Confidentiality using Symmetric Encryption

Symmetric Encryption

- Traditionally symmetric encryption is used to provide message confidentiality

- If encryption is to be used to counter attacks on confidentiality, need to decide **what to encrypt** and **where the encryption** function should be located.

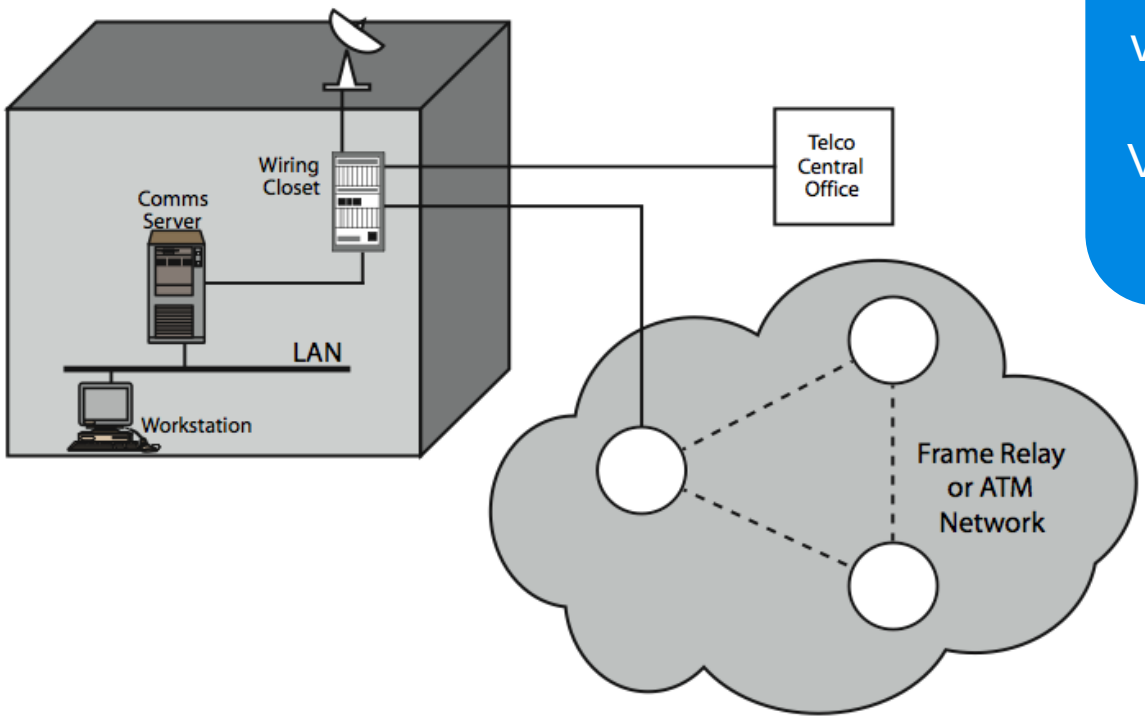
Potentials location for Confidentiality Attacks

- Potential locations of security attacks and then look at the two major approaches to encryption placement: link and end to end.
- Have many locations where attacks can occur in a typical scenario
  - workstations on LANs access other workstations & servers on LAN
  - LANs interconnected using switches/routers
  - with external lines or radio/satellite links

Potentials location for Confidentiality Attacks

- Consider attacks and placement in following scenario:
  - snooping from another workstation
  - use dial-in to LAN or server to snoop
  - physically tap line in wiring closet
  - use external router link to enter & snoop
  - monitor and/or modify traffic one external links

