operations on higher than two elements.

- Identity – For all a in G, there occur an element e in G including e · a = a · e = a.
- Inverse – For each a in G, there occur an element a′ known as the inverse of a such that a · a′ = a′ · a = e.

Abelian group

A group is an abelian group if it satisfies the following four properties more one additional property of commutativity.

Commutativity – For all a and b in G, we have a · b = b · a.

- (M4): Commutative of Multiplication – ab=ba for all a, b in R.
- (M5): Multiplicative identity – There is an element 1 in R including a1=1a for all a in R.
- (M6): No zero divisors – If a, b in R and ab = 0, therefore a = 0 or b = 0.

Field – A field F is indicated by {F, +, x}. It is a set of elements with two binary operations known as addition and multiplication, including for all a, b, c in F the following axioms are kept –

$$36 = 2 \times 2 \times 3 \times 3$$
$$60 = 2 \times 2 \times 3 \times 5$$

GCD = Multiplication of common factors

$$= 2 \times 2 \times 3$$
$$= 12$$

Examples:

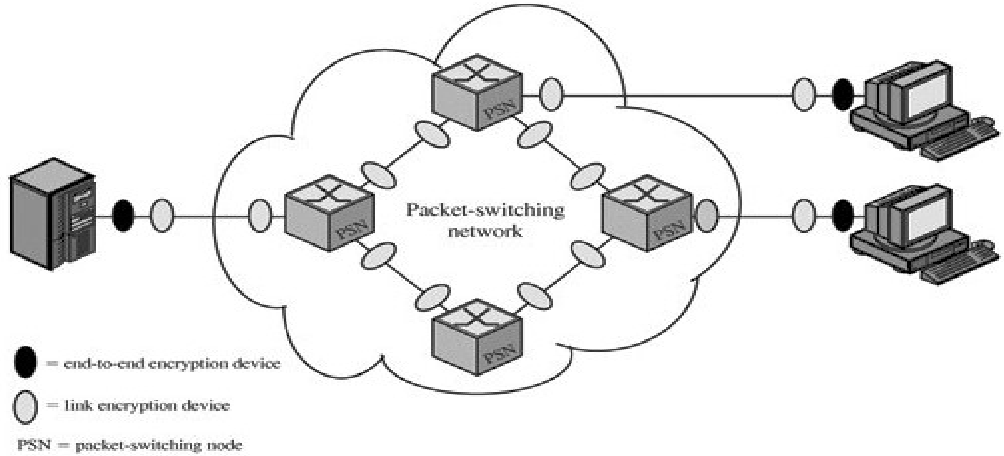
> ***Input:*** *a = 30, b = 20*
> ***Output:*** *gcd = 10, x = 1, y = -1*
> *(Note that 30*1 + 20*(-1) = 10)*
>
> ***Input:*** *a = 35, b = 15*
> ***Output:*** *gcd = 5, x = 1, y = -2*
> *(Note that 35*1 + 15*(-2) = 5)*

The extended Euclidean algorithm updates the results of gcd(a, b) using the results calculated by the recursive call gcd(b%a, a). Let values of x and y calculated by the recursive call be x_1 and y_1. x and y are updated using the below expressions.

holds (M7) - Multiplicative inverse axiom.

Because elements w of Zp are relatively prime to p, if we multiply all the elements of Zp by w, the resulting residues are all of elements Zp, permuted. Thus, exactly one of the residues has the value 1, respective multiplier is just the inverse element for w, designated w^{-1}. Now, equation (4.2) can be written without condition:

If $ab \equiv ac \bmod p$ then $b \equiv c \bmod p$ (4.4) located. To begin, this section examines the potential locations of security attacks and then looks at the two major approaches to encryption placement: link and end to end.



