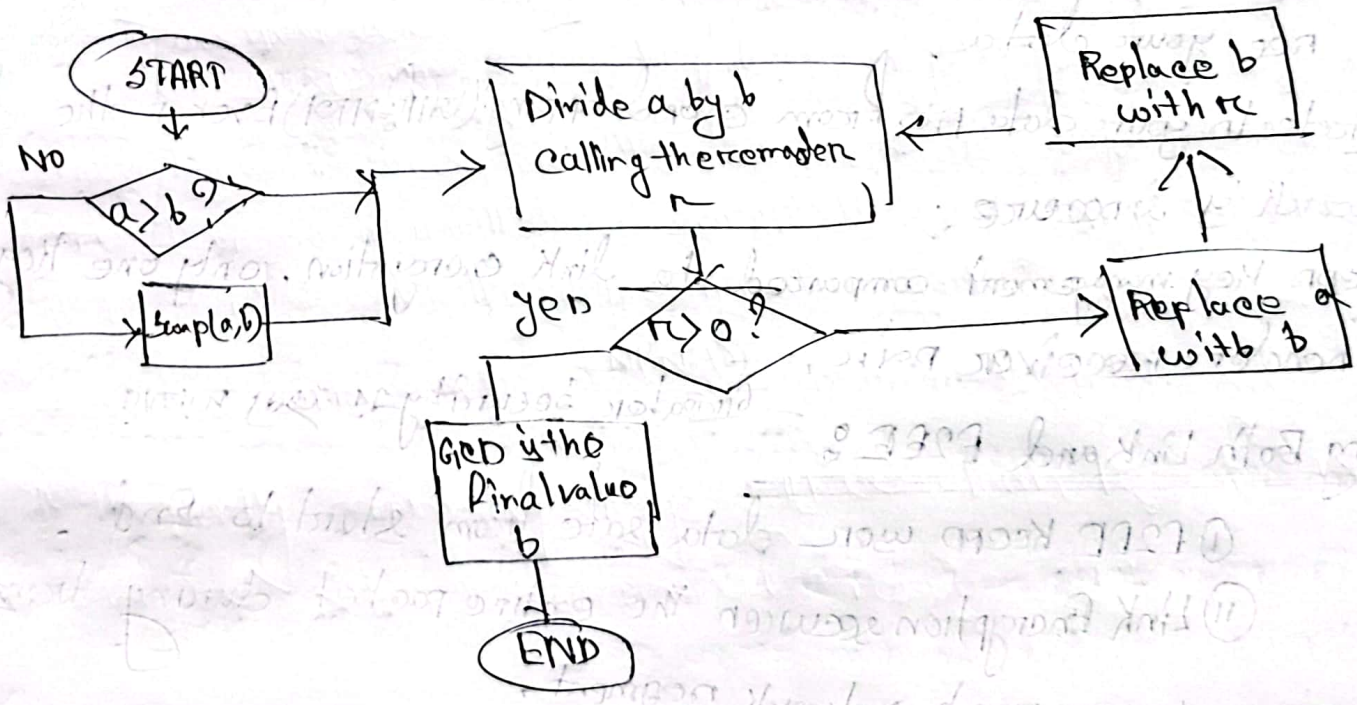
@ gcd(a,b) = gcd(|a|, |b|)

gcd(60,24) = gcd(60,-24) = 12

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.

ex: 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 ঠিকানার জন্য প্যাকেট Header খোলে। তখন Message vulnerable হয়ে পড়ে। প্রত্যেকটা Link এর ও ইউনিক Key ব্যবহার করতে হবে.

⇒ End To End Encryption (E2EE)

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

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

(ii) Protects your data 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.

CamScanner

Key Distribution:

For Symmetric 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 deliver 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
কারণ Network node level encryption ব্যবহার করলে যদি 100 Node থাকে তাহলে তাদের নিজেদের Key distribute করতে হবে।

⇒ KDC (Key distribution Center) → used for key sharing easy and safe way তে।
→ two levels of keys are used.

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

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

⇒ যত frequently session key change করবে তত ভালো, কিন্তু বেশি ঘনঘন করলে তত Network slow হবে বেশি Resource খরচ হবে।

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 include A, B and unique identifier, N1 for this transaction. which we refer to as a nonce.

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

The KDC responds with a message encrypted using K_a.

Message includes ① One time session key K_s.

② The original request message 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.

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, know 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.