Potentials location for Confidentiality Attacks



Note:
physically vulnerable points

Vulnerable points in software

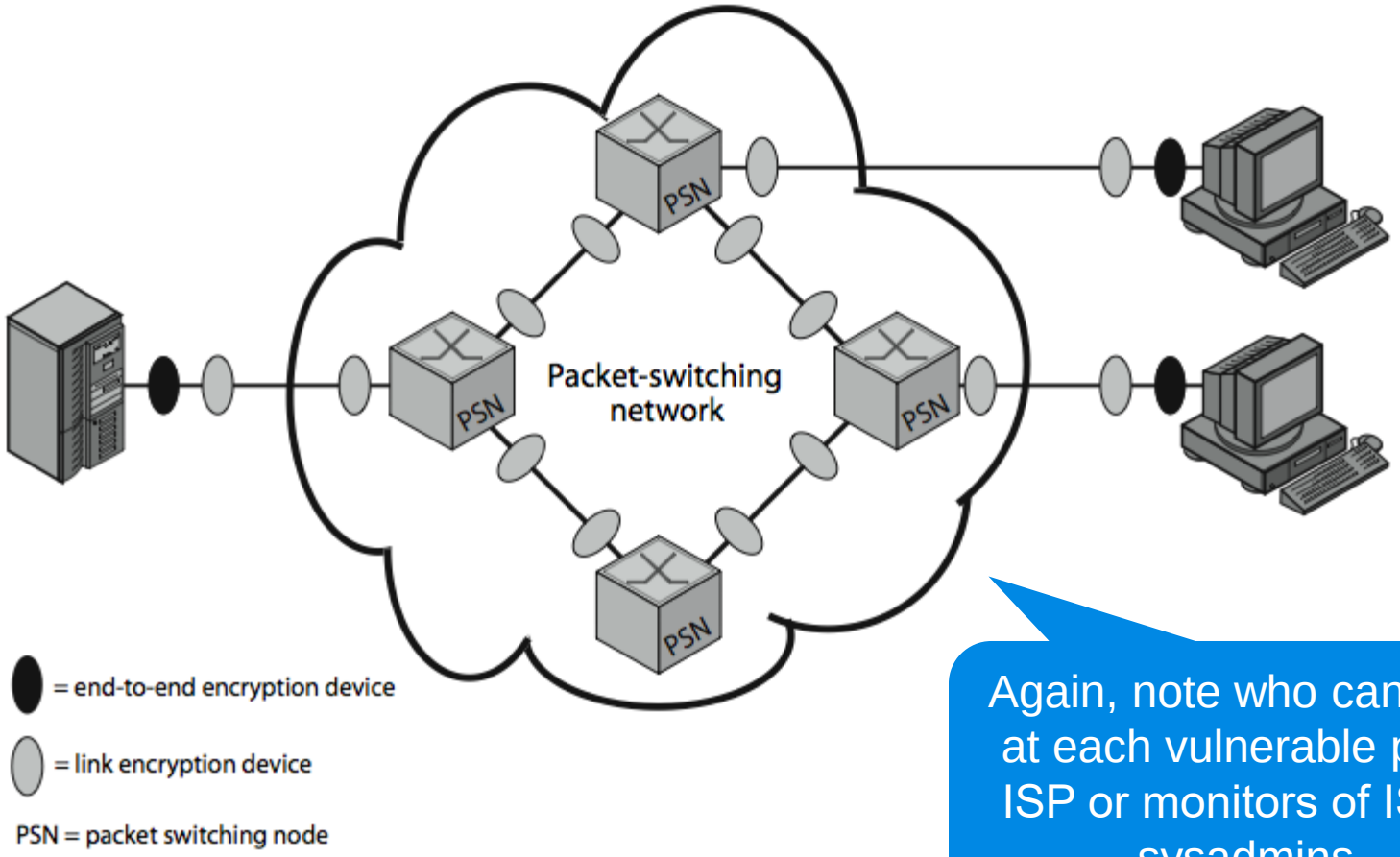
Placement of Encryption

- Have two major placement alternatives
- **Link encryption**
  - With link encryption, each vulnerable communications link is equipped on both ends with an encryption device
  - Each pair of nodes that share a link should share a unique key, with a different key used on each link
  - encryption occurs independently on every link
  - implies must decrypt traffic between links
  - requires many devices, but paired keys

Placement of Encryption

- **End-to-end encryption**
  - With end-to-end encryption, the encryption process is carried out at the two end systems.
  - encryption occurs between original source and final destination
  - need devices at each end with shared keys