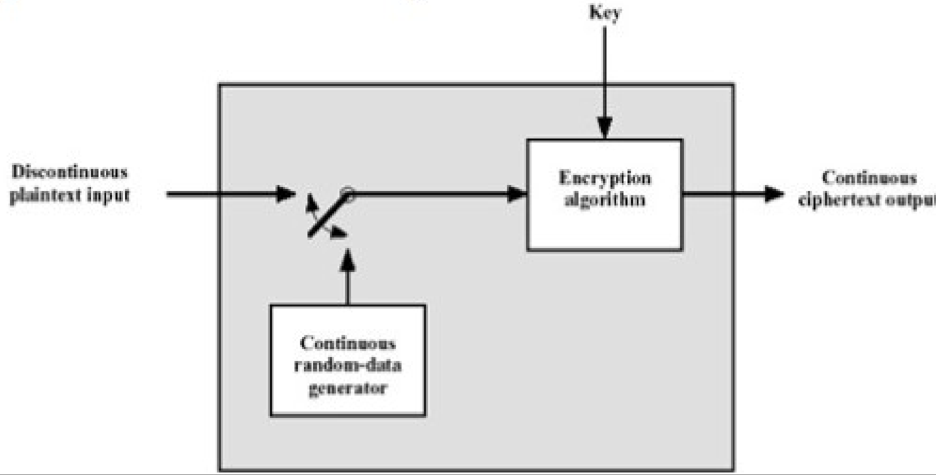
to read it.

The primary difference between link encryption and end-to-end encryption is that **link encryption** encrypts and decrypts all traffic at all points, not just at the endpoints. All data is encrypted as it travels along the communication line with this approach. When it reaches a router or another intermediary device, however, it is decrypted so that the intermediator can determine which direction to send it next.

Transparent to user	User applies encryption
Host maintains encryption facility	User must determine algorithm
One facility for all users	Users selects encryption scheme
Can be done in hardware	Software implementation
All or no messages encrypted	User chooses to encrypt, or not, for each message
Implementation Concerns	
Requires one key per (host-intermediate node) pair and (intermediate node-intermediate node) pair	Requires one key per user pair
Provides host authentication	Provides user authentication

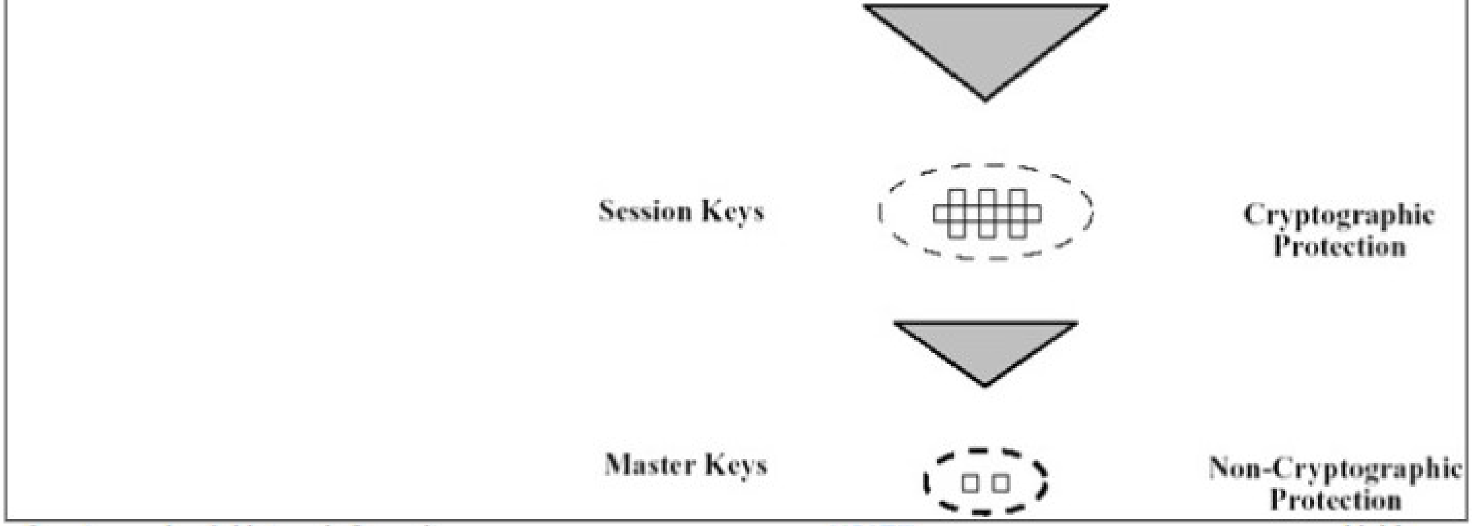
- Types of information derivable from traffic analysis
  - Identities of communicating partners
  - Frequency of communication
  - Message patterns, e.g., length, quantity, (encrypted) content
  - Correlation between messages and real world events
- Can (sometimes) be defeated through traffic padding

- Null message can be inserted randomly into the stream



- For conventional encryption to work, the two parties must share the same key and that key must be protected from access by others

- Alice's options in establishing a shared secret key with Bob include
  - Alice selects a key and physically delivers it to Bob
  - Trusted third party key distribution center (T3P or KDC) selects a key and physically delivers it to Alice and Bob
  - If Alice and Bob have previously and recently used a key, it can be used to distribute a new key
  - If Alice and Bob have keys with the T3P, rekeying can be accomplished similarly


Session Keys
Cryptographic
Protection
Master Keys
Non-Cryptographic
Protection

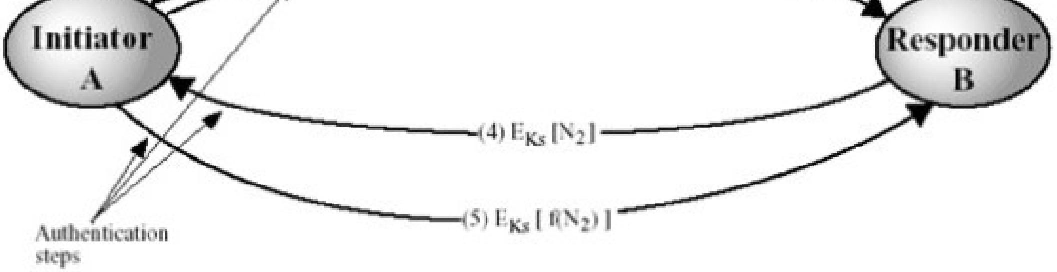


Figure 5.9 Key Distribution Scenario

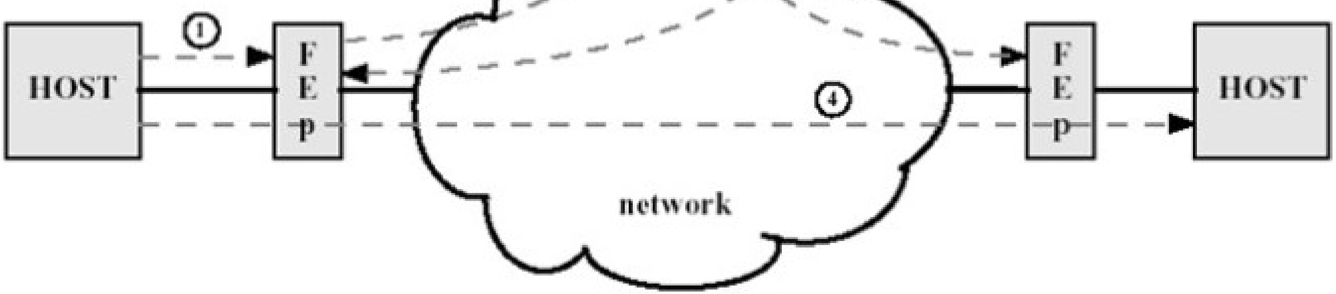


Figure 5.10 Automatic Key Distribution for Connection-Oriented Protocol

These applications give rise to two distinct and not necessarily compatible requirements for a sequence of random numbers:-randomness and unpredictability.

- Use of random numbers (in cryptography)
  - As key stream for a one-time pad
  - For session keys
  - For public key
  - For nonces (random numbers) in protocols to prevent repla

  - Good cryptography requires good random numbers

- Random number requirements
  - Statistically random (uniform distribution, etc)
  - Unpredictable (independent)

- Published lists
  - e.g., Rand Co. in 1955 published a book of 1 million numbers generated using an electronic roulette wheel
  - Predictable
- In practice, pseudorandom numbers are algorithmically derived from a deterministic PRNG (Pseudorandom Number Generator)