Placement of Encryption



Again, note who can look at each vulnerable point ISP or monitors of ISP's sysadmins

Placement of Encryption

- When using end-to-end encryption must leave headers in clear
  - so network can correctly route information
- Hence although contents protected, traffic pattern flows are not
- Ideally want both at once
  - end-to-end protects data contents over entire path and provides authentication
  - link protects traffic flows from monitoring

Placement of Encryption

- Can place encryption function at various layers in OSI Reference Model
  - link encryption occurs at layers 1 or 2
  - end-to-end can occur at layers 3, 4, 6, 7
  - as move higher less information is encrypted but it is more secure though more complex with more entities and keys

Traffic Confidentiality

- Knowledge about the number and length of messages between nodes may enable an opponent to determine who is taking to whom.
- This can have obvious implications in a military conflict.
- Even in commercial applications, traffic analysis may yield information that the traffic generators would like to conceal.

Traffic Confidentiality

- The following types of information that can be derived from a traffic analysis attack:

- Identities of partners
- how frequent the partners are communicating,
- message pattern, message length, or quantity of messages that suggest important information is being exchanged
- the events that correlate with special conversation between particular partners.

Traffic Analysis

- Is monitoring of communications flows between parties
  - useful both in military & commercial spheres
  - can also be used to create a covert channel
- Link encryption obscures header details
  - but overall traffic volumes in networks and at end-points is still visible
- Traffic padding can further obscure flows
  - but at cost of continuous traffic

Traffic Analysis

- With the use of traffic patterns a covert channel can be established.
- A covert channel is a means of communication which transfers information unintended by the designers of the communication facility.
- The channel is used to transfer information in a way that violates a security policy.

Traffic Analysis

- Network layers are encrypted, reducing the opportunity for traffic analysis.
- It is still possible in those circumstances for an attacker to assess the amount of traffic on a network and to observe the amount of traffic entering and leaving each end system.
- Countermeasure to this type of attack is traffic padding.

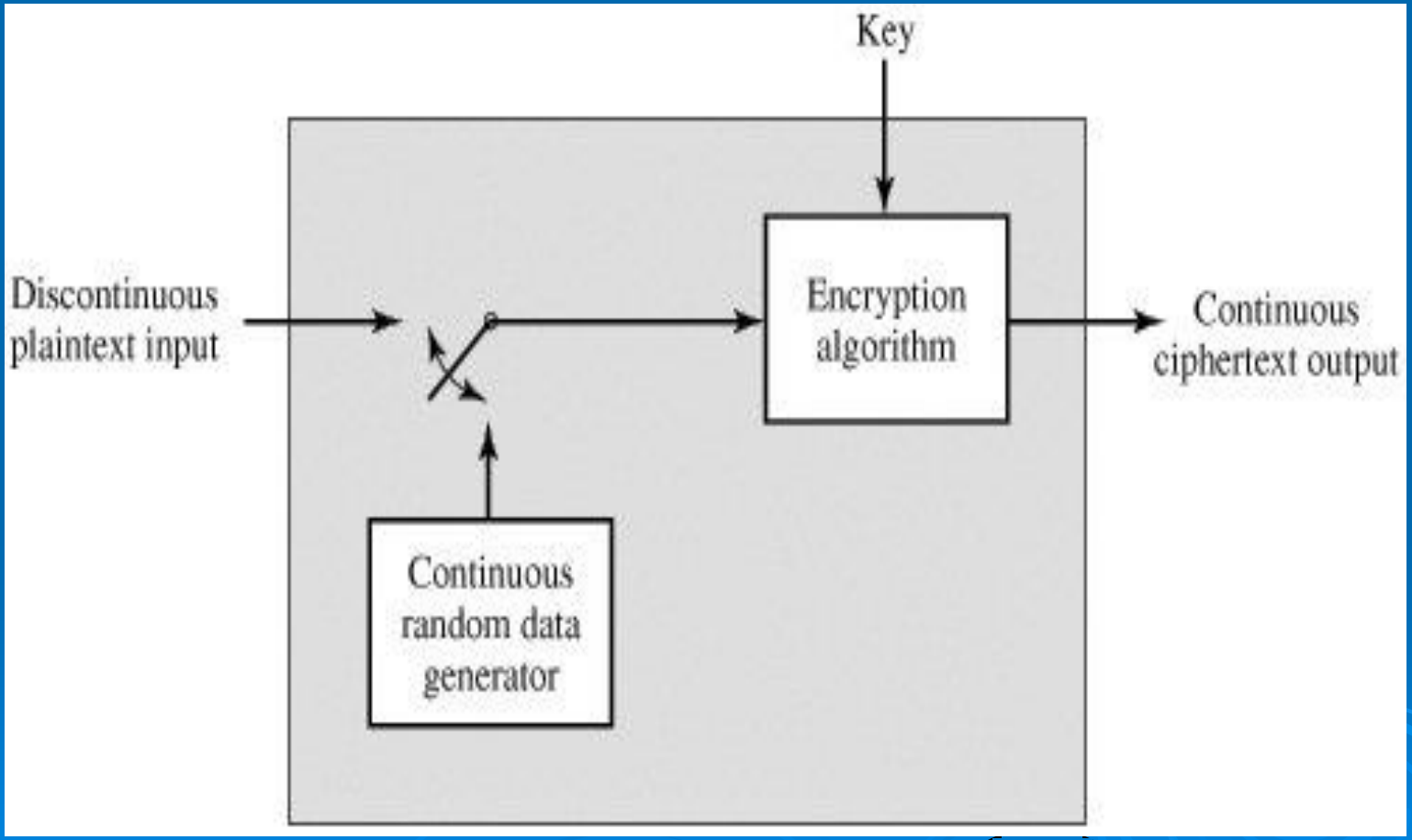
Traffic Padding

- Traffic padding produces cipher text output continuously, even in the absence of plain text.
- A continuous random data stream is generated.
- When plain text is available, it is encrypted and transmitted.
- When input plaintext is not present, random data are encrypted and transmitted.

Traffic Padding

- Traffic padding is essentially a link encryption function.
- If only end-to-end encryption is employed, then the measures available to the defender are more limited.
- If encryption is implemented at the application layer, then an opponent can determine transport layer, network-layer addresses and traffic patterns which remain accessible.

Traffic-Padding Encryption Device



Key Distribution

- Symmetric schemes require both parties to share a common secret key
- Issue is how to securely distribute this key
- Often secure system failure due to a break in the key distribution scheme

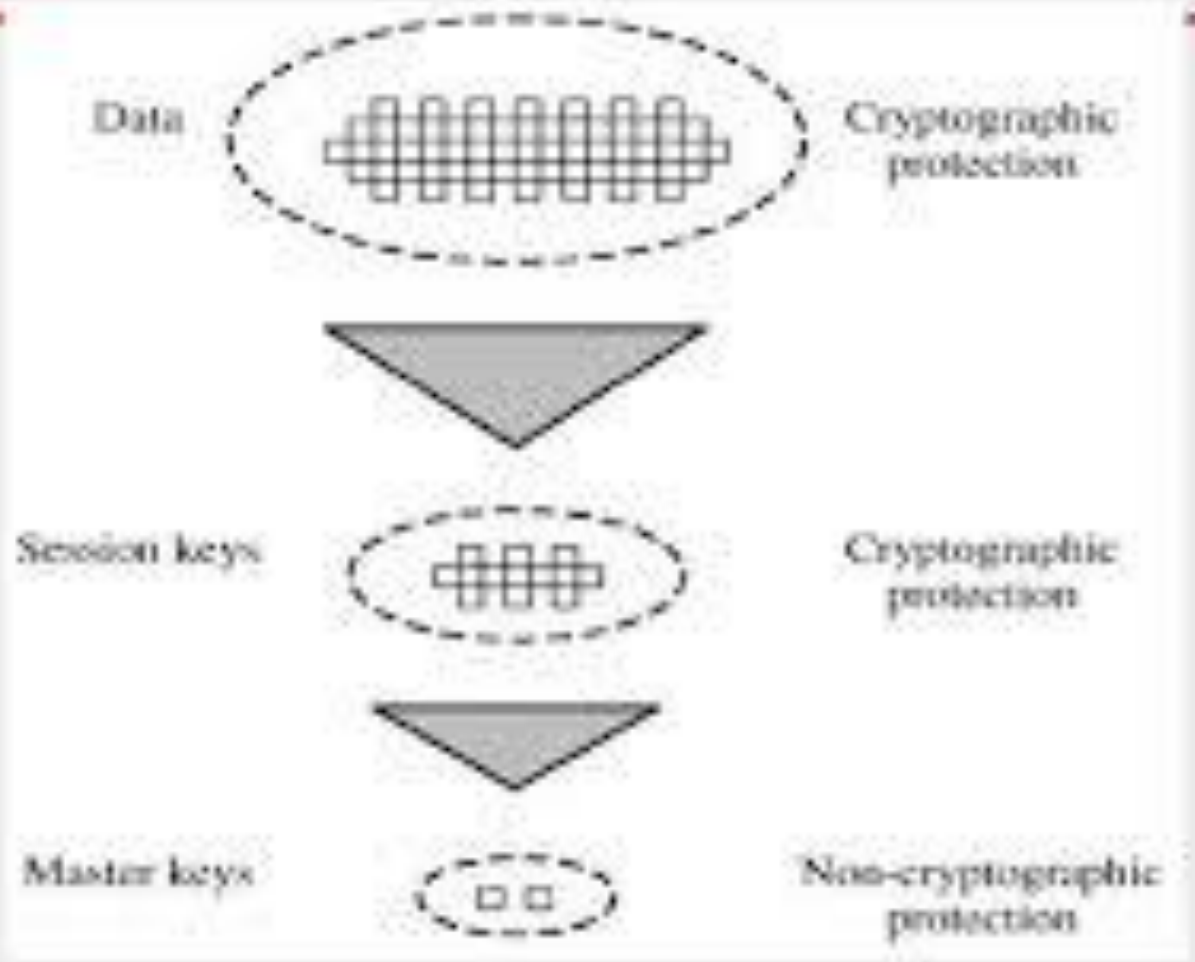
Key Distribution

- Given parties A and B have various **key distribution** alternatives:
  1. A can select key and physically deliver to B
  2. third party can select & deliver key to A & B
  3. if A & B have communicated previously can use previous key to encrypt a new key
  4. if A & B have secure communications with a third party C, C can relay key between A & B

Key Hierarchy

- Typically have a hierarchy of keys
- Session key
  - temporary key
  - used for encryption of data between users
  - for one logical session then discarded
- Master key
  - used to encrypt session keys
  - shared by user & key distribution center

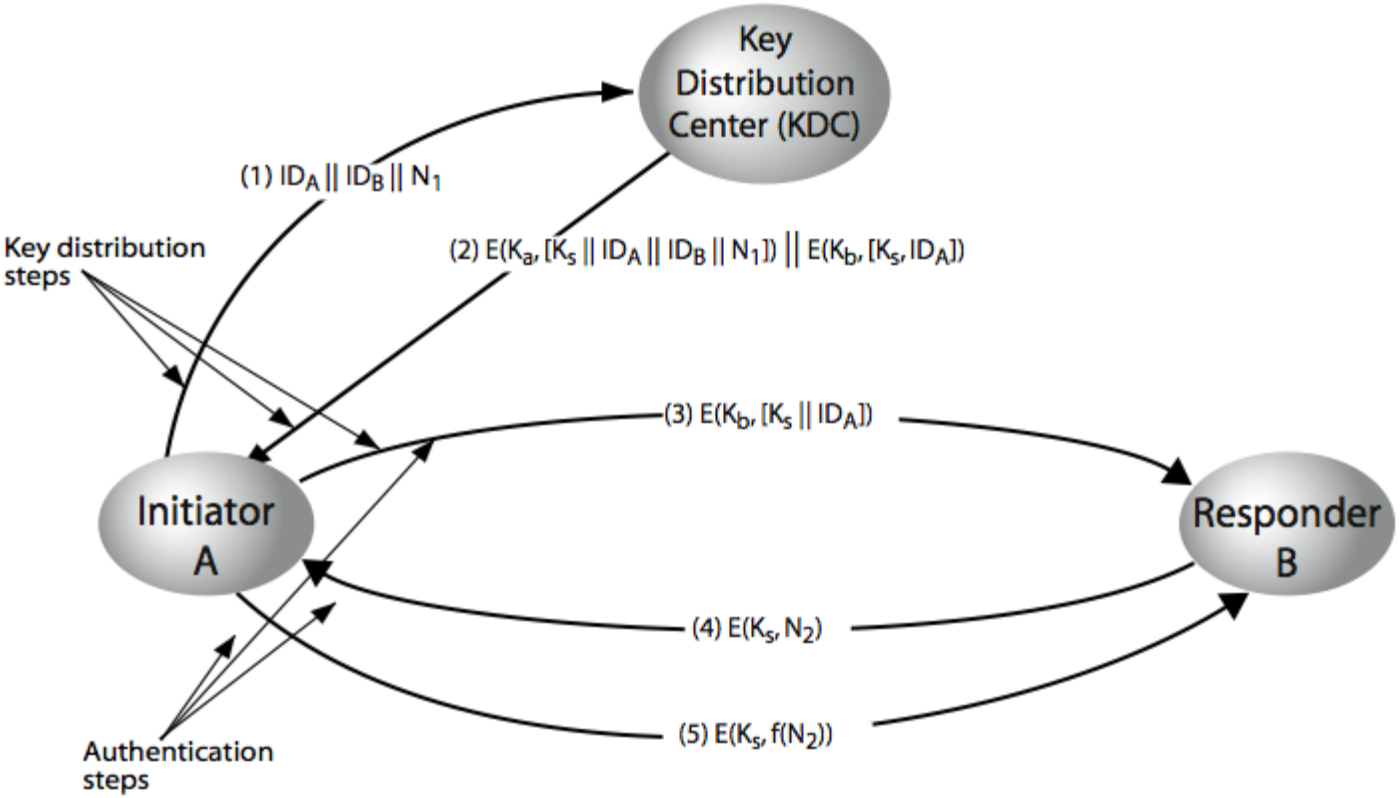
The Use of a Key Hierarchy



Key Distribution Issues

- Hierarchies of KDC's required for large networks, but must trust each other
- Session key lifetimes should be limited for greater security
- Use of automatic key distribution on behalf of users, but must trust system
- Use of decentralized key distribution
- Controlling key usage

Key Distribution Scenario



Random Numbers

- Many uses of **random numbers** in cryptography
  - nonces in authentication protocols to prevent replay
  - session keys
  - public key generation
  - keystream for a one-time pad
- In all cases its critical that these values be
  - statistically random, uniform distribution, independent
  - unpredictability of future values from previous values

Pseudorandom Number Generators (PRNGs)

- Often use deterministic algorithmic techniques to create “random numbers”
  - although are not truly random
  - can pass many tests of “randomness”
- Known as “pseudorandom numbers”
- Created by “Pseudorandom Number Generators (PRNGs)”

Using Block Ciphers as PRNGs

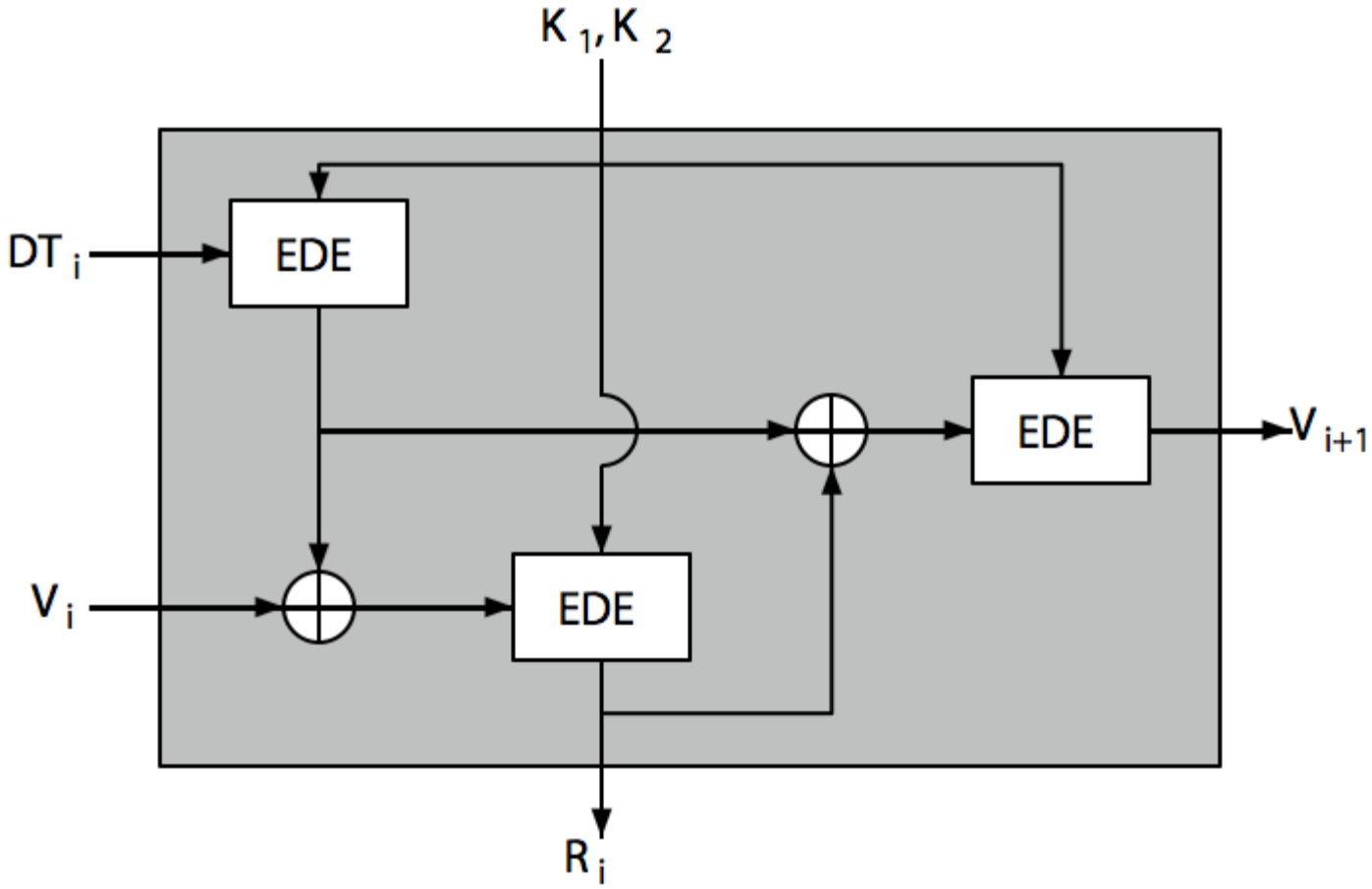
- For cryptographic applications, can use a block cipher to generate random numbers
- Often for creating session keys from master key
- Counter Mode

  $X_i = E_{Km}[i]$

- Output Feedback Mode

  $X_i = E_{Km}[X_{i-1}]$

ANSI X9.17 PRNG



Blum Blum Shub Generator

- Based on public key algorithms
- Use least significant bit from iterative equation:
  - $x_i = x_{i-1}^2 \bmod n$
  - where $n=p.q$, and primes $p,q=3 \bmod 4$
- Unpredictable, passes **next-bit** test
- Security rests on difficulty of factoring N
- Is unpredictable given any run of bits
- Slow, since very large numbers must be used
- Too slow for cipher use, good for key generation